

L2TP Interface

Document revision 1.1 (Fri Mar 05 08:26:01 GMT 2004)

This document applies to V2.9

Table of Contents

[Table of Contents](#)

[General Information](#)

[Summary](#)

[Quick Setup Guide](#)

[Specifications](#)

[Related Documents](#)

[Description](#)

[L2TP Client Setup](#)

[Property Description](#)

[Example](#)

[Monitoring L2TP Client](#)

[Property Description](#)

[Example](#)

[L2TP Server Setup](#)

[Description](#)

[Property Description](#)

[Example](#)

[L2TP Server Users](#)

[Description](#)

[Property Description](#)

[Example](#)

[L2TP Application Examples](#)

[Router-to-Router Secure Tunnel Example](#)

[Connecting a Remote Client via L2TP Tunnel](#)

[L2TP Setup for Windows](#)

[Troubleshooting](#)

[Description](#)

General Information

Summary

L2TP (Layer 2 Tunnel Protocol) supports encrypted tunnels over IP. The MikroTik RouterOS implementation includes support for both L2TP client and server.

General applications of L2TP tunnels include:

- secure router-to-router tunnels over the Internet
- linking (bridging) local Intranets or LANs (in cooperation with EoIP)
- extending PPP user connections to a remote location (for example, to separate authentication and

Internet access points for ISP)

- accessing an Intranet/LAN of a company for remote (mobile) clients (employees)

Each L2TP connection is composed of a server and a client. The MikroTik RouterOS may function as a server or client or, for various configurations, it may be the server for some connections and client for other connections.

Quick Setup Guide

To make a L2TP tunnel between 2 MikroTik routers with IP addresses **10.5.8.104** (L2TP server) and **10.1.0.172** (L2TP client), follow the next steps.

- Configuration on L2TP server router:

1. Add a L2TP user:

```
[admin@L2TP-Server] ppp secret> add name=james password=pass \  
\... local-address=10.0.0.1 remote-address=10.0.0.2
```

2. Enable the L2TP server

```
[admin@L2TP-Server] interface l2tp-server server> set enabled=yes
```

- Configuration on L2TP client router:

1. Add a L2TP client:

```
[admin@L2TP-Client] interface l2tp-client> add user=james password=pass \  
\... connect-to=10.5.8.104
```

Specifications

Packages required: *ppp*

License required: *level1 (limited to 1 tunnel), level3 (limited to 200 tunnels), level5*

Home menu level: */interface l2tp-server, /interface l2tp-client*

Standards and Technologies: [L2TP \(RFC 2661\)](#)

Hardware usage: *Not significant*

Related Documents

- [Package Management](#)
- [IP Addresses and ARP](#)
- [PPP AAA](#)
- [EoIP Tunnel Interface](#)
- [IP Security](#)

Description

L2TP is a secure tunnel protocol for transporting IP traffic using PPP. L2TP encapsulates PPP in virtual lines that run over IP, Frame Relay and other protocols (that are not currently supported by MikroTik RouterOS).

L2TP incorporates PPP and MPPE (Microsoft Point to Point Encryption) to make encrypted links. The purpose of this protocol is to allow the Layer 2 and PPP endpoints to reside on different devices interconnected by a packet-switched network. With L2TP, a user has a Layer 2 connection to an access concentrator - **LAC** (e.g., modem bank, ADSL DSLAM, etc.), and the concentrator then tunnels individual PPP frames to the Network Access Server - **NAS**. This allows the actual processing of PPP packets to be divorced from the termination of the Layer 2 circuit. From the user's perspective, there is no functional difference between having the L2 circuit terminate in a NAS directly or using L2TP.

It may also be useful to use L2TP just as any other tunneling protocol with or without encryption. The L2TP standard says that the most secure way to encrypt data is using L2TP over IPsec (**Note** that it is default mode for Microsoft L2TP client) as all L2TP control and data packets for a particular tunnel appear as homogeneous UDP/IP data packets to the IPsec system.

L2TP includes PPP authentication and accounting for each L2TP connection. Full authentication and accounting of each connection may be done through a RADIUS client or locally.

MPPE 40bit RC4 and MPPE 128bit RC4 encryption are supported.

L2TP traffic uses UDP protocol for both control and data packets. UDP port 1701 is used only for link establishment, further traffic is using any available UDP port (which may or may not be 1701). This means that L2TP can be used with most firewalls and routers (even with NAT) by enabling UDP traffic to be routed through the firewall or router.

L2TP Client Setup

Home menu level: */interface l2tp-client*

Property Description

name (*name*; default: **l2tp-outN**) - interface name for reference

mtu (*integer*; default: **1460**) - Maximum Transmission Unit. The optimal value is the MTU of the interface the tunnel is working over decreased by 40 (so, for 1500-byte Ethernet link, set the MTU to 1460 to avoid fragmentation of packets)

mru (*integer*; default: **1460**) - Maximum Receive Unit. The optimal value is the MRU of the interface the tunnel is working over decreased by 40 (so, for 1500-byte Ethernet link, set the MRU to 1460 to avoid fragmentation of packets)

connect-to (*IP address*) - The IP address of the L2TP server to connect to

user (*text*) - user name to use when logging on to the remote server

password (*text*; default: **''**) - user password to use when logging to the remote server

profile (*name*; default: **default**) - profile to use when connecting to the remote server

allow (*multiple choice: mschap2, mschap1, chap, pap*; default: **mschap2, mschap1, chap, pap**) - the protocol to allow the client to use for authentication

add-default-route (*yes | no*; default: **no**) - whether to use the server which this client is connected to as its default router (gateway)

Example

To set up L2TP client named **test2** using username **john** with password **john** to connect to the **10.1.1.12**

L2TP server and use it as the default gateway:

```
[admin@MikroTik] interface l2tp-client> add name=test2 connect-to=10.1.1.12 \
\... user=john add-default-route=yes password=john
[admin@MikroTik] interface l2tp-client> print
Flags: X - disabled, R - running
 0 X name="test2" mtu=1460 mru=1460 connect-to=10.1.1.12 user="john"
    password="john" profile=default add-default-route=yes

[admin@MikroTik] interface l2tp-client> enable 0
```

Monitoring L2TP Client

Command name: */interface l2tp-client monitor*

Property Description

status (*text*) - status of the client

- **Dialing** - attempting to make a connection
- **Verifying password...** - connection has been established to the server, password verification in progress
- **Connected** - self-explanatory
- **Terminated** - interface is not enabled or the other side will not establish a connection uptime (time) - connection time displayed in days, hours, minutes and seconds

encoding (*text*) - encryption and encoding (if asymmetric, separated with '/') being used in this connection

Example

Example of an established connection

```
[admin@MikroTik] interface l2tp-client> monitor test2
status: "connected"
uptime: 4m27s
encoding: "MPPE128 stateless"
[admin@MikroTik] interface l2tp-client>
```

L2TP Server Setup

Home menu level: */interface l2tp-server server*

Description

The L2TP server creates a dynamic interface for each connected L2TP client. The L2TP connection count from clients depends on the license level you have. Level1 license allows 1 L2TP client, Level3 or Level4 licenses up to 200 clients, and Level5 or Level6 licenses do not have L2TP client limitations.

To create L2TP users, you should consult the [PPP secret](#) and [PPP Profile](#) manuals. It is also possible to use the MikroTik router as a RADIUS client to register the L2TP users, see the [manual](#) how to do it.

Property Description

enabled (*yes | no*; default: **no**) - defines whether L2TP server is enabled or not

mtu (*integer*; default: **1460**) - Maximum Transmission Unit. The optimal value is the MTU of the interface the tunnel is working over decreased by 40 (so, for 1500-byte Ethernet link, set the MTU to 1460 to avoid fragmentation of packets)

mru (*integer*; default: **1460**) - Maximum Receive Unit. The optimal value is the MRU of the interface the tunnel is working over decreased by 40 (so, for 1500-byte Ethernet link, set the MRU to 1460 to avoid fragmentation of packets)

authentication (*multiple choice: pap | chap | mschap1 | mschap2*; default: **mschap2**) - authentication algorithm

default-profile - default profile to use

Example

To enable L2TP server:

```
[admin@MikroTik] interface l2tp-server server> set enabled=yes
[admin@MikroTik] interface l2tp-server server> print
    enabled: yes
      mtu: 1460
      mru: 1460
 authentication: mschap2
 default-profile: default
[admin@MikroTik] interface l2tp-server server>
```

L2TP Server Users

Home menu level: */interface l2tp-server*

Description

There are two types of items in L2TP server configuration - static users and dynamic connections. A dynamic connection can be established if the user database or the **default-profile** has its **local-address** and **remote-address** set correctly. When static users are added, the default profile may be left with its default values and only PPP user (in **/ppp secret**) should be configured. **Note** that in both cases PPP users must be configured properly.

Property Description

name (*name*) - interface name

user (*text*) - the name of the user that is configured statically or added dynamically

mtu - shows client's MTU

client-address - shows the IP of the connected client

uptime - shows how long the client is connected

encoding (*text*) - encryption and encoding (if asymmetric, separated with '/') being used in this connection

Example

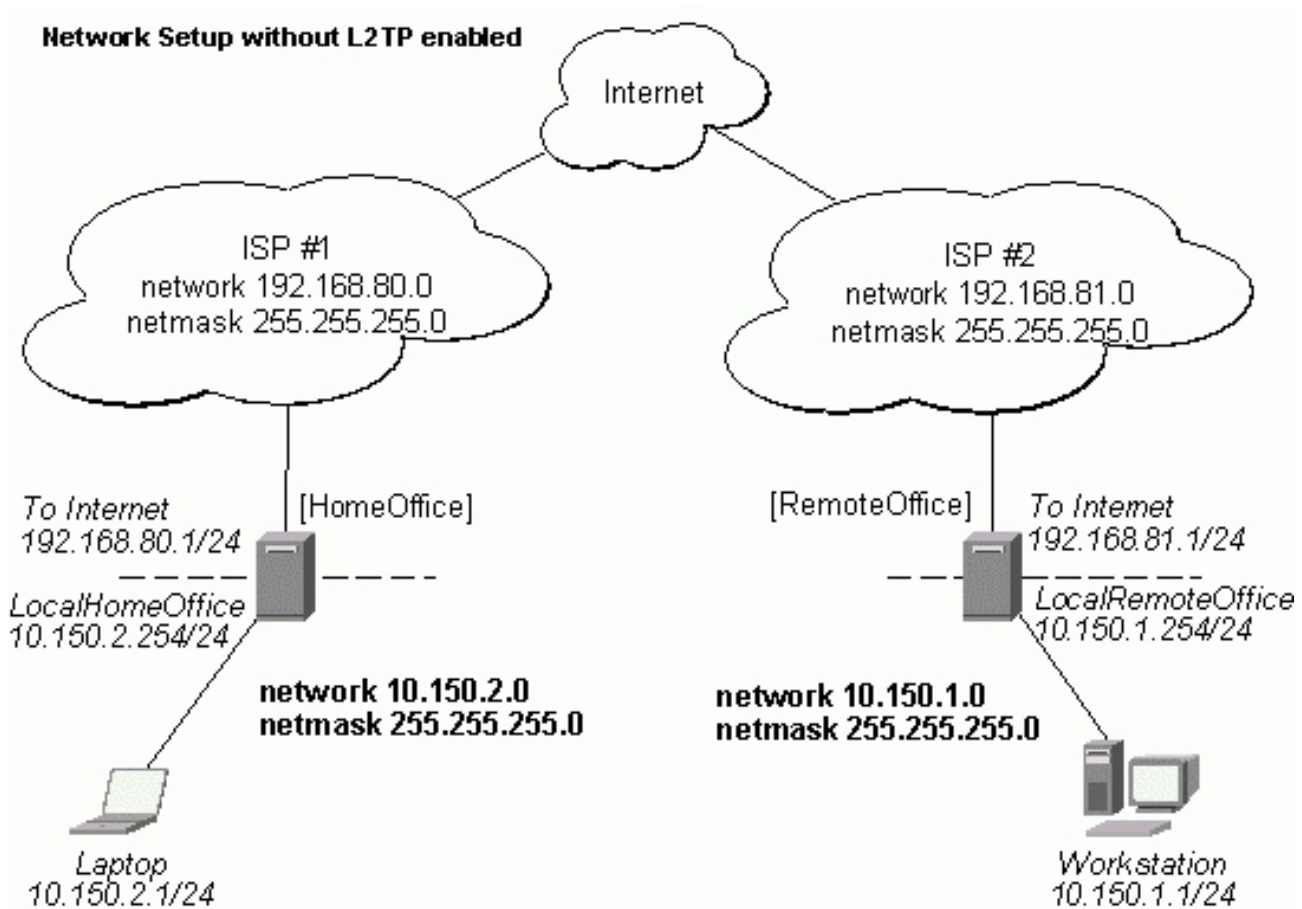
To add a static entry for **ex1** user:

```
[admin@MikroTik] interface l2tp-server> add user=ex1
[admin@MikroTik] interface l2tp-server> print
Flags: X - disabled, D - dynamic, R - running
#   NAME           USER      MTU     CLIENT-ADDRESS  UPTIME   ENC...
0   DR <l2tp-ex>    ex        1460    10.0.0.202     6m32s   none
1   l2tp-in1       ex1
[admin@MikroTik] interface l2tp-server>
```

In this example an already connected user **ex** is shown besides the one we just added.

L2TP Application Examples

Router-to-Router Secure Tunnel Example



There are two routers in this example:

- [HomeOffice]
Interface LocalHomeOffice 10.150.2.254/24
Interface ToInternet 192.168.80.1/24
- [RemoteOffice]
Interface ToInternet 192.168.81.1/24
Interface LocalRemoteOffice 10.150.1.254/24

Each router is connected to a different ISP. One router can access another router through the Internet.

On the L2TP server a user must be set up for the client:

```
[admin@HomeOffice] ppp secret> add name=ex service=l2tp password=lkjrht
local-address=10.0.103.1 remote-address=10.0.103.2
[admin@HomeOffice] ppp secret> print detail
Flags: X - disabled
0 name="ex" service=l2tp caller-id="" password="lkjrht" profile=default
local-address=10.0.103.1 remote-address=10.0.103.2 routes=""
[admin@HomeOffice] ppp secret>
```

Then the user should be added in the L2TP server list:

```
[admin@HomeOffice] interface l2tp-server> add user=ex
[admin@HomeOffice] interface l2tp-server> print
Flags: X - disabled, D - dynamic, R - running
# NAME USER MTU CLIENT-ADDRESS UPTIME ENC...
0 l2tp-in1 ex
[admin@HomeOffice] interface l2tp-server>
```

And finally, the server must be enabled:

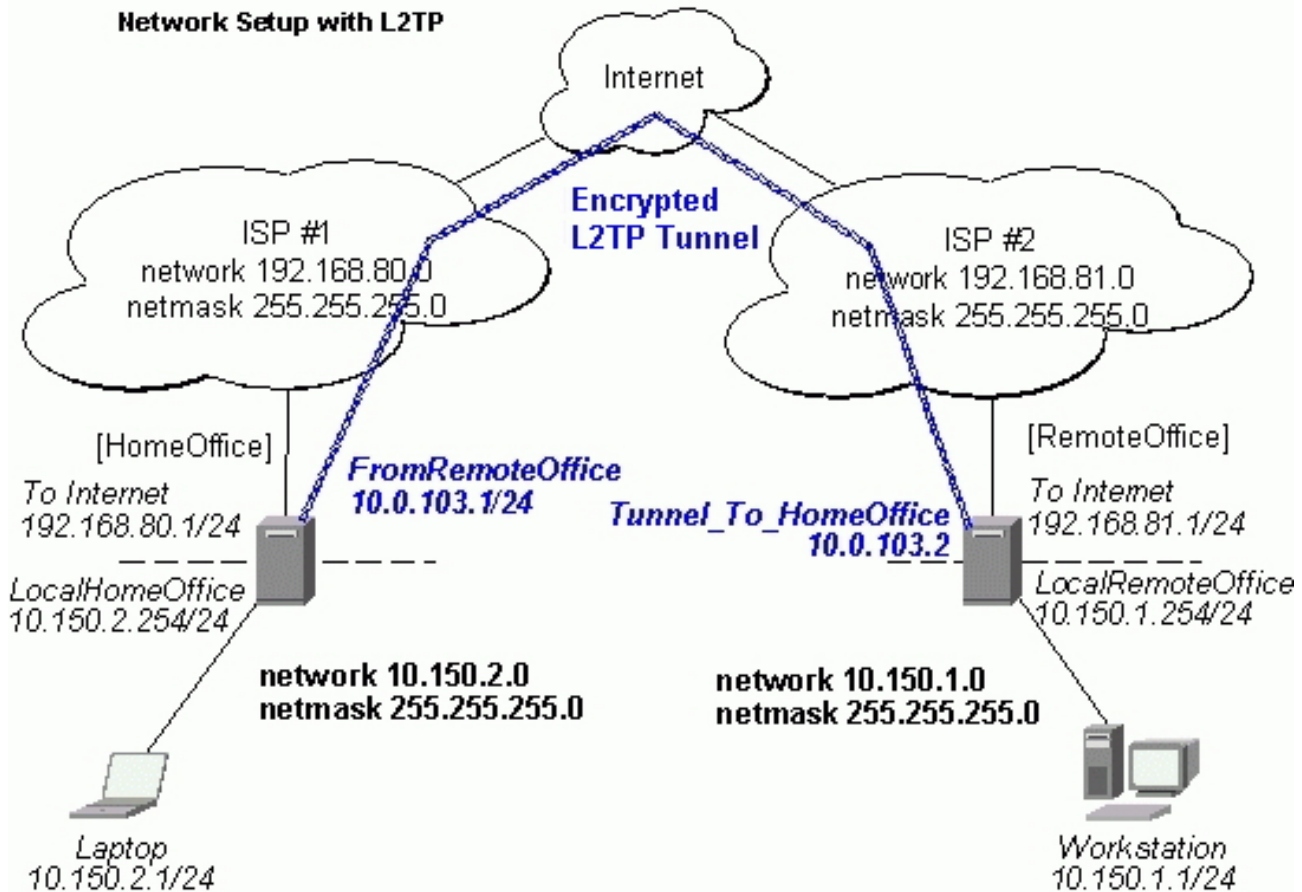
```
[admin@HomeOffice] interface l2tp-server server> set enabled=yes
[admin@HomeOffice] interface l2tp-server server> print
enabled: yes
mtu: 1460
mru: 1460
authentication: mschap2
default-profile: default
[admin@HomeOffice] interface l2tp-server server>
```

Add a L2TP client to the RemoteOffice router:

```
[admin@RemoteOffice] interface l2tp-client> add connect-to=192.168.80.1 user=ex \
...\ password=lkjrht disabled=no
[admin@RemoteOffice] interface l2tp-client> print
Flags: X - disabled, R - running
0 R name="l2tp-out1" mtu=1460 mru=1460 connect-to=192.168.80.1 user="ex"
password="lkjrht" profile=default add-default-route=no
[admin@RemoteOffice] interface l2tp-client>
```

Thus, a L2TP tunnel is created between the routers. This tunnel is like an Ethernet point-to-point connection between the routers with IP addresses 10.0.103.1 and 10.0.103.2 at each router. It enables 'direct' communication between the routers over third party networks.

Network Setup with L2TP



To route the local Intranets over the L2TP tunnel you need to add these routes:

```
[admin@HomeOffice] > ip route add dst-address 10.150.1.0/24 gateway 10.0.103.2
[admin@RemoteOffice] > ip route add dst-address 10.150.2.0/24 gateway 10.0.103.1
```

On the L2TP server it can alternatively be done using **routes** parameter of the user configuration:

```
[admin@HomeOffice] ppp secret> print detail
Flags: X - disabled
0 name="ex" service=l2tp caller-id="" password="lkjrht" profile=default
  local-address=10.0.103.1 remote-address=10.0.103.2 routes=""

[admin@HomeOffice] ppp secret> set 0 routes="10.150.1.0/24 10.0.103.2 1"
[admin@HomeOffice] ppp secret> print detail
Flags: X - disabled
0 name="ex" service=l2tp caller-id="" password="lkjrht" profile=default
  local-address=10.0.103.1 remote-address=10.0.103.2
  routes="10.150.1.0/24 10.0.103.2 1"

[admin@HomeOffice] ppp secret>
```

Test the L2TP tunnel connection:

```
[admin@RemoteOffice]> /ping 10.0.103.1
10.0.103.1 pong: ttl=255 time=3 ms
10.0.103.1 pong: ttl=255 time=3 ms
10.0.103.1 pong: ttl=255 time=3 ms
ping interrupted
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 3/3.0/3 ms
```

Test the connection through the L2TP tunnel to the LocalHomeOffice interface:

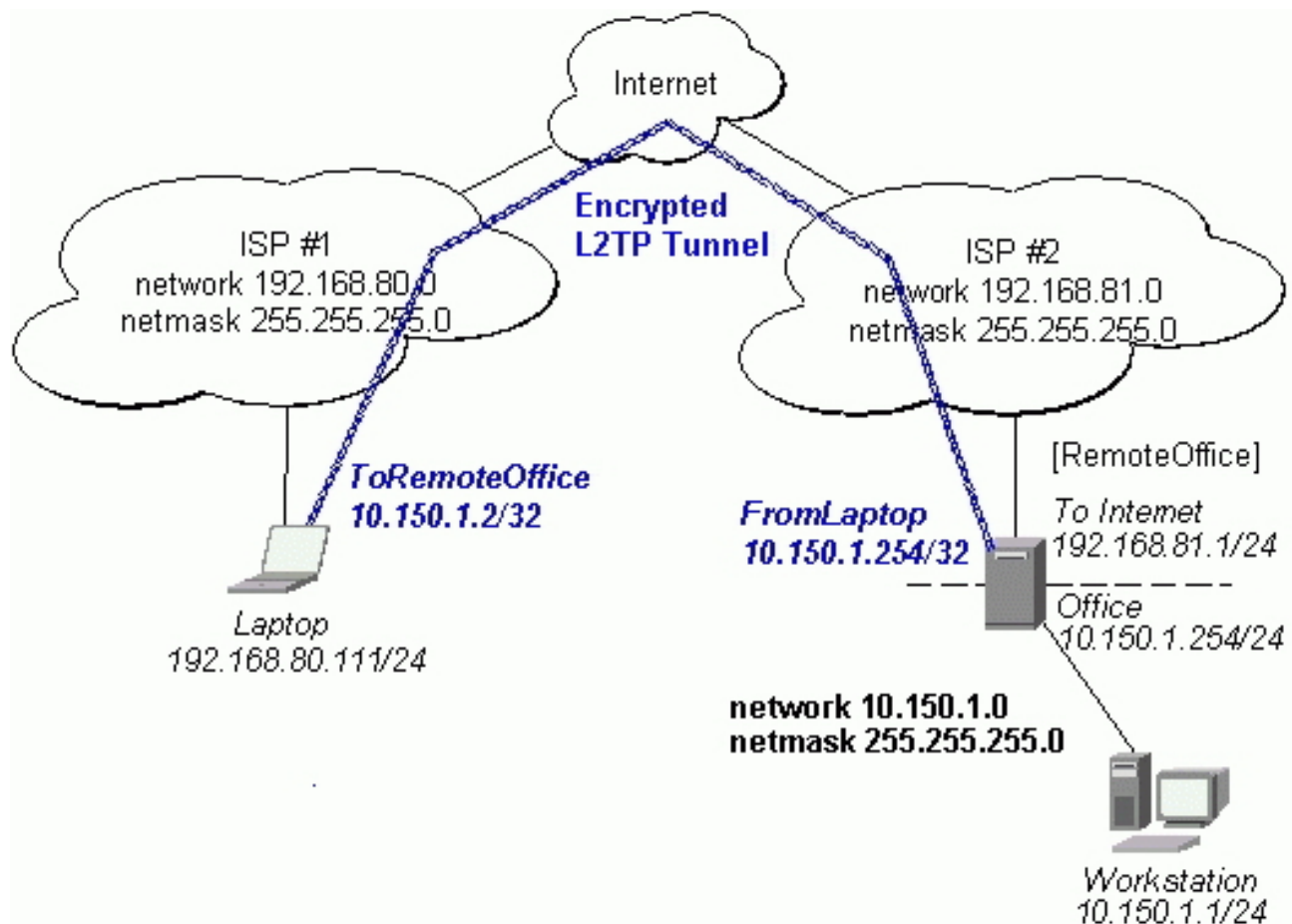
```
[admin@RemoteOffice]> /ping 10.150.2.254
10.150.2.254 pong: ttl=255 time=3 ms
10.150.2.254 pong: ttl=255 time=3 ms
10.150.2.254 pong: ttl=255 time=3 ms
ping interrupted
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 3/3.0/3 ms
```

To bridge a LAN over this secure tunnel, please see the example in the 'EoIP' section of the manual. To set the maximum speed for traffic over this tunnel, please consult the 'Queues' section.

Connecting a Remote Client via L2TP Tunnel

The following example shows how to connect a computer to a remote office network over L2TP encrypted tunnel giving that computer an IP address from the same network as the remote office has (without need of bridging over EoIP tunnels).

Please, consult the respective manual on how to set up a L2TP client with the software you are using.



The router in this example:

- [RemoteOffice]
Interface ToInternet 192.168.81.1/24
Interface Office 10.150.1.254/24

The client computer can access the router through the Internet.

On the L2TP server a user must be set up for the client:

```
[admin@RemoteOffice] ppp secret> add name=ex service=l2tp password=lkjrht
local-address=10.150.1.254 remote-address=10.150.1.2
[admin@RemoteOffice] ppp secret> print detail
Flags: X - disabled
 0 name="ex" service=l2tp caller-id="" password="lkjrht" profile=default
  local-address=10.150.1.254 remote-address=10.150.1.2 routes=""

[admin@RemoteOffice] ppp secret>
```

Then the user should be added in the L2TP server list:

```
[admin@RemoteOffice] interface l2tp-server> add name=FromLaptop user=ex
[admin@RemoteOffice] interface l2tp-server> print
Flags: X - disabled, D - dynamic, R - running
# NAME USER MTU CLIENT-ADDRESS UPTIME ENC...
0 FromLaptop ex
[admin@RemoteOffice] interface l2tp-server>
```

And the server must be enabled:

```
[admin@RemoteOffice] interface l2tp-server server> set enabled=yes
[admin@RemoteOffice] interface l2tp-server server> print
enabled: yes
mtu: 1460
mru: 1460
authentication: mschap2
default-profile: default
[admin@RemoteOffice] interface l2tp-server server>
```

Finally, the proxy ARP must be enabled on the 'Office' interface:

```
[admin@RemoteOffice] interface ethernet> set Office arp=proxy-arp
[admin@RemoteOffice] interface ethernet> print
Flags: X - disabled, R - running
# NAME MTU MAC-ADDRESS ARP
0 R ToInternet 1500 00:30:4F:0B:7B:C1 enabled
1 R Office 1500 00:30:4F:06:62:12 proxy-arp
[admin@RemoteOffice] interface ethernet>
```

L2TP Setup for Windows

Microsoft provides L2TP client support for Windows XP, 2000, NT4, ME and 98. Windows 2000 and XP include support in the Windows setup or automatically install L2TP. For 98, NT and ME, installation requires a download from Microsoft (L2TP/IPsec VPN Client).

For more information, see:

[Microsoft L2TP/IPsec VPN Client](#) [Microsoft L2TP/IPsec VPN Client](#)

On Windows 2000, L2TP setup without IPsec requires editing registry:

[Disabling IPsec for the Windows 2000 Client](#)

[Disabling IPSEC Policy Used with L2TP](#)

Troubleshooting

Description

- **I use firewall and I cannot establish L2TP connection**
Make sure UDP connections can pass through both directions between your sites.
- **My Windows L2TP/IPsec VPN Client fails to connect to L2TP server with "Error 789" or "Error 781"**
The error messages 789 and 781 occur when IPsec is not configured properly on both ends. See the respective documentation on how to configure IPsec in the Microsoft L2TP/IPsec VPN Client and in the MikroTik RouterOS. If you do not want to use IPsec, it can be easily switched off on the client side. Note: if you are using Windows 2000, you need to edit system registry using regedt32.exe or regedit.exe. Add the following registry value to **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rasman\Parameters:**

```
Value Name: ProhibitIpSec  
Data Type: REG_DWORD  
Value: 1
```

You must restart the Windows 2000 for the changes to take effect

For more information on configuring Windows 2000, see:

- [Configuring Cisco IOS and Windows 2000 Clients for L2TP Using Microsoft IAS](#)
- [Disabling IPSEC Policy Used with L2TP](#)
- [How to Configure a L2TP/IPsec Connection Using Pre-shared Key Authentication](#)