Telkom

Telkom SA Limited

User Manual for Telkom Internet Static IP addresses for DSL

Document Information

Title:	User Manual for Telkom Internet Static IP addresses for DSL
Number:	TKG-xxxxxxxversion 01.000
Publication Date:	2015-07-07
Creation Date:	2015-06-04
Author:	Buchan Milne
Template:	TKG-000149 Version 01.000
Software Version:	N/A
Contact Detail:	Telkom SA SOC Limited
Postal Address:	
City/Town Postal Code, Country	
Tel:	10210 / 10217
Fax:	N/A
	www.telkomsa.net

Table of Contents

1. INTRODUCTION

The Static IP address feature for Telkom Internet DSL allows customers using ADSL or VDSL as access technology to have a fixed IP address, even though the Telkom ADSL network currently doesn't offer this feature natively.

In order to use this feature, the customer must be eligible for the static IP address feature, and have device that supports L2TP-based VPNs in a suitable position in their network for terminating the L2TP tunnel and ensuring security of devices that access the internet via the L2TP tunnel.

This document is intended to provide the general settings that a Telkom Internet customer should use in order to be able to effectively use the feature, as well as provide some screenshots/configurations for devices that have been tested.

2. KEYWORDS, ABBREVIATIONS AND ACRONYMS

The abbreviations and acronyms used in the document are listed in the table below.

Abbreviation	Description
DSL	Digital Subscriber Line
IP	Internet Protocol
L2TP	Layer 2 Tunnelling Protocol
LAC	L2TP Access Concentrator
LNS	L2TP Network Server
VPN	Virtual Private Network

3. HOW TO USE THIS MANUAL

This user manual is intended to assist the customer, who is entitled to use the static IP feature and has activated static IPs, in configuring the Telkom-supported modem (LAC) that supports the feature, as well as providing sufficient information to allow customers with other compatible platforms to configure their client (LAC).

You must activate the Static IP service using the Telkom Internet Service Management Tool before you will be able to use the feature effectively.

Please read all of section 4, before skipping to a configuration example in section 5. The examples use an example username onlineXXXXXX@telkomsa.net, and example password 'yourpassword'. Replace these with your Telkom Internet ADSL username and password.

After configuration of the static IP feature, please verify that any network security settings (e.g. firewall rules) that you had applied before are still applied on the new interface which will handle your internet traffic.

4. CONFIGURATION PARAMETERS

An L2TP Access Controller needs to be configured correctly be able to establish an L2TP tunnel with an L2TP Network Server (LNS).

The Telkom Internet Static IP address feature supports two different configurations, with tunnel authentication, and without tunnel authentication. Some devices may support one, or the other, or both. Devices that support both tunnel authentication and no tunnel authentication should use the setting without tunnel authentication (as there is no significant security benefit to using tunnel authentication in this scenario but slightly higher overhead).

4.1 Configuration parameters without tunnel authentication

Devices that do not support tunnel authentication **MUST** be configured with the settings below (if present), and the settings below are recommended for devices that support both modes:

Parameter	Value
Server IP address or name	staticip.telkomsa.net
Tunnel authentication	No
Tunnel secret	N/A
Authentication type	PAP
Username	<Telkom Internet username e.g. online123456@telkomsa.net>
Password	<Password for username used above, e.g. Test@123>

4.2 Configuration parameters with tunnel authentication

The following settings are recommended only for devices that do not support tunnels without tunnel authentication

Parameter	Value
Server IP address or name	staticip-auth.telkomsa.net
Tunnel authentication	Yes
Tunnel secret	l2tp
Authentication type	PAP
Username	<Telkom Internet username e.g. online123456@telkomsa.net>
Password	<Password for username used above, e.g. Test@123>

5. CONFIGURATION OF SUPPORTED TELKOM-SUPPLIED MODEMS

At present, the only modem (LAC) supplied by Telkom that supports the DSL Static IP feature is the Zyxel SBG3300.

5.1 Zyxel SBG3300

The settings for L2TP tunnels are accessible under the VPN->L2TP VPN menu

The Zyxel SBG300 supports both tunnel authentication and no tunnel authentication, and both options are displayed for reference.

5.1.1 Without tunnel authentication

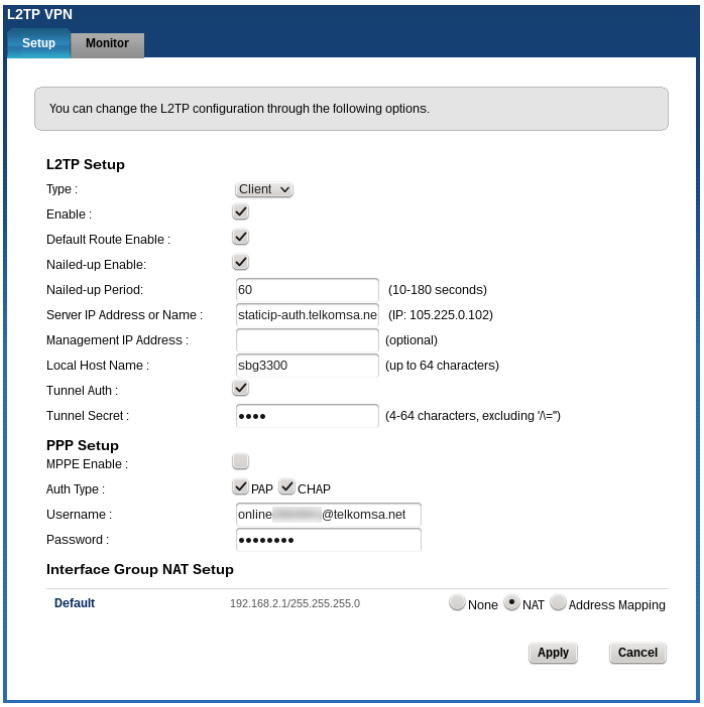
Configured as in 4.1, the Zyxel SBG3300s L2TP VPN configuration screen should look as shown. Values that were changed from their defaults in this screen are:

- Type: Client
- Server IP Address or Name: staticip.telkomsa.net
- Auth Type: check ‘PAP’
- Username: enter your Telkom Internet ADSL username
- Password: enter the password for your Telkom Internet ADSL username
- Under ‘Interface Group NAT Setup’, select NAT.

5.1.2 With tunnel authentication

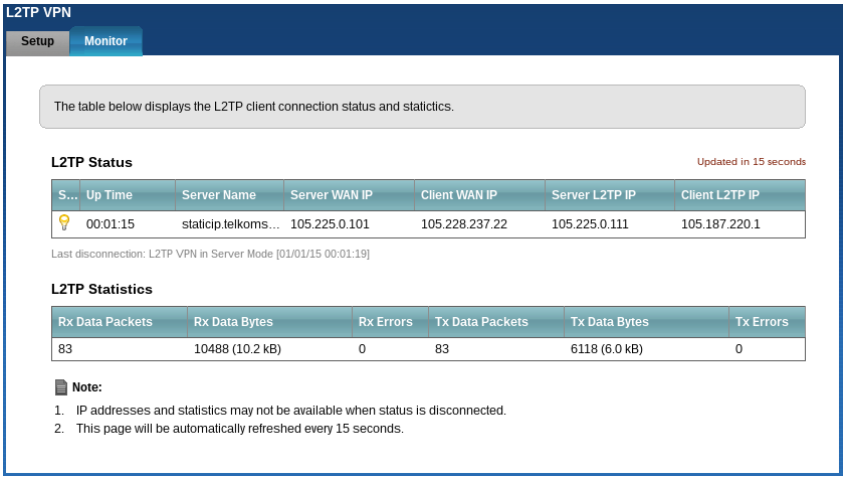
Configured as in 4.2, the Zyxel SBG3300s L2TP VPN configuration screen should look as shown. Additional values that were changed from the defaults in this screen are:

- Tunnel Auth: check the checkbox
- Tunnel secret: l2tp



5.1.3 Verification

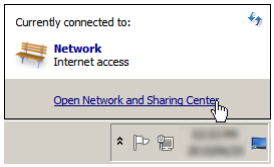
Once the L2TP connection has been configured successfully, the ‘Monitor’ tab should the L2TP connection, the ‘Client L2TP IP’ should match the IP address you were assigned when you activated the static IP feature.



6. CONFIGURATION OF UNSUPPORTED CLIENTS

The following section provides example configurations for clients besides the supported modem/client. While the configuration was tested successfully, no support can be provided for these clients. In a number of the following examples, the LAC may not be an ADSL modem, please ensure that the LAC has internet access before configuring the L2TP connection.

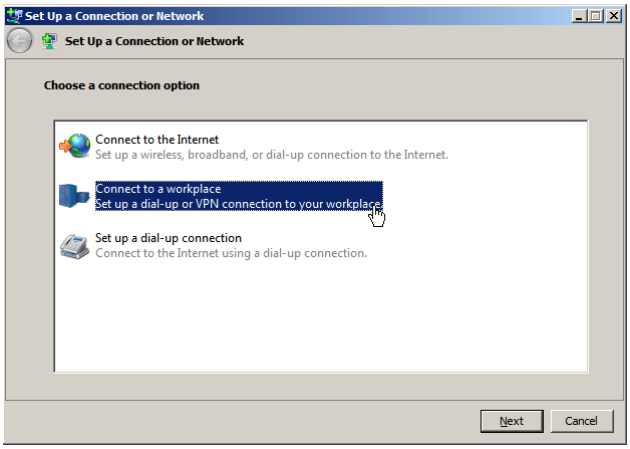
6.1 Windows



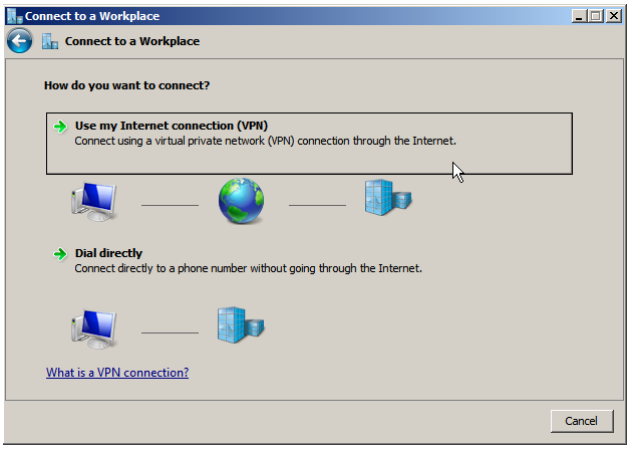
Windows Vista or later and Windows Server 2008 or later support L2TP VPNs, but default to requiring encryption and not allowing PAP authentication.

The steps to configure an L2TP VPN may differ slightly between different versions of Windows, but most dialogs are very similar.

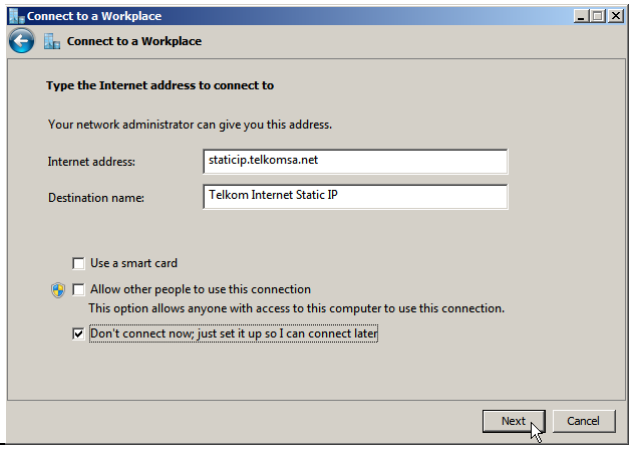
1. Create a new network connection (for example click the network icon in the system tray and click on 'Open Network and Sharing Center', then click on 'Set up a new connection or network')
2. The 'Set Up a Connection or Network' dialog will prompt you for the type of connection, choose 'Connect to a Workplace'.



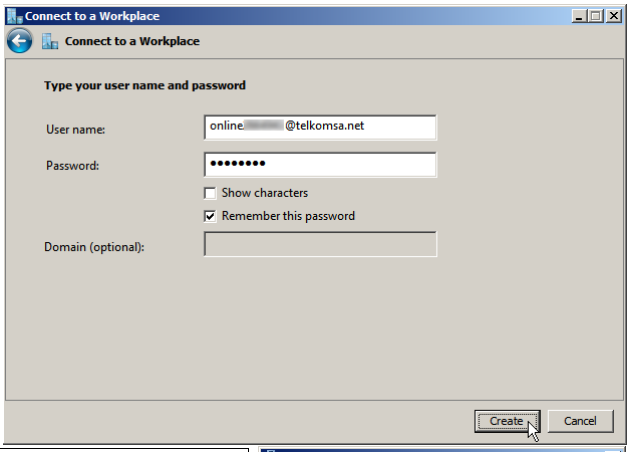
3. In the 'How do you want to connect?' dialog, choose 'Use my Internet connection (VPN)'.



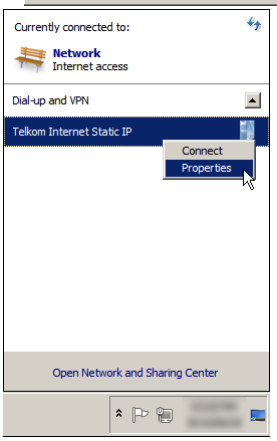
4. In the next dialog, enter 'staticip.telkomsa.net' as the 'Internet address' and enter a name you want to use for the VPN connection in the 'Destination name' text field. The connection will not be established correctly by default, so you may want to check the last checkbox.

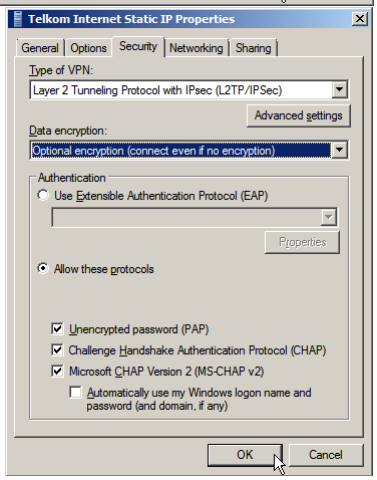


5. The next dialog will prompt for a username and password, enter your Telkom Internet ADSL username and password.
6. The next dialog will tell you that the connection is ready to use. Click the 'Close' button.



7. Edit the properties of the new virtual adapter (click on the network icon in the system tray, right click on the newly created VPN connection, and choose 'Properties').
8. In the properties dialog, select the 'Security' tab. In this tab, it is recommended to select the L2TP/IPSec option as the 'Type of VPN'. You must change 'Data encryption' to either 'Optional encryption' or 'No encryption allowed'. You must also check the 'Unencrypted password (PAP)' option under 'Allow these protocols'.





9. You should now be able to connect the L2TP connection by right-clicking on the virtual adapter and choosing 'Connect' (or from clicking on the network icon in the system tray, clicking on the virtual adapter, and clicking the 'Connect' button that appears).
10. If your ADSL connection is normally established by the same computer, you may want to select it in the 'Dial another connection first' drop-down on the 'General' tab and set this connection as the default connection.

6.2 Linux

There are a few different methods of creating L2TP VPNs under Linux. Which method might depend on which distribution you are using, and how you are using it (headless with CLI only, or GUI). We cover 2 different approaches that should work on most distributions, but there others as well.

6.2.1 Linux with L2TP plugin for Network Manager – GUI based

A plugin for configuring L2TP VPNs is available for Network Manager, which uses xl2tpd. Some Linux distributions may provide the package on the installation media or in the distribution's online package repository. Use your distribution's package manager (GUI or cli) to search for and install the plugin.

Distribution	CLI command to install the plugin
Fedora 20/21,RHEL6+ (with EPEL),Centos 6+	`yum install NetworkManager-l2tp`
Arch	`pacman -S networkmanager-l2tp`
Mageia 5+	`urpmi networkmanager-l2tp`

In a few other distributions, 3rd-party packages are available. Follow the instructions at the relevant URL to install the packages.

Distribution	Third-party package URL
Ubuntu Debian Mint	https://launchpad.net/~seriy-pr/+archive/ubuntu/network-manager-l2tp
openSUSE 13.x SUSE SLE-12	http://software.opensuse.org/package/NetworkManager-l2tp

If packages are not available for your distribution, you can install from source (https://github.com/seriyps/NetworkManager-l2tp/releases), or use one of the other approaches.

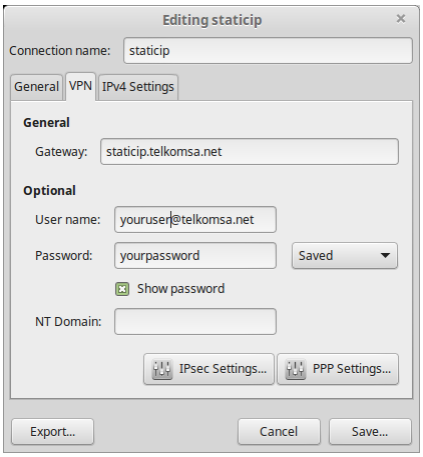
Installing the plugin should pull in the xl2tpd package, which might be enabled as a service. Be sure to disable it after installation (e.g. 'systemctl disable xl2tpd'), as having it running as a service can interfere with usage from Network Manager.

After installing the plugin, you will need to reboot (or at least restart the system messagebus) for the bus policy provided with the plugin to be applied to the system bus before you will be able to connect the VPN as non-root.

To configure the L2TP connection, use the following steps:

1. Open the Network Manager connection editor (in GTK3-based desktops you can right-click the network icon in the system tray, otherwise run 'nm-connection-editor')
2. Click the add button, and choose L2TP

3. In the dialog for the connection, enter 'staticip.telkomsa.net' for the 'Gateway', and enter your Telkom Internet ADSL username and password in the relevant text fields, and click 'Save'.



4. You should now be able to enable the VPN connection from the network icon in the system tray.
5. If you want the connection to start at boot, you may need to run some cli commands so that the configuration doesn't require a password agent:

```
nmcli c mod staticip vpn.data password-flags=0
nmcli c mod staticip +vpn.secrets password=yourpassword
```

You may want to modify the internet connection for the machine (e.g. an Ethernet or PPPoE) to start the VPN connection when the internet connection becomes available.

Alternatively, you can also configure the VPN connection using the CLI:

```
# nmcli connection add type vpn ifname staticip autoconnect true vpn-type l2tp user
onlineXXXXXX@telkomsa.net
Connection 'vpn-staticip' (98044f4f-329e-4da8-8d50-5f34490bfc05) successfully added
# nmcli con modify vpn-staticip +vpn.data gateway=staticip.telkomsa.net \
+vpn.secrets password=yourpassword
```

The VPN connections created via either method can also be started and stopped using nmcli, e.g. 'nmcli c u staticip' (or 'nmcli c u vpn-staticip') to start the connection or 'nmcli c d staticip' (or 'nmcli c d vpn-staticip') to stop it.

6.2.2 Linux with OpenL2TP (CLI)

The following configuration commands should be saved in /etc/openl2tpd.conf:

```
ppp profile modify profile_name=default auth_pap=yes default_route=yes
tunnel create tunnel_name=tistatic dest_ipaddr=staticip.telkomsa.net persist=yes \
auth_mode=none
session create tunnel_name=tistatic session_name=tistatic \
user_name=onlineXXXXXX@telkomsa.net user_password=yourpassword
```

OpenL2TP may not necessarily add a route to the LNS, you may find that you need to add a specific route to the LNS to ensure it doesn't try and route the L2TP traffic over the tunnel. For example, you may need to run the following command before starting OpenL2TP:

ip route add 105.225.0.101 via 10.0.0.2
or
ip route add 105.225.0.101 dev ppp0

You may rather want to ensure that the route is added with the internet interface comes up. The method will differ by distribution, but on Red-Hat-style systems you can do it by adding a line as follows to e.g. /etc/sysconfig/network-scripts/route-eth0 or /etc/sysconfig/network-scripts/route-ppp0:

```
105.225.0.101 dev eth0
```
or
```
105.225.0.101 dev ppp0
```

Starting openl2tpd (e.g. 'systemctl start openl2tp' or 'sudo service openl2tpd start') should result in the tunnel coming up.

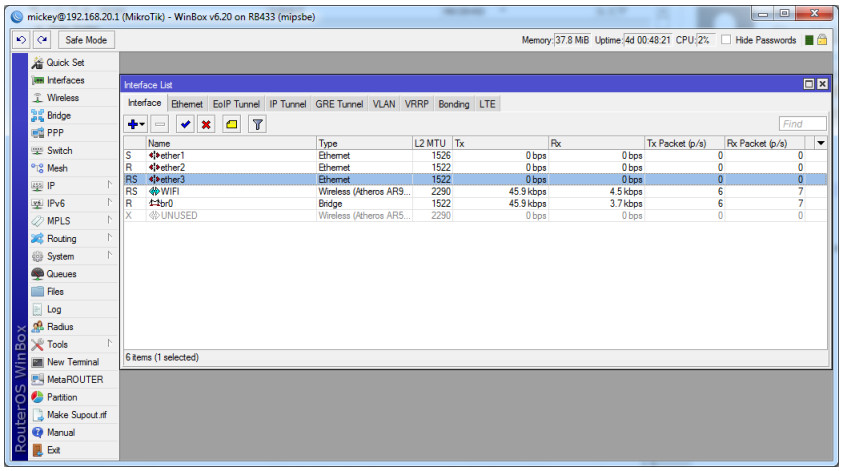
6.3 MikroTik

This example covers setting up both the ADSL connection and the static IP connection.

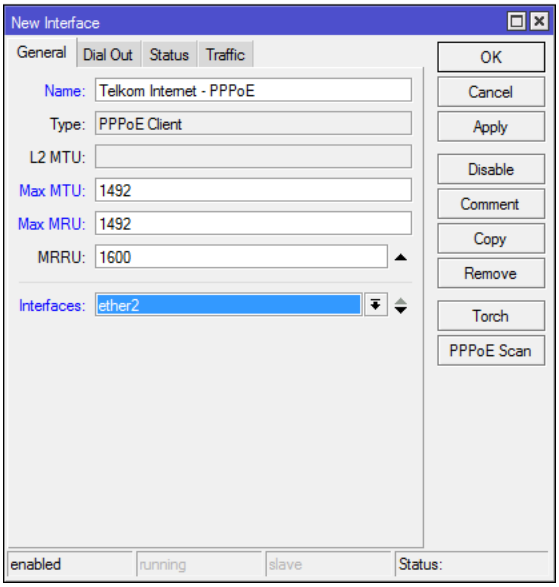
6.3.1 Setting up the ADSL connection on MicroTik

You need to have your MicroTik connected to the LAN port on your ADSL modem, which must be in Bridge, Half-Bridge or PPPoE-relay mode.

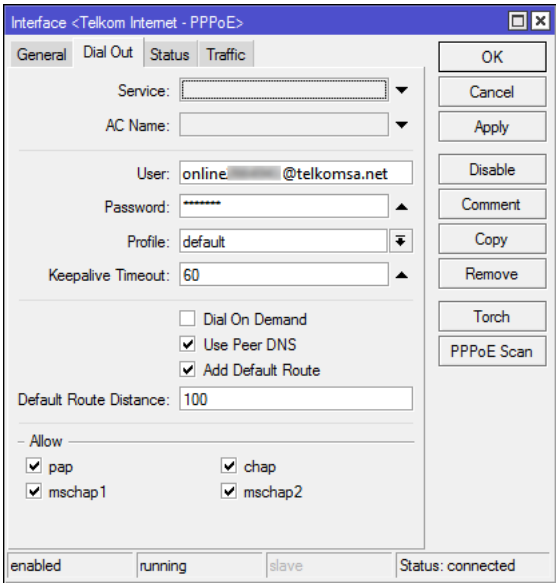
1. Open Interface window, click the plus and select PPPoE client



2. Change the MTU & MRU to 1492 and select the Interface on which PPPoE must be established

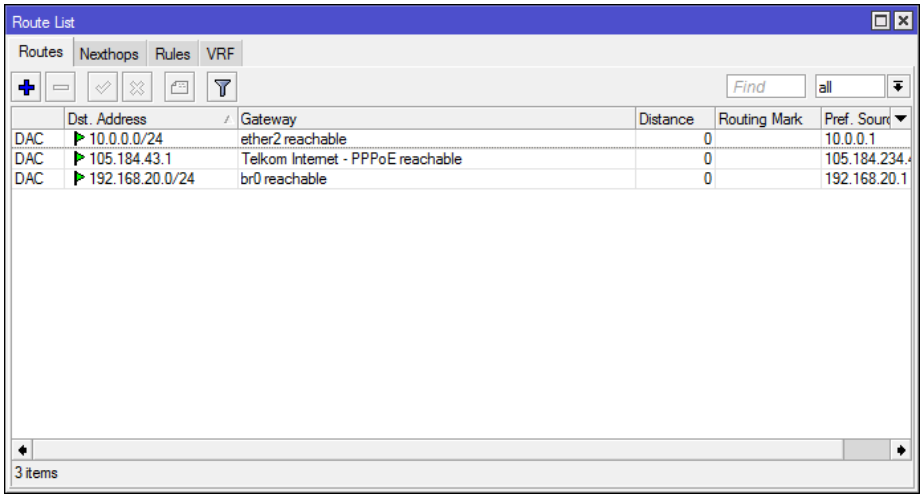


3. On the Dial Out tab, enter the username, password, select Use Peer DNS and select add Default Router with Default Route Distance of 100 (floating default route). Click OK

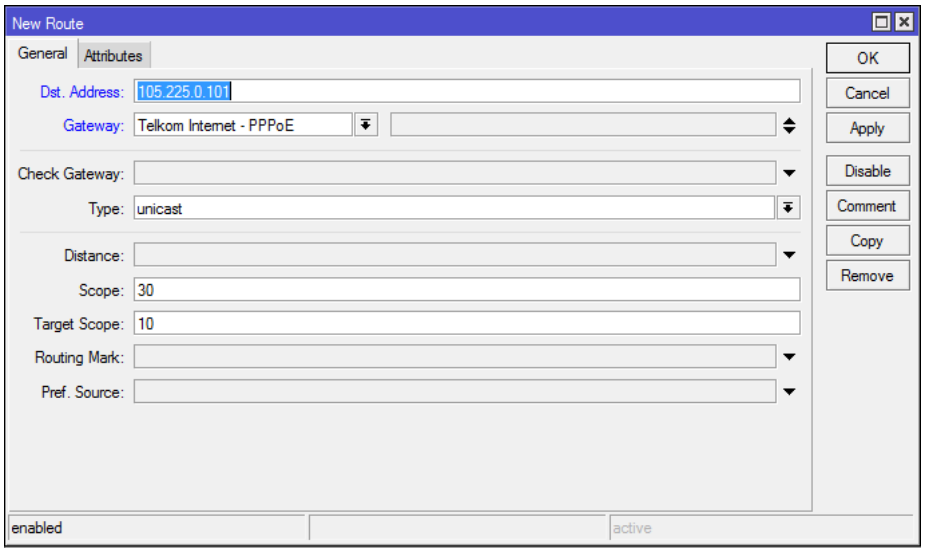


6.3.2 Setting up the L2TP connection on MikroTik

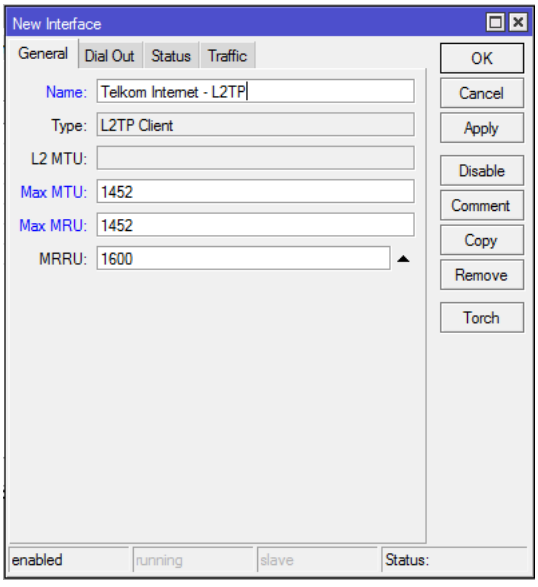
1. Open the IP -> Routes window and click the plus



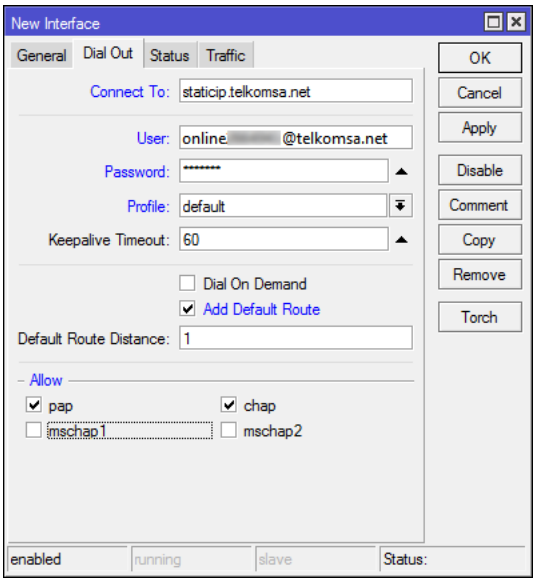
2. Add a route to 105.225.0.101 with the gateway of the newly created PPPoE interface



1. Open Interface window, click the plus and select L2TP client. On the 'General' tab, set the Max MTU and Max MRU to 1452.



2. Under the Dial Out tab, enter “staticip.telkomsa.net” into the Connect To field, populate the username & password, change the profile to default and select Add Default Route



3. Both the PPPoE and L2TP sessions should now be established
4. For basic NAT, head to the IP->Firewall window and select plus. Change “Out. Interface” to the newly create L2TP client. On the Action tab, select Action masquerade.

6.4 Cisco

This configuration presumes a Cisco router with an ADSL interface.

Create a dialler interface for the ADSL connection

```
interface Dialer1
 mtu 1492
 ip address negotiated
 ip virtual-reassembly in
 encapsulation ppp
 dialer pool 1
 dialer-group 1
 ppp pap sent-username onlineXXXXX@telkomsa.net password 0 yourpassword
 no cdp enable
!
```

Create a pseudowire class :

```
pseudowire-class L2TP
 encapsulation l2tpv2
 ip local interface Dialer1
!
```

Create a virtual PPP interface using the pseudowire:

```
interface Virtual-PPP2
 ip address negotiated
 ppp pap sent-username onlineXXXXX@telkomsa.net password 0 yourpassword
 no cdp enable
 pseudowire 105.225.0.101 1 pw-class L2TP
!
```