jamk | IT

LabraNet *Remote access guide*

INTRODUCTION	2
VPN Connection	2
Windows 10	3
Windows 10 - additional settings	6
Mac OS X	11
Linux (Graphical)	18
Advanced routing	23
Windows	23
Mac OS X	24
Linux (Graphical)	25
Accessing Shares	26
Windows	27
Mac OS X	28
Linux (Graphical)	30
Linux (Command line)	32



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.

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



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 1. Change virtual private networks



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



Figure 2. 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.



Figure 3. VPN connection security settings

Click OK.



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.



Figure 4. 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



Figure 5. List network interface metrics

Note that the InterfaceMetric value assigned to the connection *Ethernet* is 25 in this example. Please use the lowest number for 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.

		Advanced TCP/IP Settings	×
P Network Connections		IP Settings DNS WINS	
 ← → ✓ ↑ ♥ ≪ Network and Organize ▼ Disconnect this corr 	d Internet > Network Connections nnection Rename this connection View status	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.	
LabraNet VPN Properties General Options Security Networking Sharing	LabraNet VPN Labranet.jamk.fi Internet Protocol Version 4 (TCP/IPv4) Properties General	Lise default gateway on remote network Disable class based route addition	
This connection uses the following items: 1.	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. (a) Obtain an IP address automatically	Interface metric: 15	_
	Use the following IP address:		
Description Transmission Control Protocol/Internet Protocol. Transmission Control Protocol/Internet Protocol. The default	Obtain DNS server address automatically Ouse the following DNS server addresses: Preferred DNS server:		
wide area network protocol that provides communication across diverse interconnected networks.	Alternate DNS server:	Advanced	ncel
OK Cancel	ОК	Cancel	

Figure 6. 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.

🔀 Administrator: Windows Powe	erShell			— C]
PS C:\Windows\system32> Get	-NetIPInterface	Select InterfaceAlias,	InterfaceMetric	Sort InterfaceMetr	ric
InterfaceAlias	InterfaceMetric				
thernet	25				
thernet	25				
Loopback Pseudo-Interface 1	L 75				
Loopback Pseudo-Interface 1	. 75				
▶S C:\Windows\system32> Get InterfaceAlias	-NetIPInterface InterfaceMetric	Select InterfaceAlias,	InterfaceMetric	Sort InterfaceMetr	ric
labranet VPN	15 /				
themest	25				
Ethernet Compack Recude Intenface 1	25				
Ethernet Loopback Pseudo-Interface 1	25 I 75				
Ethernet Loopback Pseudo-Interface 1 Ethernet Loopback Pseudo-Interface 1	25 L 75 4250				
Ethernet Loopback Pseudo-Interface 1 Ethernet Loopback Pseudo-Interface 1	25 I 75 4250 I 4300				
Ethernet Loopback Pseudo-Interface 1 Ethernet Loopback Pseudo-Interface 1 PS C:\Windows\system32> _	25 75 4250 I 4300				

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



Mac OS X

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

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.

Lc	cation: Automatic		O
Wi-Fi Connected Connected Not Connected	Status:	Connected Wi-Fi is connected to address 172.17.20.210	Turn Wi-Fi Off JAMK and has the IP 6.
• ThundeIt Bridge	Network Name:	JAMK JAkt to join new Known networks wi no known networks to manually select	cont this network networks Il be joined automatically. If a are available, you will have a network.
+ - * -	✓ Show Wi-Fi status	in menu bar	Advanced ?
			Revert Apply

Figure 8. 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)
	Cancel Create

Figure 9. Connection type

Click Create.

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

• Wi-Fi Connected	Status: Not Configured
Not Connected	
Not Connected	Configuration Default
VPN (L2TP)	Server Address Add Configuration
Not Configured	Account Name Rename "Default" Delete "Default"
	Authentication Settings
	Connect
+ - *	Show VPN status in menu bar Advanced ?

Figure 10. 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.

Connected	Status: Not Connected	
Bluetooth PAN Not Connected		
ThundeIt Bridge Not Connected	Configuration: LabraNet	0
VPN (L2TP)	Server Address: sslvpn.labranet.jamk.fi	
Not Configured	Account Name: YourLabranetUserID	
	Authentication Settin Connect	ıgs
+ - &-	Show VPN status in menu bar	Advanced

Figure 11. Configure basic settings



Remote access guide

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.

• Wi-Fi Connected	User Authentication: Password: RSA SecurID		••••	
 Bluetooth PAN Not Connected Thundelt Bridge Not Connected 	Kerberos CryptoCard	Select		0
• VPN (L2TP) Not Configured	Machine Authenticati Shared Secret: Certificate Group Name:	on: (Option Cancel	Select nal)	
+ - &~	Show VPI	N status in menu b	bar	Advanced ? Revert Apply

Figure 12. 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.



Remote access guide

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

	1.6	
• Wi-Fi Connected	Status: Conne	cted
	Connect Time: 0:00:48	Sent: Uppluggggggg
Connected	IP Address: 192.16	8.53.15 Received:
Bluetooth PAN Not Connected	Configuration: Labra	Net ᅌ
ThundeIt Bridge	Server Address: sslvpr	.labranet.jamk.fi
Not Connected	Account Name: YourLa	abraNetStudentID
	Disc	onnect
+ - *	Show VPN status in menu	bar Advanced
		Devert Ann

Figure 13. Completed connection

You can disconnect from the VPN connection by clicking Disconnect.



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. Full tunnel seems to work best in MacOS, check advanced routing chapter for instructions on how to change this.



Linux (Graphical)

These apply to Linux-distributions which use Network-Manager. In the examples we use Ubuntu 18.04 LTS (tested up to 20.04.5 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 update sudo apt install network-manager-sstp network-manager-sstp-gnome sstpclient

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

https://gitlab.com/eivnaes/sstp-client https://gitlab.gnome.org/GNOME/network-manager-sstp



Remote access guide

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



Figure 14. Network settings



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



Figure 15. Connection type



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

٩	Settings		Ne	etwork	l li	000
(i= 4	Wi-Fi	Wire	d		+	
*	Bluetooth Background	Cancel	Add VPN	Add)	
D	Dock	Name LabraNet VPN			+	
• Q	Notifications Search	General Gateway sslvpp.li	abranet.iamk.fi			
	Region & Language	Optional			f 🔯	
C D	Universal Access	Password ····	ur LabraNet username	å 0		
4	Privacy	NT Domain LA	Show password BRANET			
<	Sharing	CA Certificate (N	one)	<u>C</u>		
u(1)	Sound	 Ignore certificat Use TLS hostnan 	e warnings ne extensions			
Ge	Power			X Advanced		
ĝ	Network	_				
ō	Devices	>				
٨	Details	>				

Figure 16. 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.



Figure 17. Advanced settings

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



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.

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.



Mac OS X

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.

	Options TCP/IP DNS Pro	oxies
	Session Ontions:	
	Disconnect when switching user a	ccounts
	Disconnect when user logs out	
	🗹 Send all traffic over VPN connecti	on
	Advanced Options:	
	Use verbose logging	
?		Cancel OK



Click *OK* and *Apply*.



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.

٩	Settings			Network			
((1=	Wi-Fi						
*	Bluetooth		Wired			+	
⊴	Background	Cancel	LabraNet VPN V	'PN	APPY		
D	Dock	Details Identity IPV	, IPVO			+	
À	Notifications	IPv4 Method	 Automatic (DHCP) Manual 	 Link-Local C Disable 	Only		
Q	Search						
0	Region & Language	DNS		Automatic	ON	f 🗱	
6	Universal Access	Separate IP addresses wit	th commas				
en e		Poutor		Automatic			
-11	online Accounts	Address	Netmask	Gateway	Metric		
	Privacy			N 1	8		
<	Sharing	Use this connecti	on only for resources on	ICS NELWORK			
II (1)	Sound						
Ge	Power						
ō,							
÷	Devices	>					
٨	Details	>					

Figure 19. Advanced routing



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/*



Remote access guide

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.



Figure 20. Enter the network path



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.lab	pranet.jamk.fi/hom	es/vourid	+ 0~
avorite Servers:	,		
? Remove		Browse	Connect

Figure 21. 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.

<i>î</i> Mî	Enter your na "storage.labr	ame and password for the server anet.jamk.fi".	
•	Connect As:	Guest	
		Registered User	
	Name:	Your LabraNet username	
	Password:	•••••	
	Rememb	per this password in my keychain	
		Cancel	nect

Figure 22. Credentials for user



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.



Figure 23. Connecting to server shares



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



Figure 24. Creating the connection

Remote access guide



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.