PPTP
PPTP as Client VPN

Internet

PPTP Tunnel

Office
Public: 192.168.80.1/24
Local: 10.1.101.1/24

Workstation 1
10.1.101.2/24

Workstation 2
10.1.101.3/24

Workstation 3
10.1.101.4/24

10.1.101.100/32
10.1.101.32

Laptop: 10.1.101.100/32
PPTP as Site to Site VPN
Point to Point Tunneling Protocol

- PPTP specification was published in July 1999 as RFC 2637.
- PPTP has not been proposed nor ratified as a standard by the Internet Engineering Task Force.
- PPTP uses a control channel over TCP and a GRE tunnel to encapsulate PPP packets.
  - A PPTP tunnel is initiated by communication to the peer on TCP port 1723.
  - This TCP connection is then used to initiate and manage a second GRE tunnel to the same peer.
  - PPTP uses IP protocol number 47 with non GRE standard packets
  - The GRE tunnel is used to carry encapsulated PPP packets.
PPTP & MikroTik

- PPTP can be bridged using the BCP (Bridging Control Protocol)
  - Bridging of PPTP tunnels only works between ROS devices
- ROS supports MLPPP over PPTP
- You must use the PPTP Firewall Service Port (NAT Helpers) to connect to/from your private LAN
- ROS will always choose the highest security option when multiple authentication methods are selected
PPTP & Microsoft Windows

- PPTP was the first VPN protocol that was supported by Microsoft Dial-up Networking.

- All releases of Microsoft Windows since Windows 95 OSR2 are bundled with a PPTP client, although they are limited to only 2 concurrent outbound connections.

- The Microsoft implementation uses single DES in the MS-CHAP authentication protocol.

- Windows Vista and later support the use of PEAP (Protected EAP) with PPTP.

- Windows Vista removed support for using the MSCHAP-v1 protocol to authenticate remote access connections.
The authentication methods that will work between current Windows OSs and MikroTik are:

- PAP (Unencrypted Passwords)
- CHAP (Challenge Handshake Authentication Protocol)
- MSCHAPv2 (Microsoft CHAP)

Proxy-ARP has to be enabled on the router (LAN interface/never the WAN interface)
PPTP Server Setup
PPTP Server Settings

- Enabled or Disabled
- Max Maximum Transmission Unit
- Max Receive Unit
- Max Received Reconstructed Unit
- How long to wait before sending packets to the client to confirm they are still connected
PPTP Server Settings

- Profile to be used
- Authentication Method

Options Include:
- Enabled
- Max MTU: 1450
- Max MRU: 1450
- MRRU:
- Keepalive Timeout: 30
- Default Profile: default-encryption
- Authentication: mschap2, mschap1, chap, pap
PPTP Client
Creating a New PPTP Client
PPTP Client Settings

- Administrative Name
- Tunnel Type
- Layer 2 Max Transmission Unit
- Max Packet size the client can send without fragmentation
- Max Receive Unit – Max the client can receive without fragmentation
- Multilink Maximum Received Reconstructed Unit – Used with MLPPP
PPTP Client Settings

- IP address of server
- Username
- Password
- Profile to be used
- How long to keep the connection alive before timing out
- When selected, the tunnel will only establish when traffic is generated – Do not use
- Whether to add a default route (all traffic goes through tunnel) & distance
- Authentication Methods Allowed

![PPTP Client Settings interface](image)
PPTP Client Settings

- Status Tab provides connection info

<table>
<thead>
<tr>
<th>General</th>
<th>Dial Out</th>
<th>Status</th>
<th>Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Link Down Time:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Last Link Up Time:</td>
<td>Jun/02/2015 11:24:12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Link Downs:</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Uptime:</td>
<td>0:00:14</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encoding:</td>
<td>MPPE128 stateless</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MTU:</td>
<td>1450</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MRU:</td>
<td>1450</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Local Address:</td>
<td>192.168.50.255</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote Address:</td>
<td>192.168.50.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>enabled</td>
<td>running</td>
<td>slave</td>
<td>Status: connected</td>
</tr>
</tbody>
</table>
PPTP Client Settings

- Traffic Tab provides details on the traffic going through the tunnel.
PPTP LAB

1) Pair up with another student and decide who will be the server and who will be the client

2) Connect an Ethernet cable between you and assign the interfaces a /30 address (Remember to remove the interfaces from any bridges or switch groups)

3) Connect your PPTP tunnel and verify that you can ping both sides of the tunnel IP address

4) Switch roles and create a new tunnel.
PPTP With RADIUS

![Diagram of PPTP with RADIUS configuration in WinBox software. The configuration panel is highlighted, showing options for PPP and PPPoE settings.](image-url)
RADIUS Settings
Which service is going to talk to the RADIUS server

Caller ID (Not usually required) - PPPoE - service name, PPTP - server's IP address, L2TP - server's IP address.

Windows Domain (Not usually required)
RADIUS Settings

- Address of RADIUS Server (Use 127.0.0.1 when Usermanager is running on the same router)
- Shared secret with RADIUS server
- Standard RADIUS ports
- How long to wait for a reply before it times out. Set to seconds, not milliseconds
RADIUS Settings

- Whether or not this configuration is for a backup RADIUS server
- Realm – also known as user domain. Used by some ISP’s RADIUS servers
- Source address of packets to be sent to the RADIUS server. (Not usually used)
RADIUS Settings

- The Status Tab is where you can see if the service to be used is sending info to the RADIUS server and whether or not the RADIUS server is replying to those requests.
Usermanager

Default Login is admin
No password
The RADIUS server has to know which routers (NAS Nodes) it's talking to.
Userman Settings – Step 2

Create a New Profile that is going to be applied to the user
Userman Settings – Step 2 (Cont)

Set the Validity
Set the Start to “Now”
Then Save the Profile
Userman Settings – Step 3

- Set the Userman & Password
- Then Save the User

- Notice that the Actual profile does not show up at first
Userman Settings – Step 4

Log out and then log back in
Verify the user has the correct profile
PPTP Client Settings

- Delete any secrets from the router and restart the PPTP Client
- When the client has reconnected, verify that there is an “R” flag for RADIUS
PPTP & RADIUS Lab

1) With the same partner from the previous lab, recreate your tunnels using RADIUS. Make sure your local databases are clear of any secrets.

2) Switch roles and verify that both of you are able to create the tunnel client and set up the server/ RADIUS
Adding Dynamic Queues

- Dynamically created queues can be added by utilizing the Limitations feature in the Usermanager Profile.
Adding Dynamic Queues

Remember to add the limit and save the profile
Adding Dynamic Queues

A new limitation set by RADIUS requires that the client has to reconnect before the queue will be created.
Dynamic Queue Lab

- Set a new limitation of 1 Meg up and 1 Med down and test with the bandwidth test tool. Remember to test to IP address of the tunnel and not the IP address of the router.

- Swap roles and test the other direction.
L2TP as Client VPN
L2TP as Site to Site VPN
L2TP

- Published in 1999 as proposed standard RFC 2661.
- A new version of this protocol, L2TPv3, appeared as proposed standard RFC 3931 in 2005. MikroTik implements most of this standard. (L2TPv3 adds security.)
- UDP port 1701 is used only for link establishment, tunnel traffic will use any available UDP port (which may or may not be 1701)
  - This allows L2TP tunnels to traverse most firewalls
- L2TP can be used by some versionso Microsoft Windows, but is difficult to setup without IPSEC. Other tunnels are recommends for this application.
L2TP in MikroTik

- Functionally, an L2TP is identically to the PPTP tunnel; exact same setup
- L2TP tunnels can be encrypted when both the server and client are MikroTik routers.
  - There can be limited connectivity with other OSs, but the results may be unpredictable.
L2TP Lab

- Repeats the step of the PPTP lab with a L2TP connection.
- Leave the PPTP tunnel functional.
- Take turns with your partner creating a L2TP client and connecting to the server through RADIUS.

- Hint: You are going to have to modify the User in Usermanager for both tunnels to become active.
L2TP Lab

This is what it will look like when you are done.
Starting with ROS 6.16 there is a “1 button L2TP/IPSEC” server setup

This preconfigures the L2TP server and IPSEC to used a “Road Warrior” configuration that is compatible with most vendors

Will work with RADIUS
L2TP & IPSEC
L2TP & IPSEC LAB

- Take turns with your partner creating a L2TP/IPSEC client and connecting to the server through RADIUS.
  - Observe the L2TP interface and status
  - Observe the IPSEC settings that are dynamically created
## Tunnel Comparaison

<table>
<thead>
<tr>
<th>Tunnel</th>
<th>Introduced</th>
<th>Layer</th>
<th>Port</th>
<th>Port can be changed</th>
<th>Default MTU</th>
<th>Authentication Protocols</th>
<th>Encryption Protocols</th>
<th>Encryption Level</th>
<th>Clients can call home</th>
<th>Bridging or BCP Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>GRE</td>
<td>Oct 1994</td>
<td>3</td>
<td>N/A</td>
<td>No</td>
<td>1476</td>
<td>N/A</td>
<td>N/A</td>
<td>None</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>IPIP</td>
<td>Oct 1996</td>
<td>3</td>
<td>N/A</td>
<td>No</td>
<td>1500</td>
<td>N/A</td>
<td>N/A</td>
<td>None</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>VLAN</td>
<td>1998</td>
<td>2</td>
<td>N/A</td>
<td>No</td>
<td>1500</td>
<td>N/A</td>
<td>N/A</td>
<td>None</td>
<td>N/A</td>
<td>Yes</td>
</tr>
<tr>
<td>IPSEC</td>
<td>Nov 1998</td>
<td>3</td>
<td>UDP500</td>
<td>Yes</td>
<td>N/A</td>
<td>None, MD5, SHA1, SHA256, SHA512</td>
<td>None, DES, 3DES, AES, Blowfish, Twofish, Camellia</td>
<td>None, 64bits, 128bit, 192bit, 256bit</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>PPNsE</td>
<td>Feb 1999</td>
<td>2</td>
<td>N/A</td>
<td>N/A</td>
<td>1480</td>
<td>PAP, CHAP, MSCHAP v1, MSCHAP v2</td>
<td>None or 40bit or 128bit</td>
<td>N/A</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>PPPvU</td>
<td>July 1999</td>
<td>3</td>
<td>TCP1723</td>
<td>No</td>
<td>1450</td>
<td>PAP, CHAP, MSCHAP v1, MSCHAP v2</td>
<td>None or 40bit or 128bit</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>L2TP</td>
<td>Aug 1999</td>
<td>3</td>
<td>UDP1701</td>
<td>No</td>
<td>1450</td>
<td>PAP, CHAP, MSCHAP v1, MSCHAP v2</td>
<td>None or 40bit or 128bit</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>OVPN</td>
<td>May 2001</td>
<td>3</td>
<td>TCP1194</td>
<td>Yes</td>
<td>1500</td>
<td>None, MD5, SHA1, SHA256, SHA512</td>
<td>None, Blowfish 128, AES 128, AES 192, AES 256</td>
<td>None, 128bit, 192bit, or 256bit</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>EOIP</td>
<td>Sept 2002</td>
<td>3</td>
<td>N/A</td>
<td>No</td>
<td>1500</td>
<td>N/A</td>
<td>N/A</td>
<td>None</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>SSTP</td>
<td>Jan 2007</td>
<td>3</td>
<td>TCP443</td>
<td>Yes</td>
<td>1500</td>
<td>PAP, CHAP, MSCHAP v1, MSCHAP v2, TLS 1.0</td>
<td>None or 40bit or 128bit, 256bit</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>
# Tunnel Comparaison of Loss

<table>
<thead>
<tr>
<th>Tunnel</th>
<th>Initial Bandwidth</th>
<th>With Tunnel</th>
<th>% of Loss</th>
</tr>
</thead>
<tbody>
<tr>
<td>GRE</td>
<td>691M RX</td>
<td>195M RX</td>
<td>71.80%</td>
</tr>
<tr>
<td>IPIP</td>
<td>691M RX</td>
<td>204M RX</td>
<td>70.50%</td>
</tr>
<tr>
<td>VLAN</td>
<td>691M RX</td>
<td>582M RX</td>
<td>15.80%</td>
</tr>
<tr>
<td>IPSEC</td>
<td>691M RX</td>
<td>667M RX</td>
<td>3.50%</td>
</tr>
<tr>
<td>PPPoE</td>
<td>691M RX</td>
<td>94M RX</td>
<td>86.40%</td>
</tr>
<tr>
<td>PpP</td>
<td>691M RX</td>
<td>61M RX</td>
<td>91.20%</td>
</tr>
<tr>
<td>L2TP</td>
<td>691M RX</td>
<td>59M RX</td>
<td>91.50%</td>
</tr>
<tr>
<td>OVPN</td>
<td>691M RX</td>
<td>29M RX</td>
<td>95.90%</td>
</tr>
<tr>
<td>EOIP</td>
<td>691M RX</td>
<td>190M RX</td>
<td>72.50%</td>
</tr>
<tr>
<td>SSTP</td>
<td>691M RX</td>
<td>29M RX</td>
<td>95.80%</td>
</tr>
</tbody>
</table>
End of Module