

L2TPv3 Tunnel Configuration on Donyx Routers

L2TPv3 (Layer 2 Tunneling Protocol version 3) is a tunneling protocol that encapsulates **Data Link Layer (L2)** traffic for transmission over **IP networks**.

Operating on a point-to-point basis, it supports two primary modes:

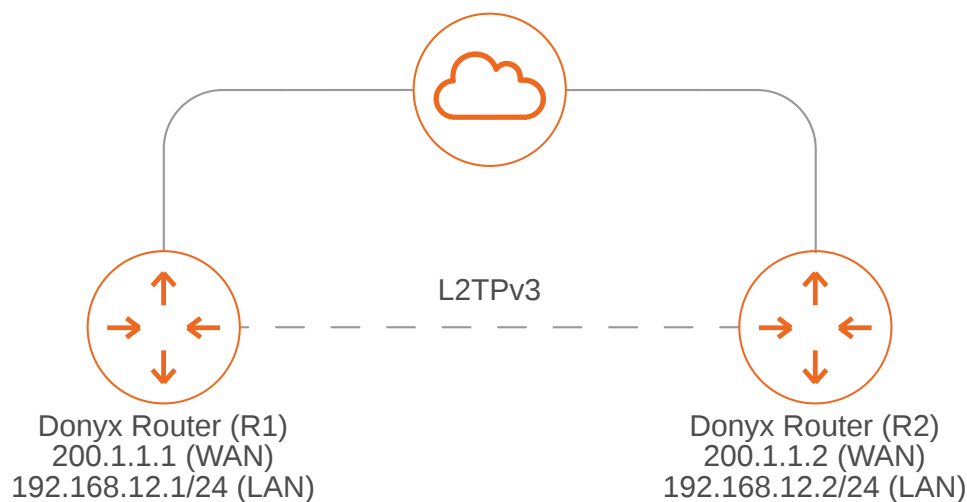
- **IP Protocol mode:** Operates directly as IP protocol number *115*. This mode is recommended when no **NAT** exists between the tunnel endpoints.
- **UDP mode:** Operates over the **UDP** protocol, enabling the tunnel to traverse **NAT** boundaries.

As with many other tunneling protocols, **L2TPv3** does not include built-in encryption. Consequently, it should be implemented within private networks or secured using additional encryption, such as **IPsec**.



L2-over-L3 tunneling should be utilized only when necessary, specifically in scenarios where requirements cannot be met through standard routing within **L3** tunnels.

Integration of equipment into a single L2 segment via an L2TPv3 tunnel:



In this example, both routers are assigned public IP addresses, over which the tunnel is established. The local networks on both routers reside within the same subnet. These networks are integrated into a single **L2** segment using the **L2TPv3** tunnel. To prevent IP address conflicts, the **DHCP** server must be disabled on the local network interfaces designated for integration.

To establish the tunnel, the following steps are performed in the `/tunnel/l2tpv3` section of the web interface or CLI:

1. Click the **Add** button.
2. Assign a name to the new tunnel.
3. Complete the configuration fields.

L2TPv3 Tunnel Configuration with UDP Encapsulation (without IPsec)

In this example, the tunnel interfaces are named *L2TPv3*, and the WAN interfaces are named *WAN*.

Configuration on Router R1

L2TPv3	
Disabled	<input type="checkbox"/>
Local IP	WAN
Remote IP	200.1.1.2
Tunnel IP	
Encryption	none
MAC	auto
MTU	1458
L2 Spec	default
Tunnel ID	1000
Peer Tunnel ID	2000
Session ID	3000
Peer Session ID	4000
Encapsulation	udp
Peer UDP Port	9001
UDP Port	9000

Table 1. Parameters for Router R1

Field	Value
Local IP	WAN (selected from the list).
Remote IP	200.1.1.2 (specified by the user).
L2 Spec	Default (selected from the list).
Tunnel ID	1000 (specified by the user).
Peer Tunnel ID	2000 (specified by the user).
Session ID	3000 (specified by the user).
Peer Session ID	4000 (specified by the user).
Encapsulation	UDP (selected from the list).
Peer UDP Port	9001 (specified by the user).
UDP Port	9000 (specified by the user).

CLI Configuration (without IPsec Encryption)

To configure the tunnel via the CLI, establish an SSH session using administrator credentials and execute the following commands:

```
/tunnel l2tp-v3 add name=L2TPv3
  disabled false
  encap udp
  encryption none
  local-ip WAN
  l2spec-type default
  macaddr auto
  mtu 1458
  peer-session-id 4000
  peer-tunnel-id 2000
  remote-ip 200.1.1.2
  session-id 3000
  tunnel-id 1000
  tunnel-ip -
  udp-dport 9001
  udp-sport 9000
  apply
```

Configuration on Router R2

L2TPv3

Disabled	<input type="checkbox"/>
Local IP	WAN
Remote IP	200.1.1.1
Tunnel IP	
Encryption	none
MAC	auto
MTU	1458
L2 Spec	default
Tunnel ID	2000
Peer Tunnel ID	1000
Session ID	4000
Peer Session ID	3000
Encapsulation	udp
Peer UDP Port	9000
UDP Port	9001

Table 2. Parameters for Router R2

Field	Value
Local IP	WAN (selected from the list).
Remote IP	200.1.1.1 (specified by the user).
L2 Spec	Default (selected from the list).
Tunnel ID	2000 (specified by the user).
Peer Tunnel ID	1000 (specified by the user).
Session ID	4000 (specified by the user).
Peer Session ID	3000 (specified by the user).
Encapsulation	UDP (selected from the list).
Peer UDP Port	9000 (specified by the user).
UDP Port	9001 (specified by the user).

CLI Configuration (without IPsec Encryption)

```
/tunnel l2tp-v3 add name=L2TPv3
  disabled false
  encap udp
  encryption none
  local-ip WAN
  l2spec-type default
  macaddr auto
  mtu 1458
  peer-session-id 3000
  peer-tunnel-id 1000
  remote-ip 200.1.1.1
  session-id 4000
  tunnel-id 2000
  tunnel-ip -
  udp-dport 9000
  udp-sport 9001
  apply
```

Tunnel statuses are displayed on the router's dashboard

L2TPv3	status	running
	type	l2tpv3
	uptime	00:43:06
	remote-ip	200.1.1.2
	local-ip	WAN
	rx-tx	1.11KB/1.25KB

Firewall Configuration

The firewall must be configured to permit incoming packets; this configuration is performed in the `/firewall/filter` section.

R1

Disabled	<input type="checkbox"/>
Chain	input
Source	zone-wan
Source Address	
Destination	
Destination Address	:9000
Protocol	udp
Firewall Mark	
Action	accept
IPSec Policy	
Extra Params	

The port number must match the **UDP Port** value previously specified in the tunnel configuration.

CLI Configuration

```
/firewall filter add chain=input
  action accept
  dst-addr :9000
  protocol udp
  src zone-wan
  reorder position=-1
  apply
/firewall filter status
```

R2

Disabled	<input type="checkbox"/>
Chain	input
Source	zone-wan
Source Address	
Destination	
Destination Address	:9001
Protocol	udp
Firewall Mark	
Action	accept
IPSec Policy	
Extra Params	

CLI Configuration

```
/firewall filter add chain=input
  action accept
  dst-addr :9001
  protocol udp
  src zone-wan
  reorder position=-1
  apply
/firewall filter status
```

L2TPv3 Tunnel Configuration with UDP Encapsulation (with IPsec)

Configuration on Router R1

L2TPv3

Disabled	<input type="checkbox"/>
Local IP	<input type="text" value="WAN"/>
Remote IP	<input type="text" value="200.1.1.2"/>
Tunnel IP	<input type="text"/>
Encryption	<input type="text" value="ipsec"/>
Pre-Shared Key	<input type="text" value="....."/>
MAC	<input type="text" value="auto"/>
MTU	<input type="text" value="1458"/>
L2 Spec	<input type="text" value="default"/>
Tunnel ID	<input type="text" value="1000"/>
Peer Tunnel ID	<input type="text" value="2000"/>
Session ID	<input type="text" value="3000"/>
Peer Session ID	<input type="text" value="4000"/>
Encapsulation	<input type="text" value="udp"/>
Peer UDP Port	<input type="text" value="9001"/>
UDP Port	<input type="text" value="9000"/>

Table 3. Parameters for Router R1

Field	Value
Local IP	WAN (selected from the list).
Remote IP	200.1.1.2 (specified by the user).
Encryption	ipsec
Pre-Shared Key	Password
L2 Spec	Default (selected from the list).
Tunnel ID	1000 (specified by the user).
Peer Tunnel ID	2000 (specified by the user).
Session ID	3000 (specified by the user).
Peer Session ID	4000 (specified by the user).
Encapsulation	UDP (selected from the list).
Peer UDP Port	9001 (specified by the user).
UDP Port	9000 (specified by the user).

CLI Configuration (with IPsec Encryption)

```

/tunnel l2tp-v3 add name=L2TPv3
  encap udp
  encryption ipsec
  local-ip bridge1
  l2spec-type default
  macaddr auto
  mtu 1458
  peer-session-id 4000
  peer-tunnel-id 2000
  psk password
  remote-ip 200.1.1.2
  session-id 3000
  tunnel-id 1000
  udp-dport 9001
  udp-sport 9000

/tunnel l2tp-v3 apply

```

Configuration on Router R2

L2TPv3






Disabled	<input type="checkbox"/>
Local IP	WAN 
Remote IP	200.1.1.1
Tunnel IP	
Encryption	ipsec 
Pre-Shared Key 
MAC	auto
MTU	1458
L2 Spec	default 
Tunnel ID	2000
Peer Tunnel ID	1000
Session ID	4000
Peer Session ID	1000
Encapsulation	udp 
Peer UDP Port	9000
UDP Port	9001

Table 4. Parameters for Router R1

Field	Value
Local IP	WAN (selected from the list).
Remote IP	200.1.1.1 (specified by the user).
Encryption	ipsec
Pre-Shared Key	Password
L2 Spec	Default (selected from the list).
Tunnel ID	2000 (specified by the user).
Peer Tunnel ID	1000 (specified by the user).
Session ID	4000 (specified by the user).
Peer Session ID	3000 (specified by the user).
Encapsulation	UDP (selected from the list).
Peer UDP Port	9000 (specified by the user).
UDP Port	9001 (specified by the user).

CLI Configuration (with IPsec Encryption)

```

/tunnel l2tp-v3 add name=L2TPv3
  encap udp
  encryption ipsec
  local-ip bridge1
  l2spec-type default
  macaddr auto
  mtu 1458
  peer-session-id 3000
  peer-tunnel-id 1000
  psk password
  remote-ip 200.1.1.1
  session-id 4000
  tunnel-id 2000
  udp-dport 9000
  udp-sport 9001
/tunnel l2tp-v3 apply

```



If the tunnel is configured with **IPsec** encryption, additional firewall configuration is **not required**.

Local Network Connectivity

To facilitate communication between local networks, the virtual tunnel interfaces must be added to the corresponding bridges.

The following procedure is performed in the *network/bridge* section:

1. Select the bridge interface responsible for the local network segment (e.g., *bridge0*).
2. Add the tunnel interface (e.g., *L2TPv3*) to the *Untagged* ports list.
3. Click **Apply**.

CLI Configuration

1. Use the */ip interface status* command to display the list of existing bridges and their parameters.
2. Identify the bridge interface assigned the required IP address and subnet (e.g., *192.168.12.1/24*). In this example, the target is *bridge0*.

```
/ip interface status
```

3. Navigate to the bridge configuration section */network bridge bridge0*
4. View the current ports within the bridge using the *port* command.
5. Add the tunnel interface to the port list. To maintain existing connectivity, the tunnel interface is added to the current list (e.g., *port port1,L2TPv3*, where *L2TPv3* is the name assigned to the tunnel).
6. Execute the *apply* command to confirm the bridge settings.

```
/network bridge bridge0 port L2TPv3
apply
```

An identical configuration procedure must be performed on the second router.



By default, tunnel interfaces are not filtered by the firewall. If filtering is required, it must be configured in the */firewall/filter* section.

Ping (/tools/ping) — R2 from R1

Tunnel operation can be verified by sending a ping from the local address of router R1 to the address of the remote router R2.

```
⏪ Again  ✕ Stop  ✕ Close

PING 192.168.12.2 (192.168.12.2) 56(84) bytes of data.
64 bytes from 192.168.12.2: icmp_req=1 ttl=64 time=1.12 ms
64 bytes from 192.168.12.2: icmp_req=2 ttl=64 time=0.787 ms
64 bytes from 192.168.12.2: icmp_req=3 ttl=64 time=0.824 ms
64 bytes from 192.168.12.2: icmp_req=4 ttl=64 time=0.794 ms
64 bytes from 192.168.12.2: icmp_req=5 ttl=64 time=0.737 ms
64 bytes from 192.168.12.2: icmp_req=6 ttl=64 time=0.674 ms
64 bytes from 192.168.12.2: icmp_req=7 ttl=64 time=0.680 ms
64 bytes from 192.168.12.2: icmp_req=8 ttl=64 time=0.831 ms
64 bytes from 192.168.12.2: icmp_req=9 ttl=64 time=0.674 ms
64 bytes from 192.168.12.2: icmp_req=10 ttl=64 time=0.688 ms
--- 192.168.12.2 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 13ms
rtt min/avg/max/mdev = 0.674/0.780/1.120/0.133 ms, ipg/ewma 1.468/0.848 ms
Finished
```

Tcpdump (/tools/sniffer) — R2

Use the sniffer to capture and analyze traffic passing through the interface.

```

▶ Again ✕ Stop ✕ Close
19:45:07.550193 IP (tos 0x0, ttl 64, id 48915, offset 0, flags [none], proto ICMP (1), length 84)
    192.168.12.2 > 192.168.12.1: ICMP echo reply, id 1719, seq 5, length 64
19:45:07.551388 IP (tos 0x0, ttl 64, id 49140, offset 0, flags [DF], proto ICMP (1), length 84)
    192.168.12.1 > 192.168.12.2: ICMP echo request, id 1719, seq 6, length 64
19:45:07.551547 IP (tos 0x0, ttl 64, id 48916, offset 0, flags [none], proto ICMP (1), length 84)
    192.168.12.2 > 192.168.12.1: ICMP echo reply, id 1719, seq 6, length 64
19:45:07.552896 IP (tos 0x0, ttl 64, id 49141, offset 0, flags [DF], proto ICMP (1), length 84)
    192.168.12.1 > 192.168.12.2: ICMP echo request, id 1719, seq 7, length 64
19:45:07.553054 IP (tos 0x0, ttl 64, id 48917, offset 0, flags [none], proto ICMP (1), length 84)
    192.168.12.2 > 192.168.12.1: ICMP echo reply, id 1719, seq 7, length 64
19:45:07.554334 IP (tos 0x0, ttl 64, id 49142, offset 0, flags [DF], proto ICMP (1), length 84)
    192.168.12.1 > 192.168.12.2: ICMP echo request, id 1719, seq 8, length 64
19:45:07.554526 IP (tos 0x0, ttl 64, id 48918, offset 0, flags [none], proto ICMP (1), length 84)
    192.168.12.2 > 192.168.12.1: ICMP echo reply, id 1719, seq 8, length 64
19:45:07.555737 IP (tos 0x0, ttl 64, id 49143, offset 0, flags [DF], proto ICMP (1), length 84)
    192.168.12.1 > 192.168.12.2: ICMP echo request, id 1719, seq 9, length 64
19:45:07.555895 IP (tos 0x0, ttl 64, id 48919, offset 0, flags [none], proto ICMP (1), length 84)
    192.168.12.2 > 192.168.12.1: ICMP echo reply, id 1719, seq 9, length 64

```

The successful exchange of **ICMP** packets indicates that the configuration is complete.

L2TPv3 Tunnel Configuration with IP Encapsulation

Configuration using **IP encapsulation** is performed in a similar manner.



All modifications are permanently saved to the router configuration only after executing the `/system config commit` command or clicking the **commit** button in the web interface.