L2TP

Overview

Layer Two Tunneling Protocol "L2TP" extends the PPP model by allowing the L2 and PPP endpoints to reside on different devices interconnected by a packet-switched network. 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. 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 standard is defined in RFC 2661. The L2TPv3 support added in 7.1 version. Support IPv4, IPv6.

Introduction

It may 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 the 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.

Multilink PPP (MP) is supported in order to provide MRRU (the ability to transmit full-sized 1500 and larger packets) and bridging over PPP links (using Bridge Control Protocol (BCP) that allows sending raw Ethernet frames over PPP links). This way it is possible to setup bridging without EoIP. The bridge should either have an administratively set MAC address or an Ethernet-like interface in it, as PPP links do not have MAC addresses.

> ⚠ L2TP does not provide encryption mechanisms for tunneled traffic. IPsec can be used for additional security layers.

L2TP Client

Properties

Property	Description
add-default-route (*yes | no*; Default: **no**)	Whether to add L2TP remote address as a default route.
allow (*mschap2 | mschap1 | chap | pap*; Default: **mschap2, mschap1, chap, pap**)	Allowed authentication methods.

connect-to (*IP|IPv6*; Default:)	Remote address of L2TP server (if the address is in VRF table, VRF should be specified)
	`/interface l2tp-client`
	`add connect-to=192.168.88.1@vrf1 name=l2tp-out1 user=l2tp-client)`

comment (*string*; Default:)	Short description of the tunnel.
default-route-distance (*byte*; Default:)	Since v6.2, sets distance value applied to auto created default route, if add-default-route is also selected
dial-on-demand (*yes | no*; Default: **no**)	connects only when outbound traffic is generated. If selected, then route with gateway address from 10.112.112.0/24 network will be added while connection is not established.
disabled (*yes | no*; Default: **yes**)	Enables/disables tunnel.
keepalive-timeout (*integer [1..4294967295]*; Default: **60s**)	Since v6.0rc13, tunnel keepalive timeout in seconds.
max-mru (*integer*; Default: **1450**)	Maximum Receive Unit. Max packet size that L2TP interface will be able to receive without packet fragmentation.
max-mtu (*integer*; Default: **1450**)	Maximum Transmission Unit. Max packet size that L2TP interface will be able to send without packet fragmentation.

mrru (*disabled | integer*; Default: **disabled**)	Maximum packet size that can be received on the link. If a packet is bigger than tunnel MTU, it will be split into multiple packets, allowing full size IP or Ethernet packets to be sent over the tunnel.
name (*string*; Default:)	Descriptive name of the interface.
password (*string*; Default: **""**)	Password used for authentication.
profile (*name*; Default: **default-encryption**)	Specifies which PPP profile configuration will be used when establishing the tunnel.
user (*string*; Default:)	User name used for authentication.
use-ipsec (*yes | no*; Default: **no**)	When this option is enabled, dynamic IPSec peer configuration and policy is added to encapsulate L2TP connection into IPSec tunnel.
allow-fast-path (*yes | no*; Default:)	Allow to forward packets without additional processing in the Linux kernel.
l2tp-proto-version (l2tpv2 | *l2tpv3-ip | l2tpv3-udp | l2tpv*; Default: **l2tpv2**)	Specify protocol version.
l2tpv3-cookie-length (0 | *4-bytes | 8-bytes* ; Default: **0**)	Configures an L2TPv3 pseudowire static session cookie.
l2tpv3-digest-hash (*md5 | none | sha1* ; Default: **md5**)	Specifies which hash function to be used.
use-peer-dns (*yes | no | exclusively*; Default: **no**)	To use peer dns.
copy-from	To copy created peer.
src-address	Specify source address.
l2tpv3-circuit-id	Set the virtual circuit identifier to bind the one end of the L2TPv3 control channel.
ipsec-secret (*string*; Default:)	Preshared key used when use-ipsec is enabled.

L2TP Server

An interface is created for each tunnel established to the given server. There are two types of interfaces in the L2TP server's configuration

- Static interfaces are added administratively if there is a need to reference the particular interface name (in firewall rules or elsewhere) created for the particular user;
- Dynamic interfaces are added to this list automatically whenever a user is connected and its username does not match any existing static entry (or in case the entry is active already, as there can not be two separate tunnel interfaces referenced by the same name);

Dynamic interfaces appear when a user connects and disappear once the user disconnects, so it is impossible to reference the tunnel created for that use in router configuration (for example, in firewall), so if you need persistent rules for that user, create a static entry for him/her. Otherwise, it is safe to use a dynamic configuration.

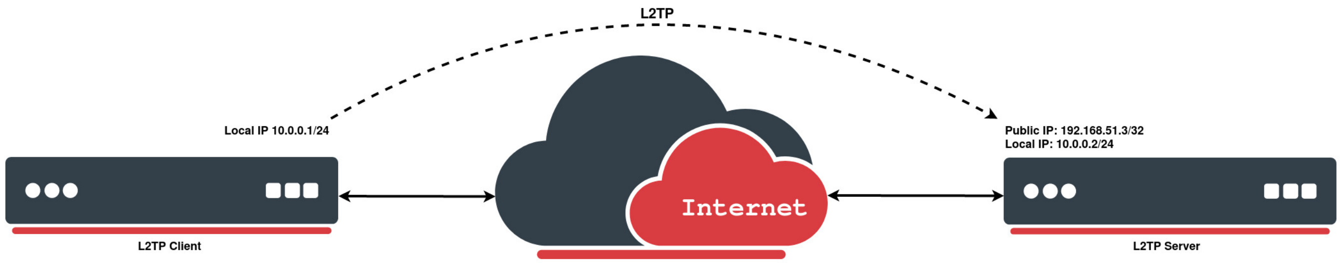
> ⚠ in both cases PPP users must be configured properly - static entries do not replace PPP configuration.

Properties

Property	Description
authentication (*pap | chap | mschap1 | mschap2*; Default: **mschap1,mschap2**)	Authentication methods that server will accept.
default-profile (*name*; Default: **default-encryption**)	default profile to use
enabled (*yes | no*; Default: **no**)	Defines whether L2TP server is enabled or not.

max-mru (*integer*; Default: **1 450**)	Maximum Receive Unit. Max packet size that L2TP interface will be able to receive without packet fragmentation.
keepalive-timeout (*integer*; Default: **30**)	If server during keepalive-timeout period does not receive any packets, it will send keepalive packets every second, five times. If the server still does not receive any response from the client, then the client will be disconnected after 5 seconds. Logs will show 5x "LCP missed echo reply" messages and then disconnect.
max-mtu (*integer*; Default: **1 450**)	Maximum Transmission Unit. Max packet size that L2TP interface will be able to send without packet fragmentation.
use-ipsec (*no | yes | require*; Default: **no**)	When this option is enabled, dynamic IPSec peer configuration is added to suite most of the L2TP road-warrior setups. When require is selected server will accept only those L2TP connection attempts that were encapsulated in the IPSec tunnel.
ipsec-secret (*string*; Default:)	Preshared key used when use-ipsec is enabled
accept-proto-version (all / l2tpv2 / l2tpv3; Default: **all**) cli-only	Specify protocol version.
accept-pseudowire-type (all / ether / ppp; Default: **all**)	Set the pseudowire signaling protocol for specific pseudowire type.
allow-fast-path (*no | yes*; Default: **no**)	To forward packets without additional processing in the Linux kernel.
caller-id-type (ip-address / number; Default: **ip-address**)	If same source IP address is used for multiple clients set id type to number.
max-sessions (unlimited / number; Default: **unlimited**)	Set number of needed sessions.
one-session-per-host (*no | yes* | ; Default: **no**)	To allow one session per host.
l2tpv3-circuit-id (Default:)	Set the virtual circuit identifier to bind the one end of the L2TPv3 control channel.
l2tpv3-cookie-length (0 / 4-bytes / 8-bytes; Default: **0**)	Configures an L2TP pseudowire static session cookie.
l2tpv3-digest-hash (md5 / none / sha1; Default: **md5**)	Specifies which hash function to be used.
l2tpv3-ether-interface-list (Default:)	Set your interface list for example the default ones- all, dynamic, none, static.
mrru (*disabled | integer*; Default: **disabled**)	Maximum packet size that can be received on the link. If a packet is bigger than tunnel MTU, it will be split into multiple packets, allowing full size IP or Ethernet packets to be sent over the tunnel.

Quick Example



L2TP Server

On the servers side we will enable L2TP-server and create a PPP profile for a particular user:

```
[admin@MikroTik] > /interface l2tp-server server set enabled=yes
[admin@MikroTik] > /ppp secret add local-address=10.0.0.2 name=MT-User password=StrongPass profile=default-
encryption remote-address=10.0.0.1 service=l2tp
```

L2TP Client

L2TP client setup in the RouterOS is very simple. In the following example, we already have a preconfigured 3 unit setup. We will take a look more detailed on how to set up L2TP client with username "MT-User", password "StrongPass" and server 192.168.51.3:

```
[admin@MikroTik] > /interface l2tp-client \
add connect-to=192.168.51.3 disabled=no name=MT-User password=StrongPass user=MT-User
[admin@MikroTik] > /interface l2tp-client print
Flags: X - disabled, R - running
0 R name="MT-User" max-mtu=1450 max-mru=1450 mrru=disabled connect-to=192.168.51.3 user="MT-User"
password="StrongPass" profile=default-encryption keepalive-timeout=60 use-ipsec=no ipsec-secret=""
allow-fast-path=no add-default-route=no dial-on-demand=no allow=pap,chap,mschap1,mschap2
```

L2TP Ether

Overview

Layer 2 Tunnel Protocol Version 3 (L2TPv3) is a draft from the Internet Engineering Task Force (IETF) working group. It introduces various improvements to the original L2TP, allowing the encapsulation of Layer 2 (L2) payloads within L2TP. More precisely, L2TPv3 outlines the protocol for tunnelling Layer 2 payloads across an IP core network using L2 virtual private networks (VPNs).

Properties

Property	Description
connect-to (*IP*; Default:)	Remote address of L2TP server.
comment (st*ring*; Default:)	Short description of the tunnel.
disabled (*yes* | *no*; Default: **yes**)	Enables/disables tunnel.
mac-address (string; Default: **auto**)	Set desired mac address of interface.
unmanaged-mode (*yes* | *no*; Default: **no**)	Set unmanaged mode active, the configuration for additional settings will be possible, such as: **peer-cookie, send-cookie, local-tunnel-id, local-session-id, remote-tunnel-id, remote-session-id, local-address.**
local-tunnel-id (string; Default: disabled)	Set value for local-tunnel-id, an integer required.
local-session-id (string; Default: disabled)	Set value for local-session-id, an integer required.
remote-tunnel-id (string; Default: **disabled)**	Set value for remote-tunnel-id, an integer required.
remote-session-id (string; Default: **disabled)**	Set value for remote-session-id, an integer required.
peer-cookie (string; Default: **disabled)**	Sets optional peer cookie. To enable cookie enter remote cookie value (8 or 16 character hex string value expected) to disable leave empty.
send-cookie (string; Default: **disabled)**	Sets optional cookie. To enable cookie enter remote cookie value (8 or 16 character hex string value expected) to disable leave empty.

mtu (*auto*; Default: **1420**)	Maximum Transmission Unit. Max packet size that L2TP interface will be able to send without packet fragmentation.
name (*string*; Default:)	Descriptive name of the interface.
local-address (*IP address*; Default:)	Set local address for **unmanaged** mode.
use-ipsec (*yes | no*; Default: **no**)	When this option is enabled, dynamic IPSec peer configuration and policy is added to encapsulate L2TP connection into IPSec tunnel.
allow-fast-path (*yes | no*; Default: **no**)	Allow to forward packets without additional processing in the Linux kernel.
l2tp-proto-version (*l2tpv3-ip | l2tpv3-udp |* ; Default: ***l2tpv3-udp***)	Specify protocol version.
cookie-length (0 | *4-bytes | 8-bytes* ; Default: **0**)	Configures an L2TPv3 pseudowire static session cookie.
digest-hash (*md5 | none | sha1* ; Default: **md5**)	Specifies which hash function to be used.
use-l2-specific-sublayer (*yes | no*; Default: **no**)	Specify source address.
circuit-id	Set the virtual circuit identifier to bind the one end of the L2TPv3 control channel, this works as identifier for each redundant pseudowire.
ipsec-secret (*string*; Default:)	Preshared key used when use-ipsec is enabled.