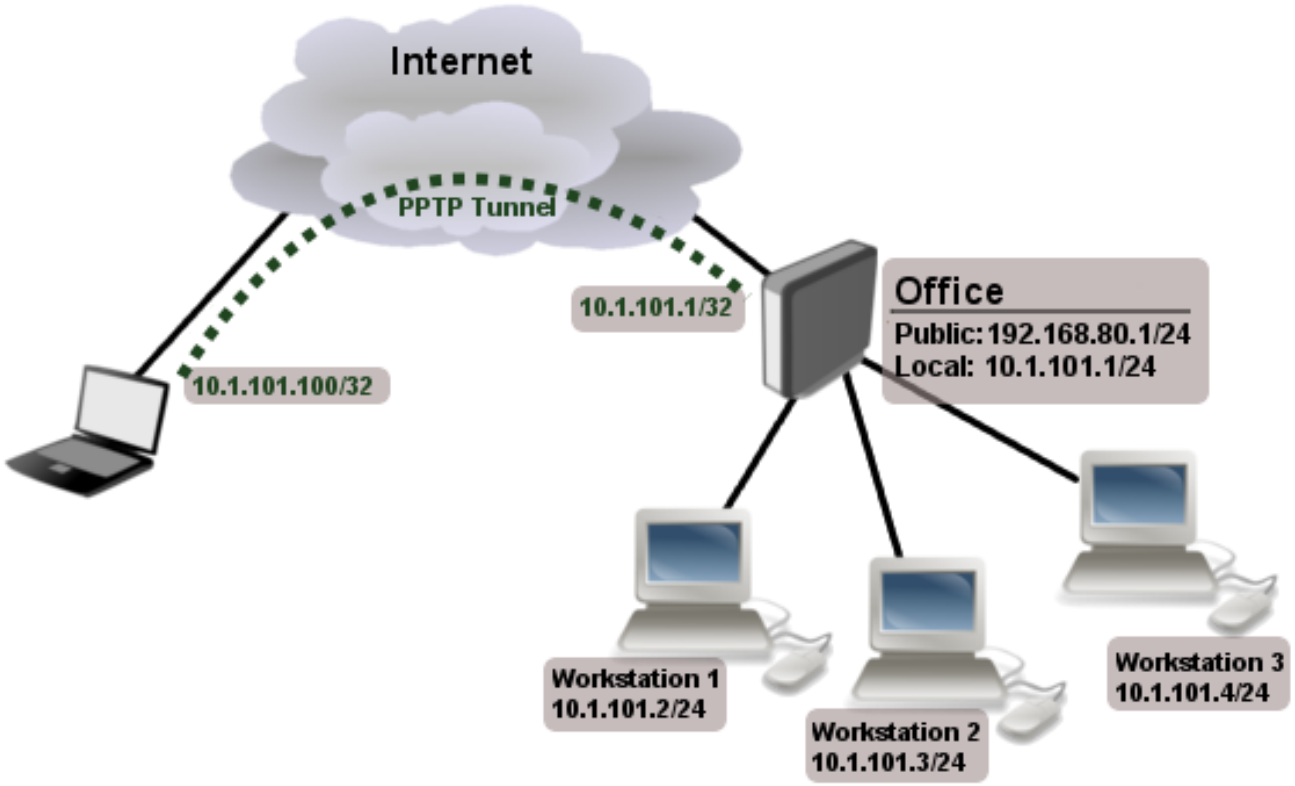
Rick Frey Consulting
www.rickfreyconsulting.com

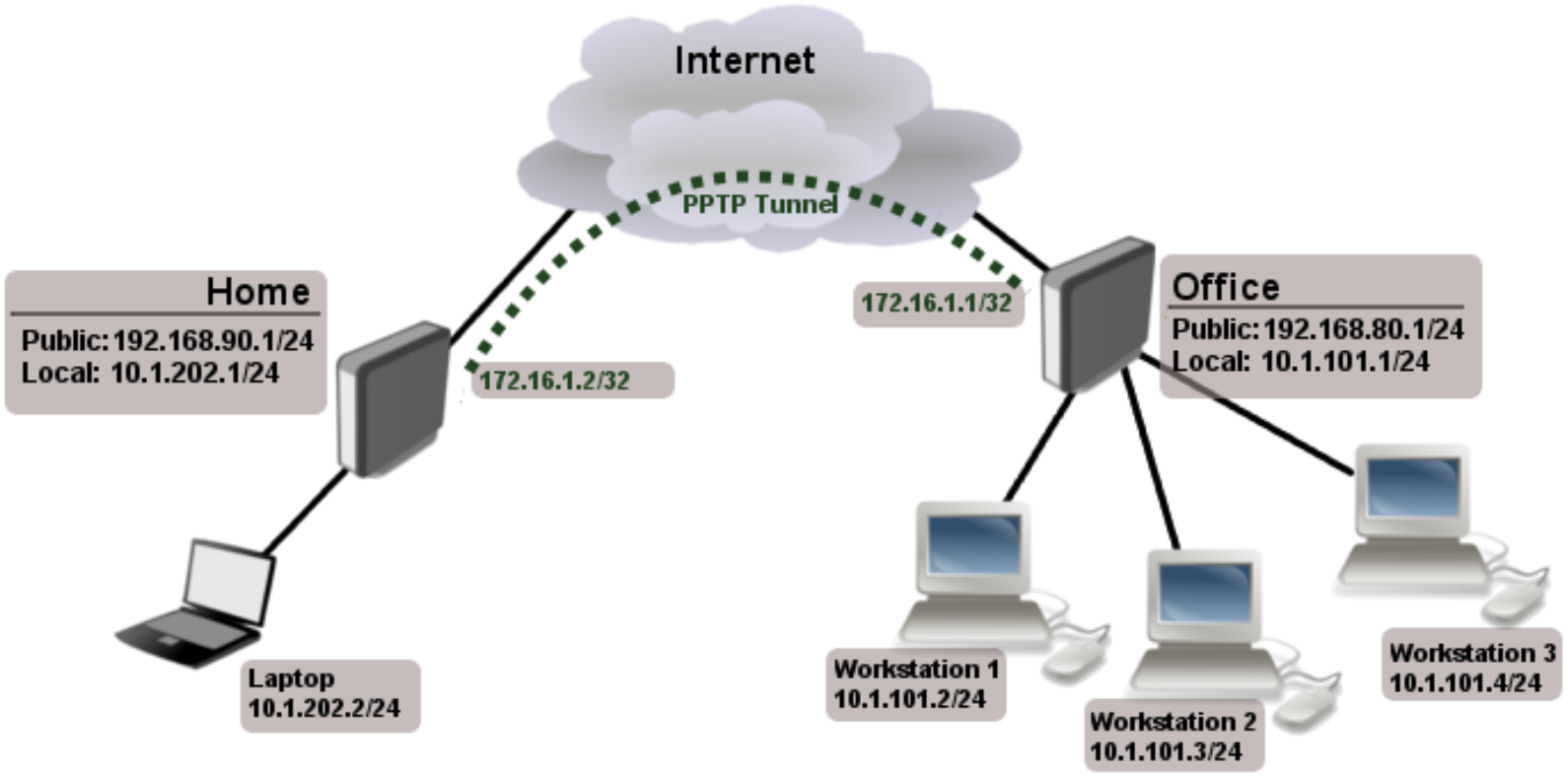
PPTP & L2TP

PPTP

PPTP as Client VPN



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

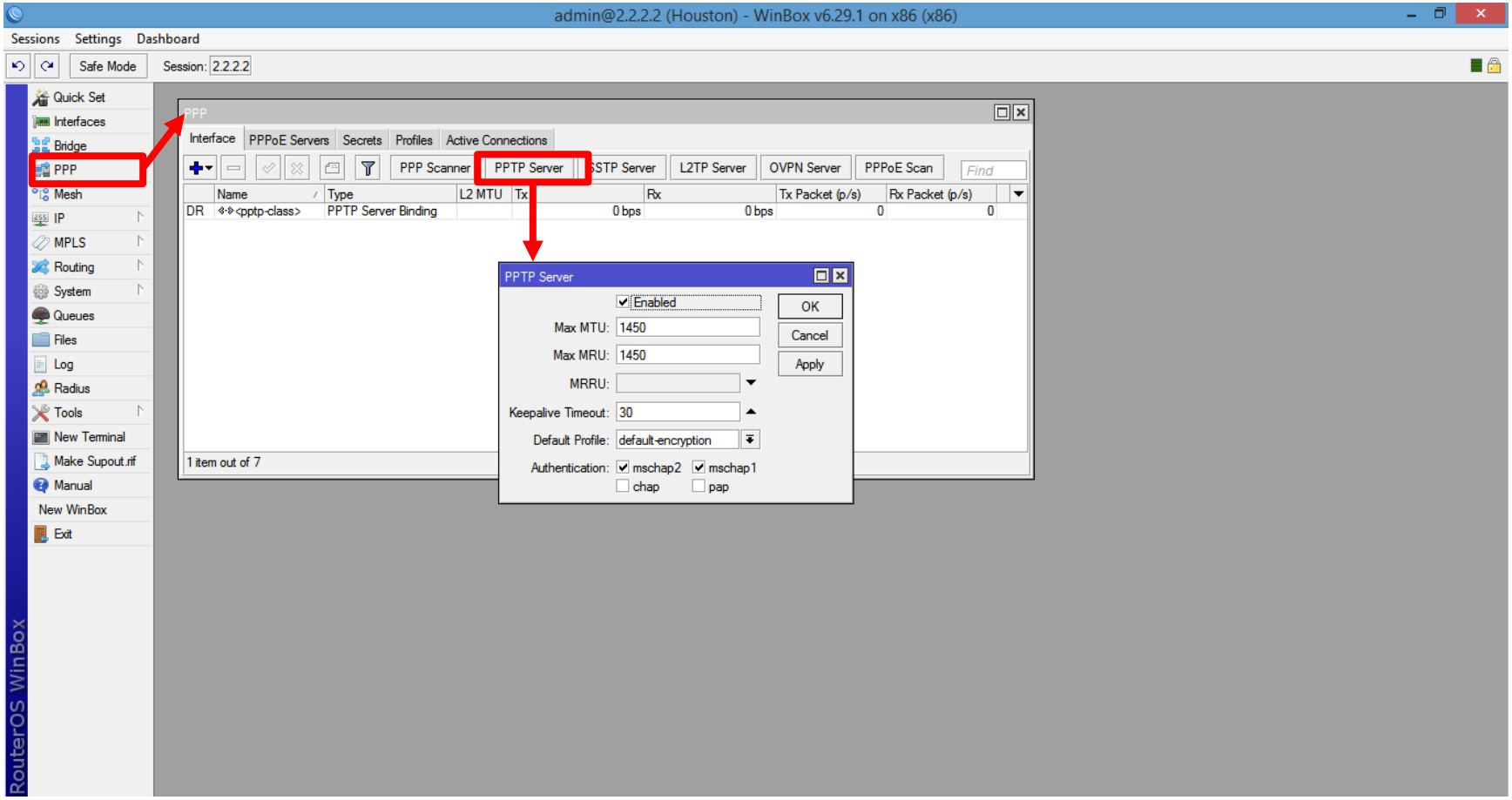
PPTP & Microsoft Windows

- 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.

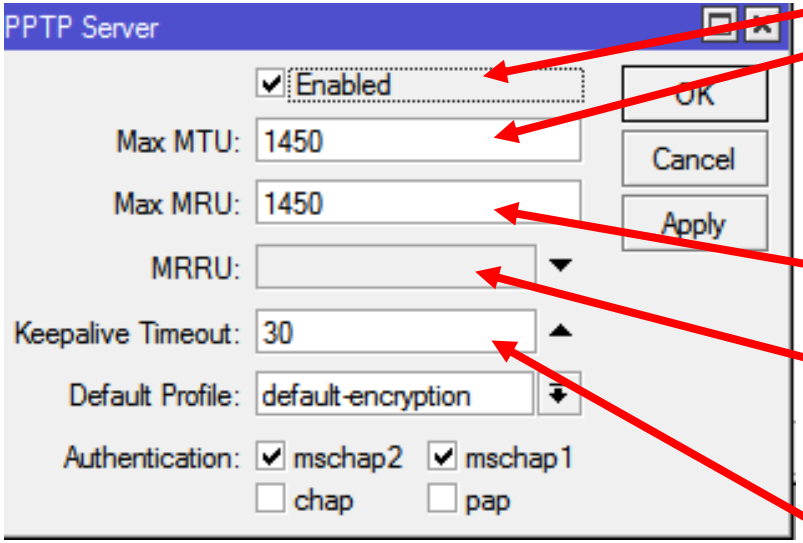
PPTP & Microsoft Windows

- 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

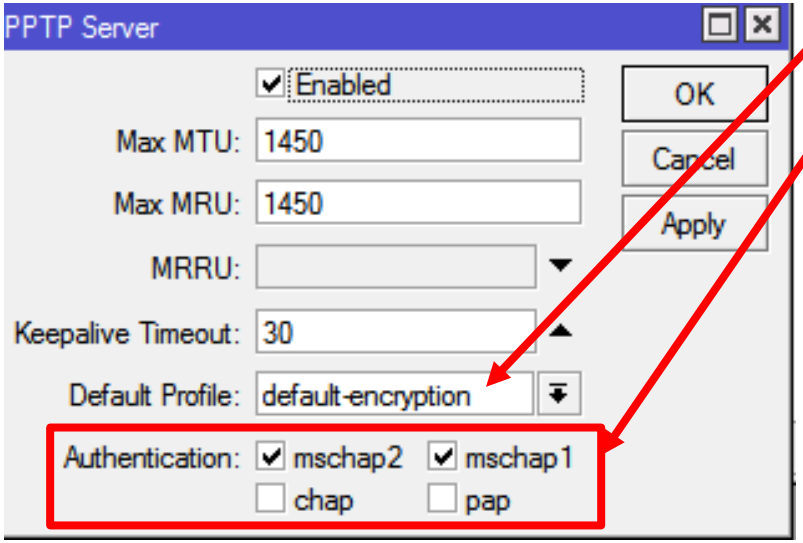


PPTP Server Settings



- 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

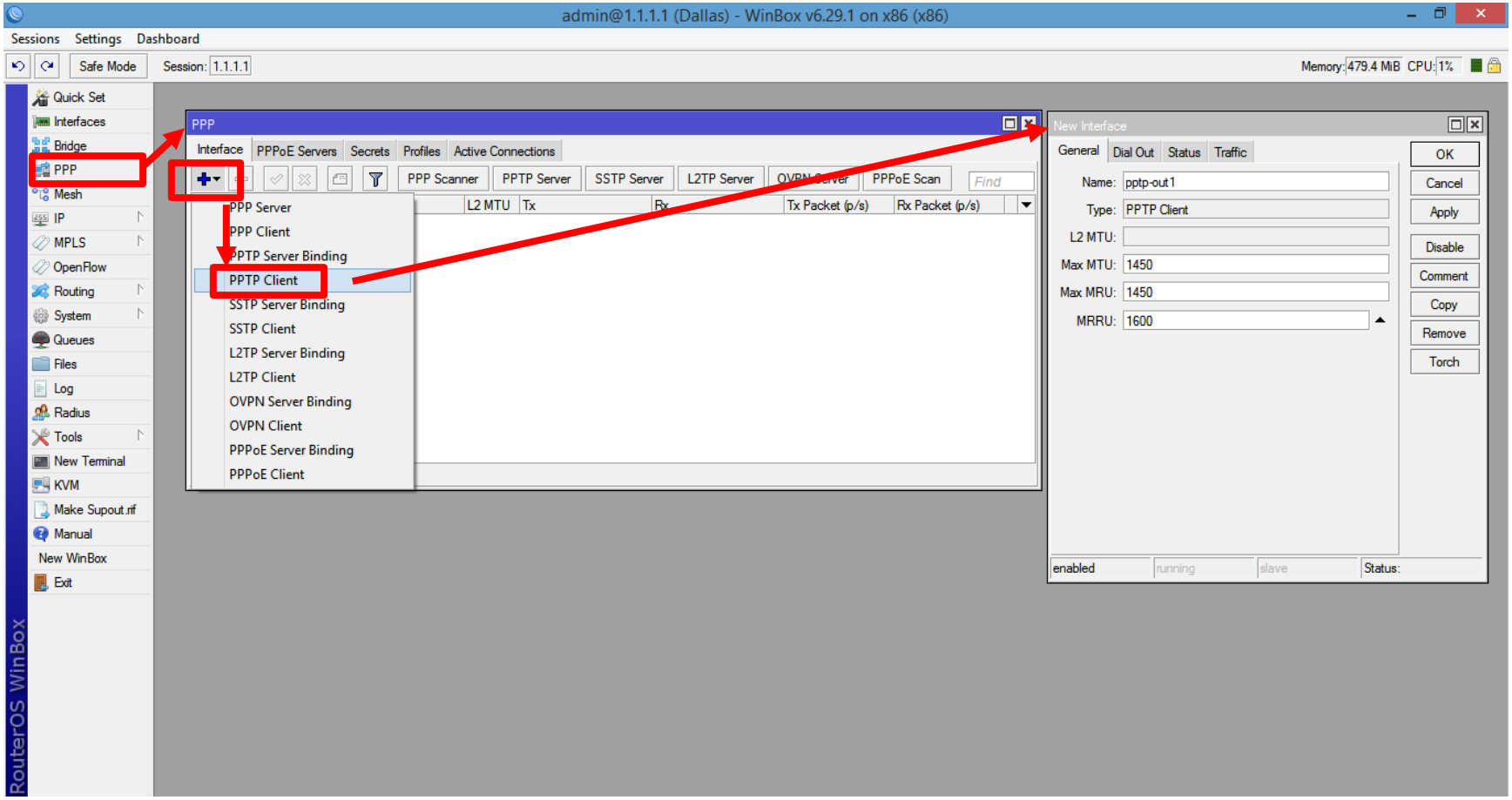
PPTP Server Settings



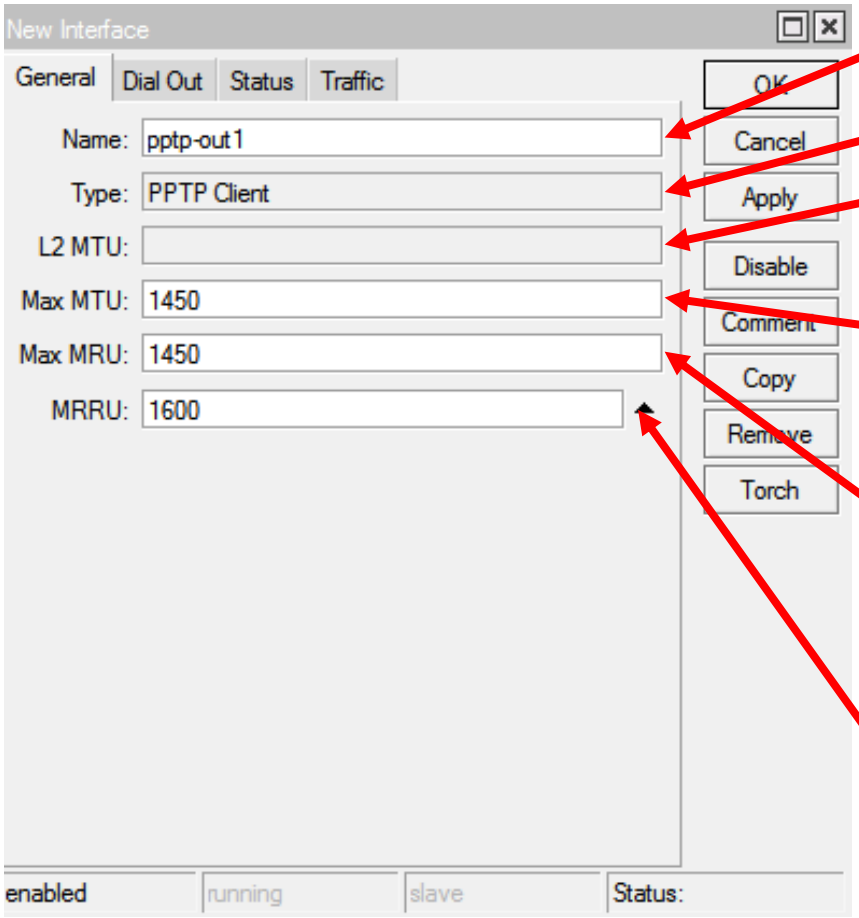
- Profile to be used
- Authentication Method

PPTP Client

Creating a New PPTP Client

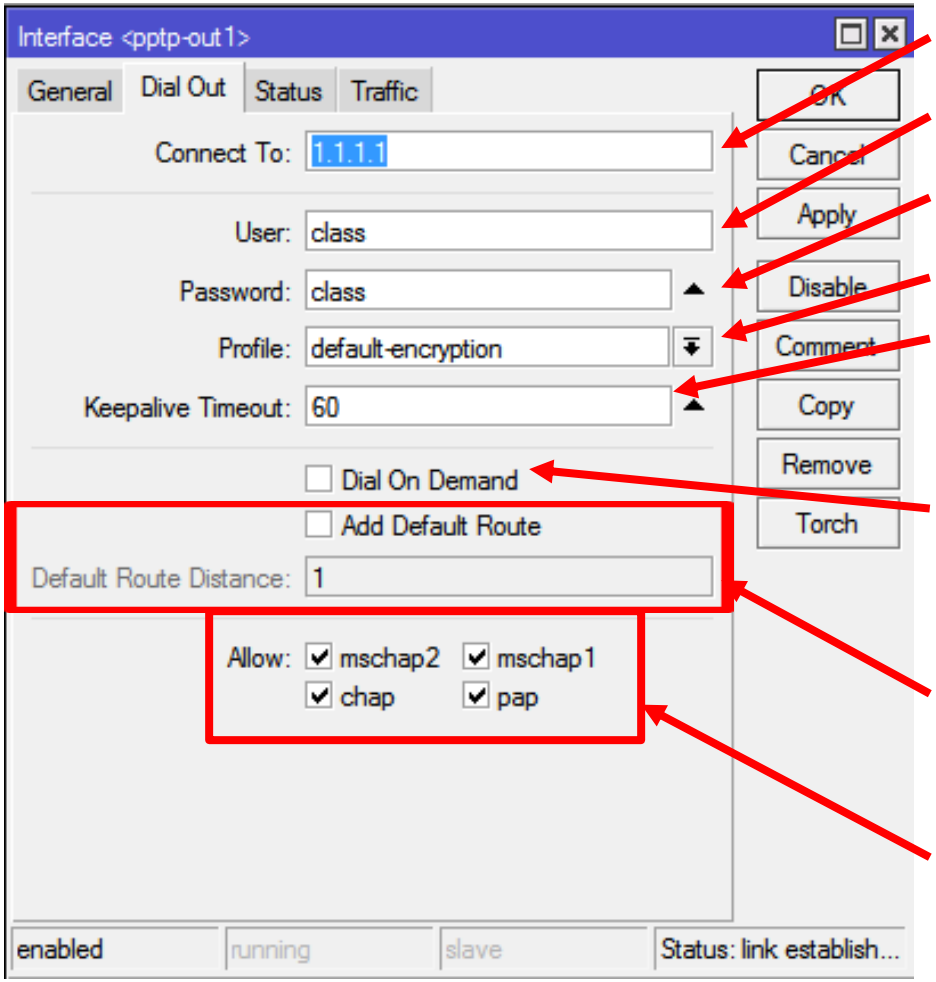


PPTP Client Settings



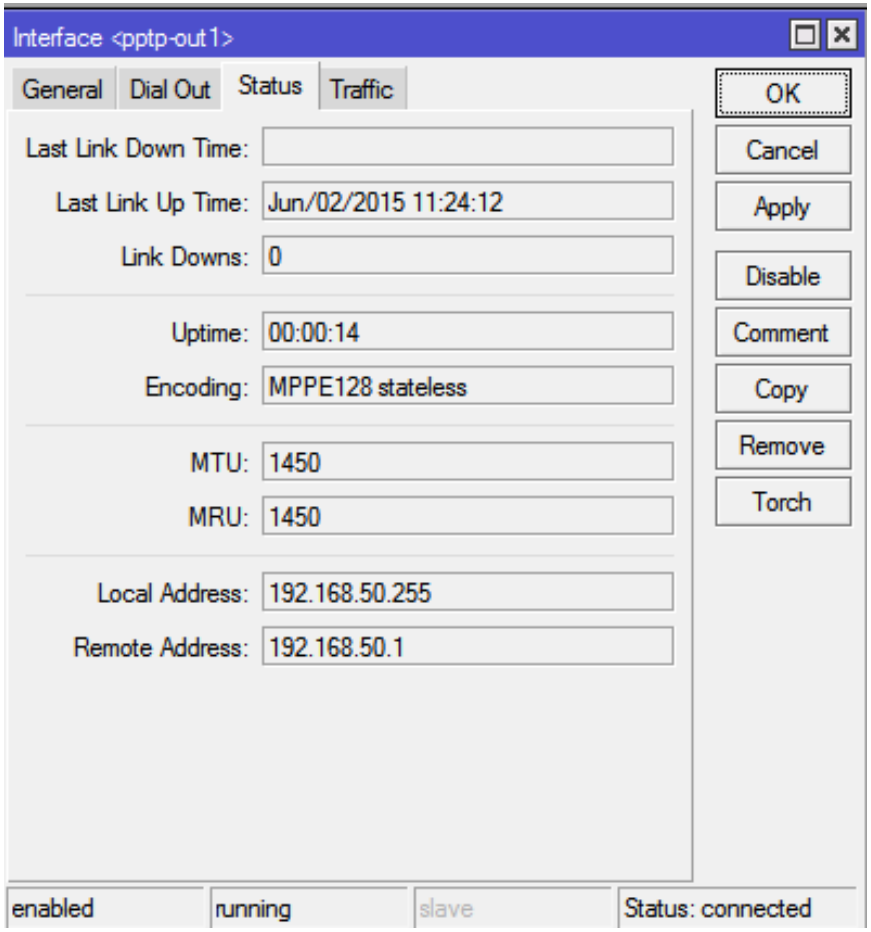
- Administrative Name
- Tunnel Type
- Layer 2 Max Transmission Unit
- Max Packet size the client can send without fragmentation
- Max Receive Unit – Max the client can receive without fragmentation
- Multilink Maximum Received Reconstructed Unit – Used with MLPPP

PPTP Client Settings



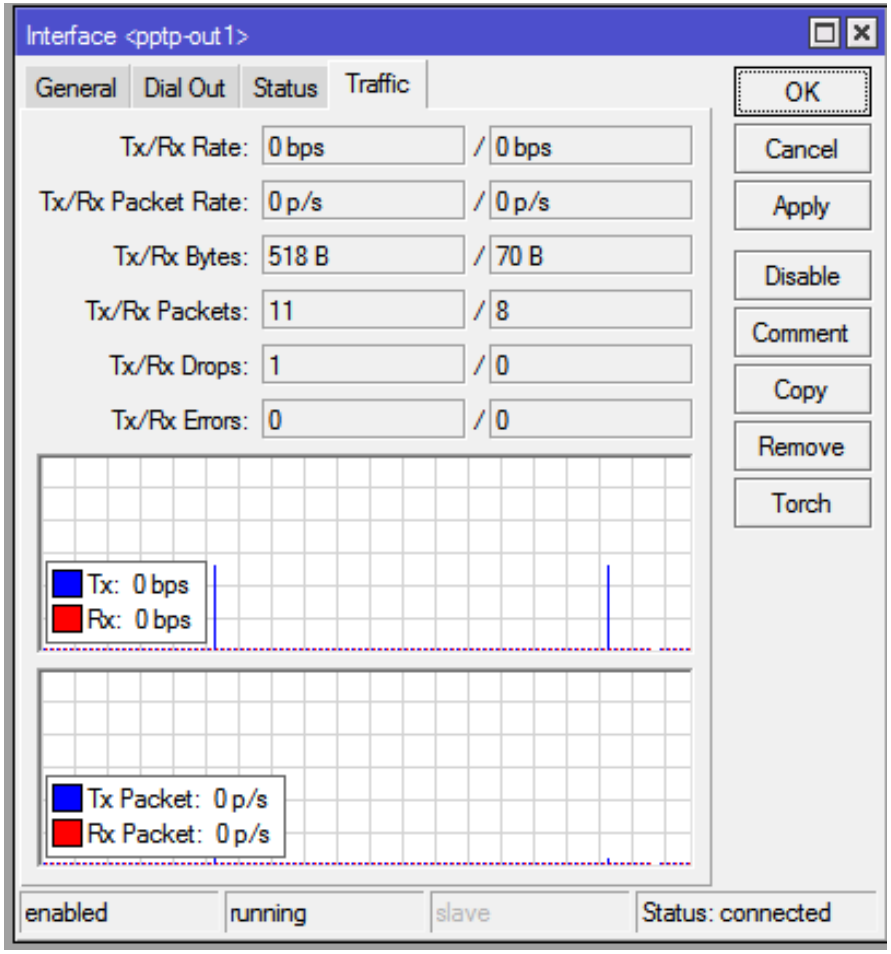
- IP address of server
- Username
- Password
- Profile to be used
- How long to keep the connection alive before timing out
- When selected, the tunnel will only establish when traffic is generated – Do not use
- Whether to add a default route (all traffic goes through tunnel) & distance
- Authentication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

PPTP Client Settings



- Status Tab provides connection info

PPTP Client Settings

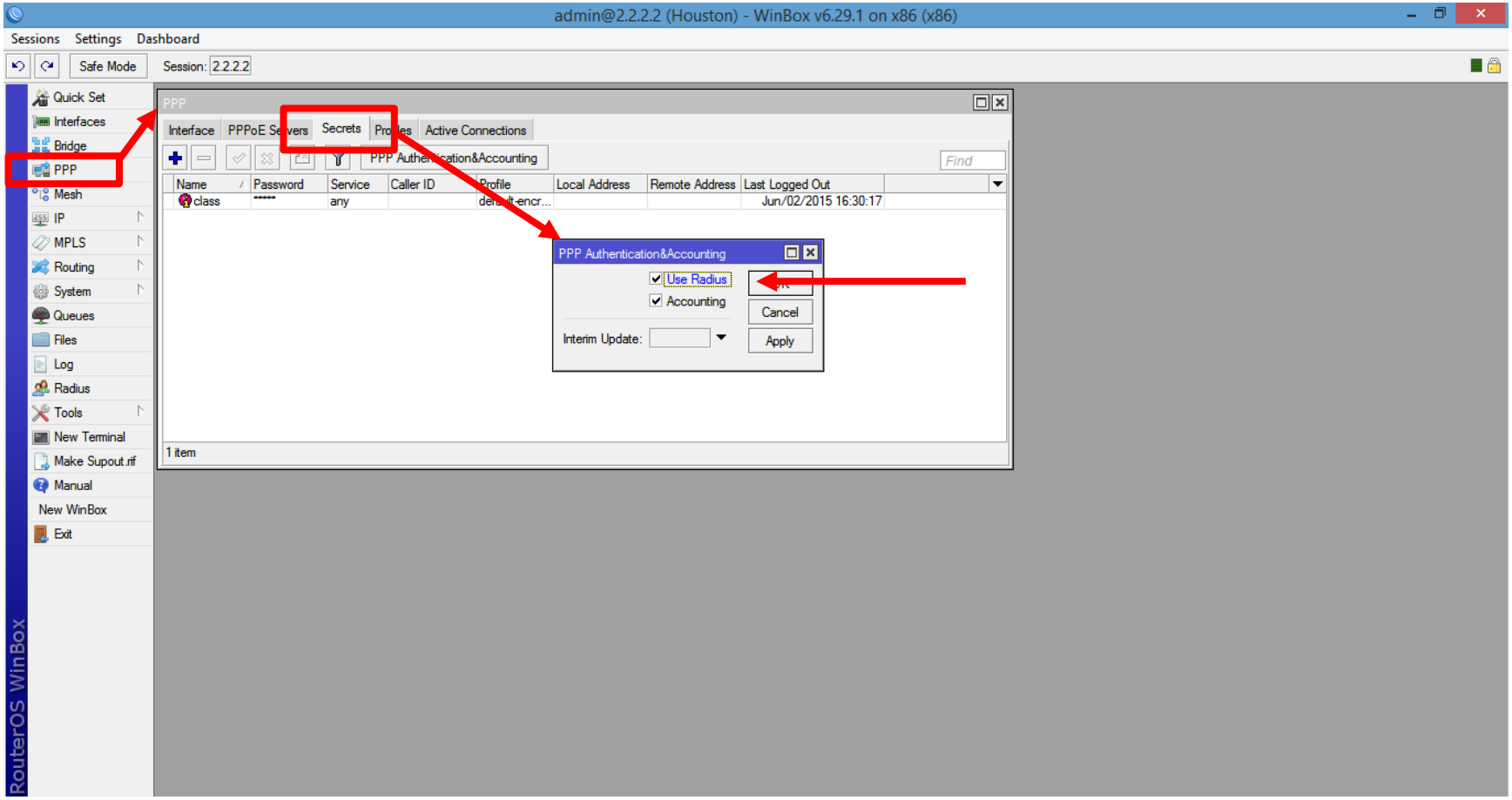


- Traffic Tab provide details on the traffic going through the tunnel

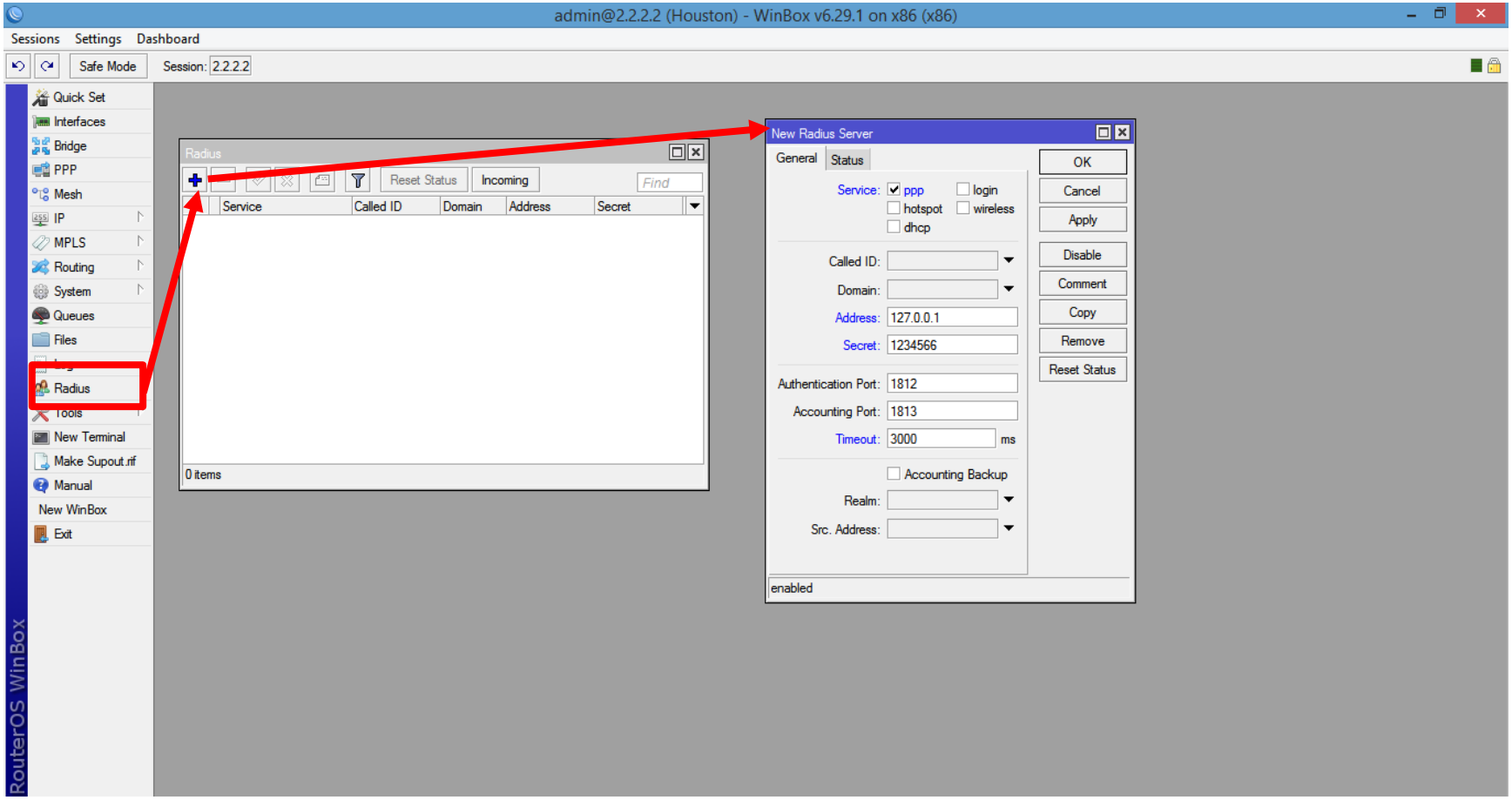
PPTP LAB

- 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.

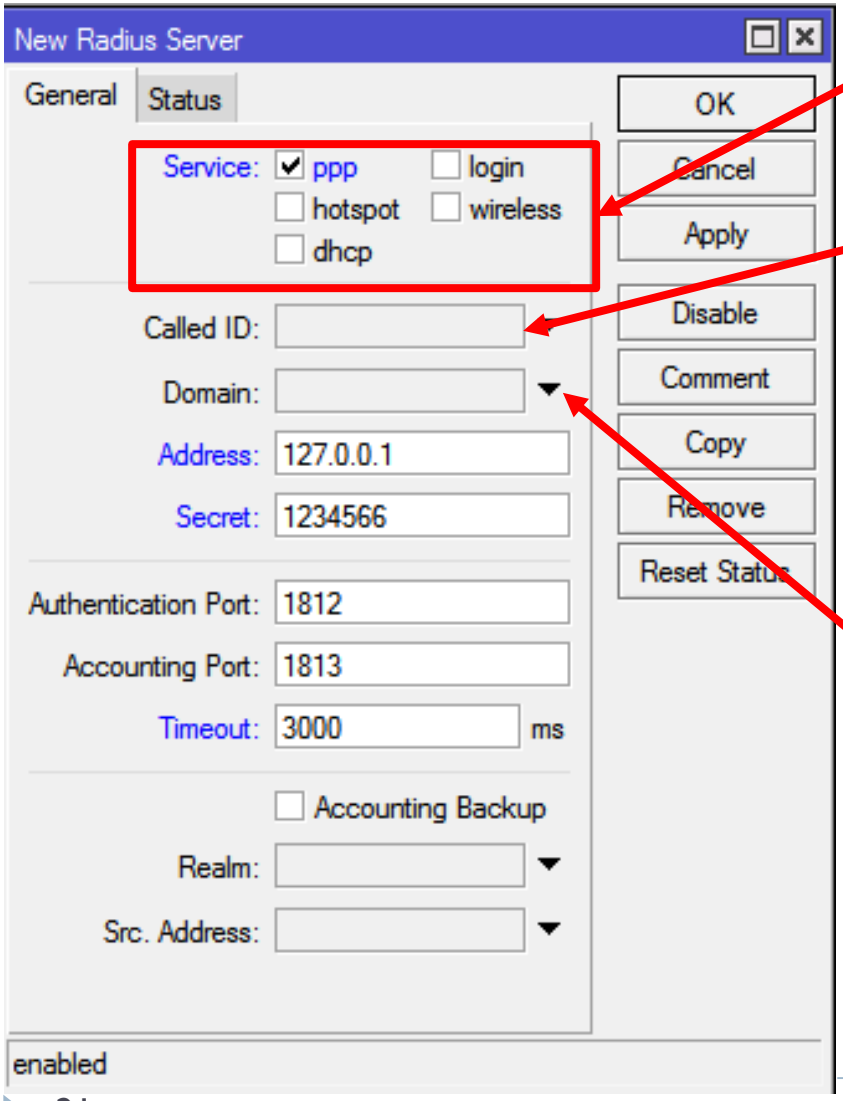
PPTP With RADIUS



RADIUS Settings

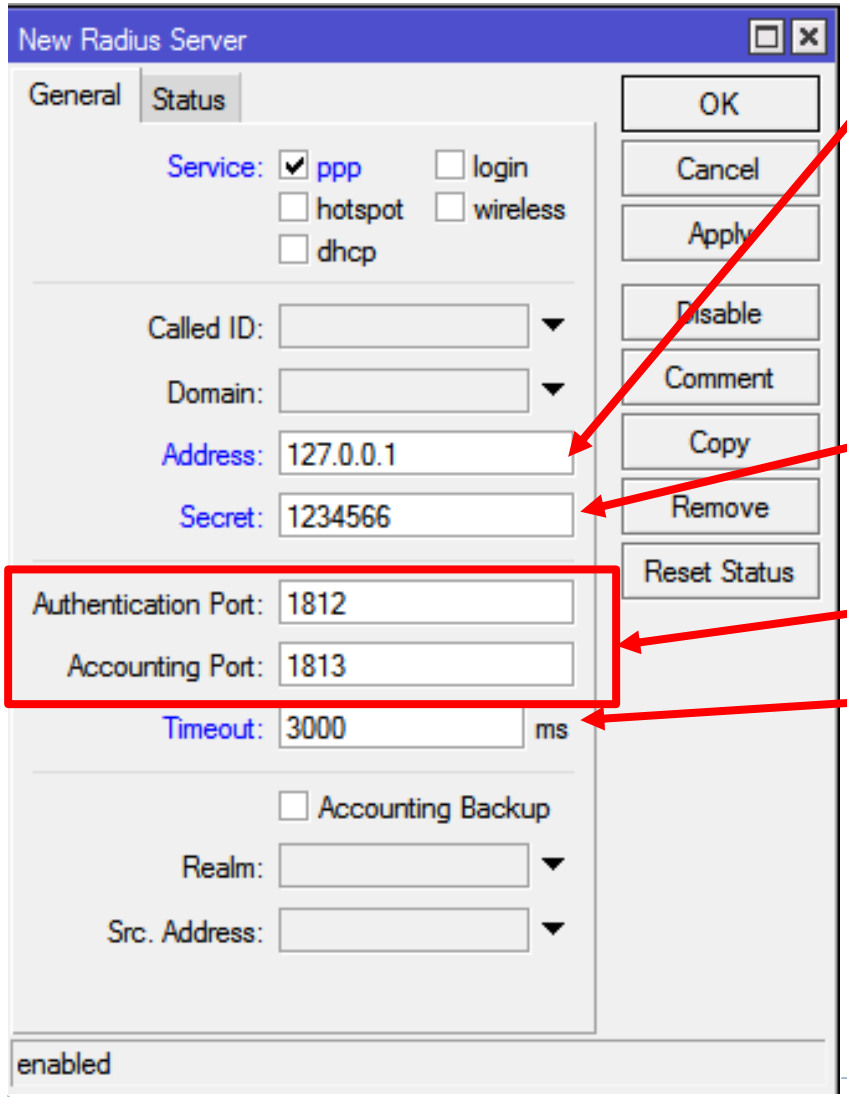


RADIUS Settings



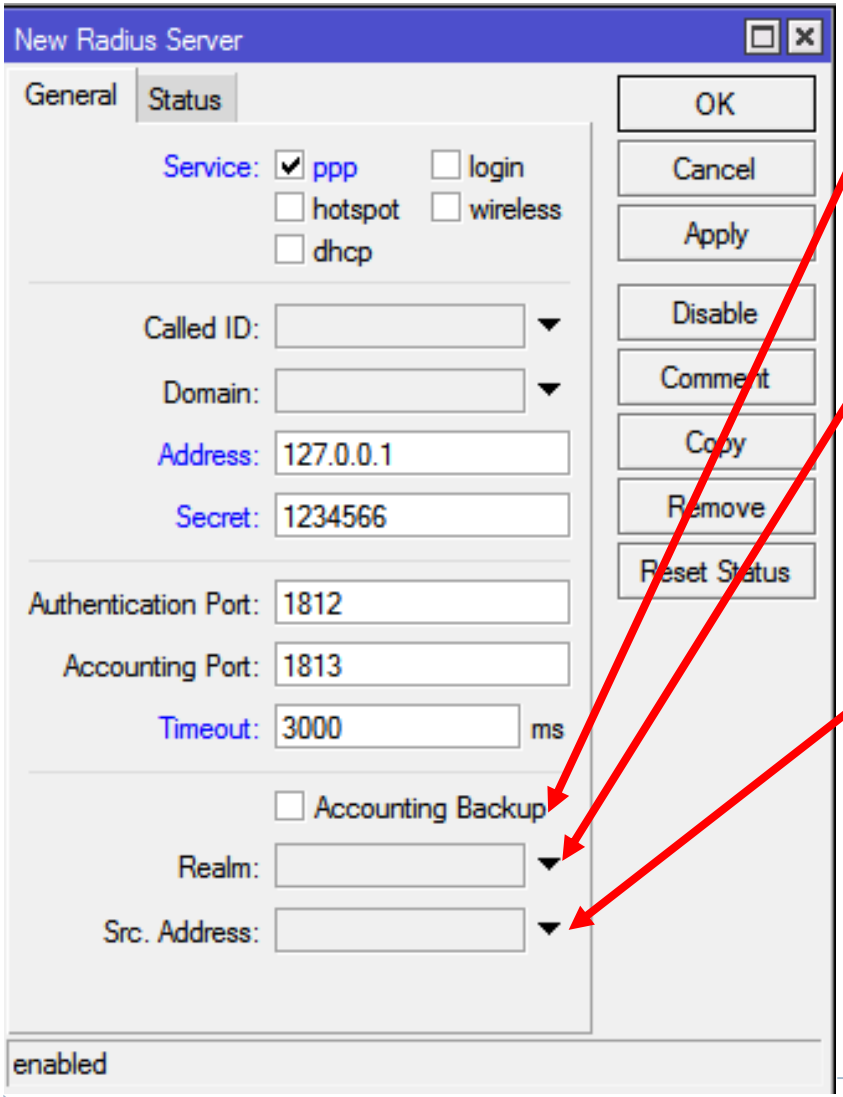
- Which service is going to talk to the RADIUS server
- Caller ID (Not usually required) - PPPoE - service name, PPTP - server's IP address, L2TP - server's IP address.
- Windows Domain (Not usually required)

RADIUS Settings



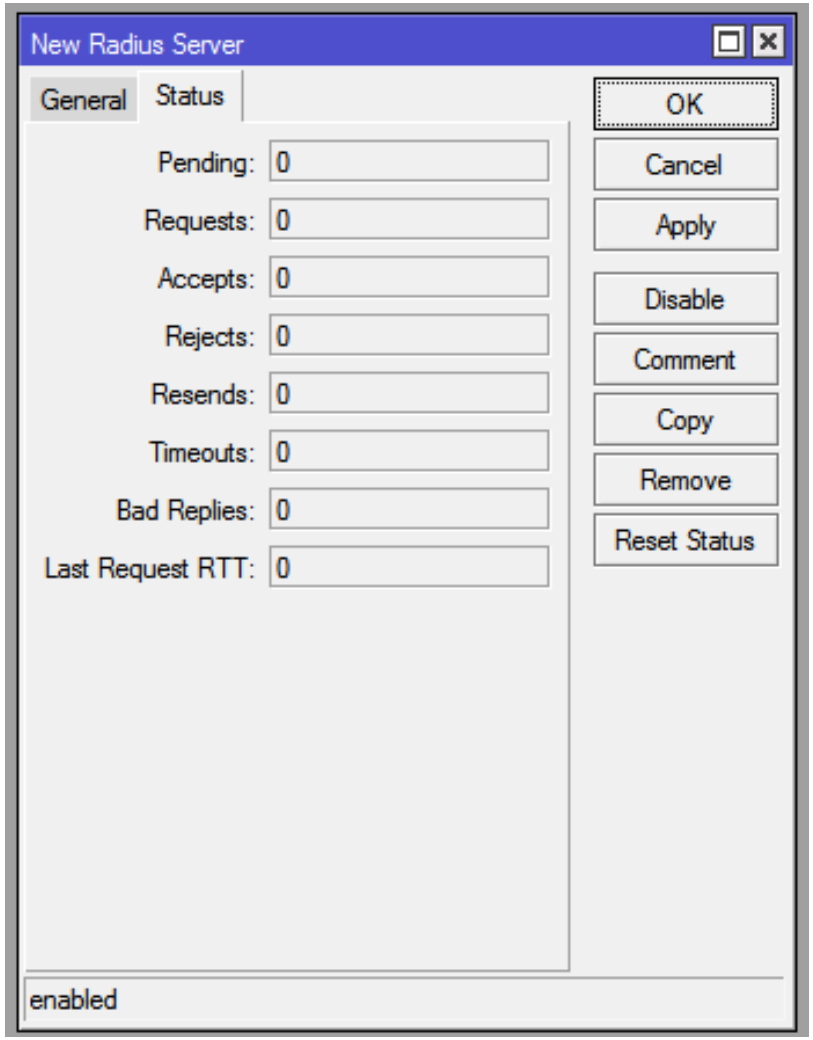
- Address of RADIUS Server (Use 127.0.0.1 when Usermanager is running on the same router)
- Shared secret with RADIUS server
- Standard RADIUS ports
- How long to wait for a reply before it times out. Set to seconds, not milliseconds

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

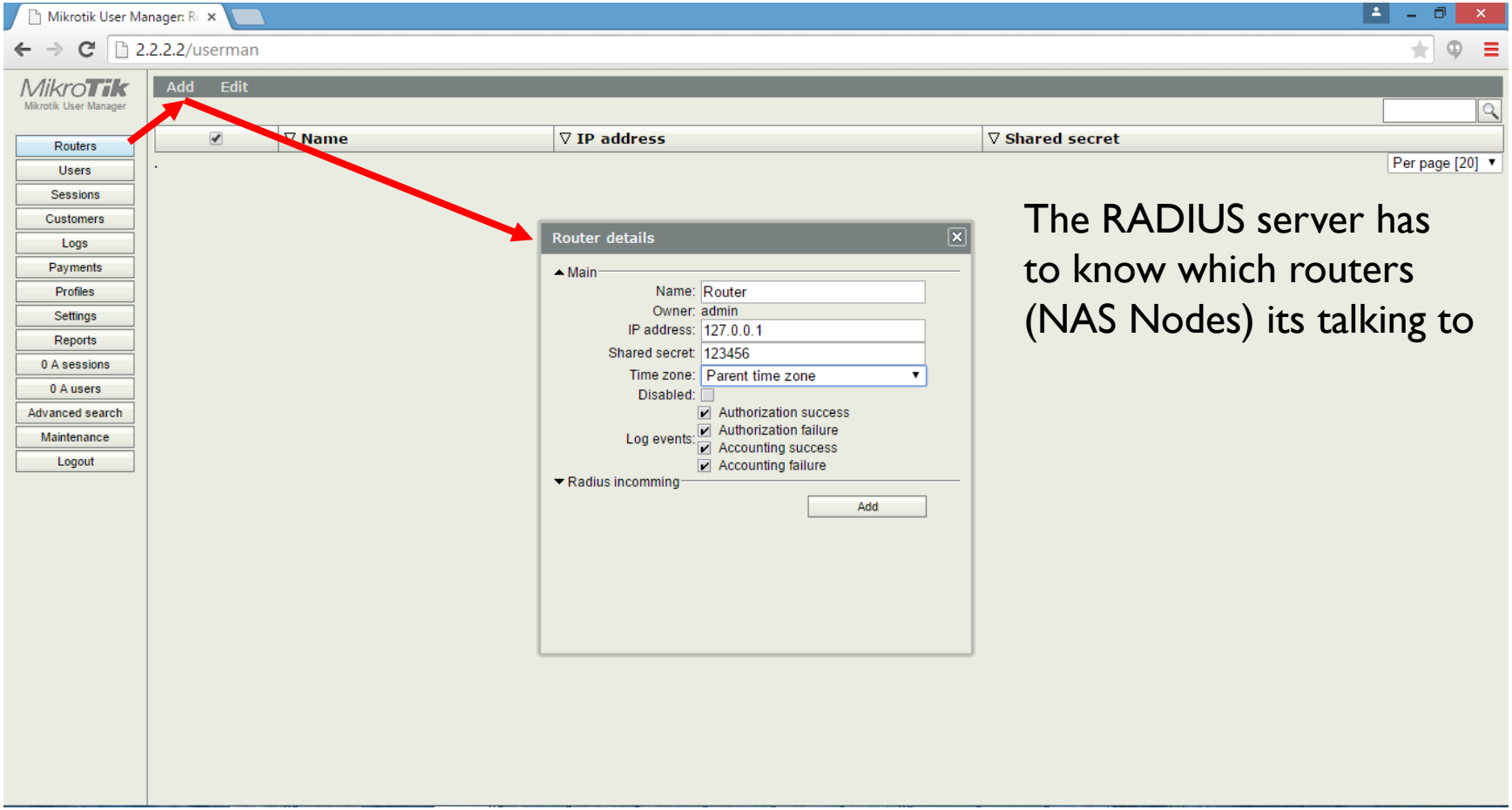


- The Status Tab is where you can see if the service to be used is sending info to the RADIUS server and whether or not the RADIUS server is replying to those requests

Usermanager

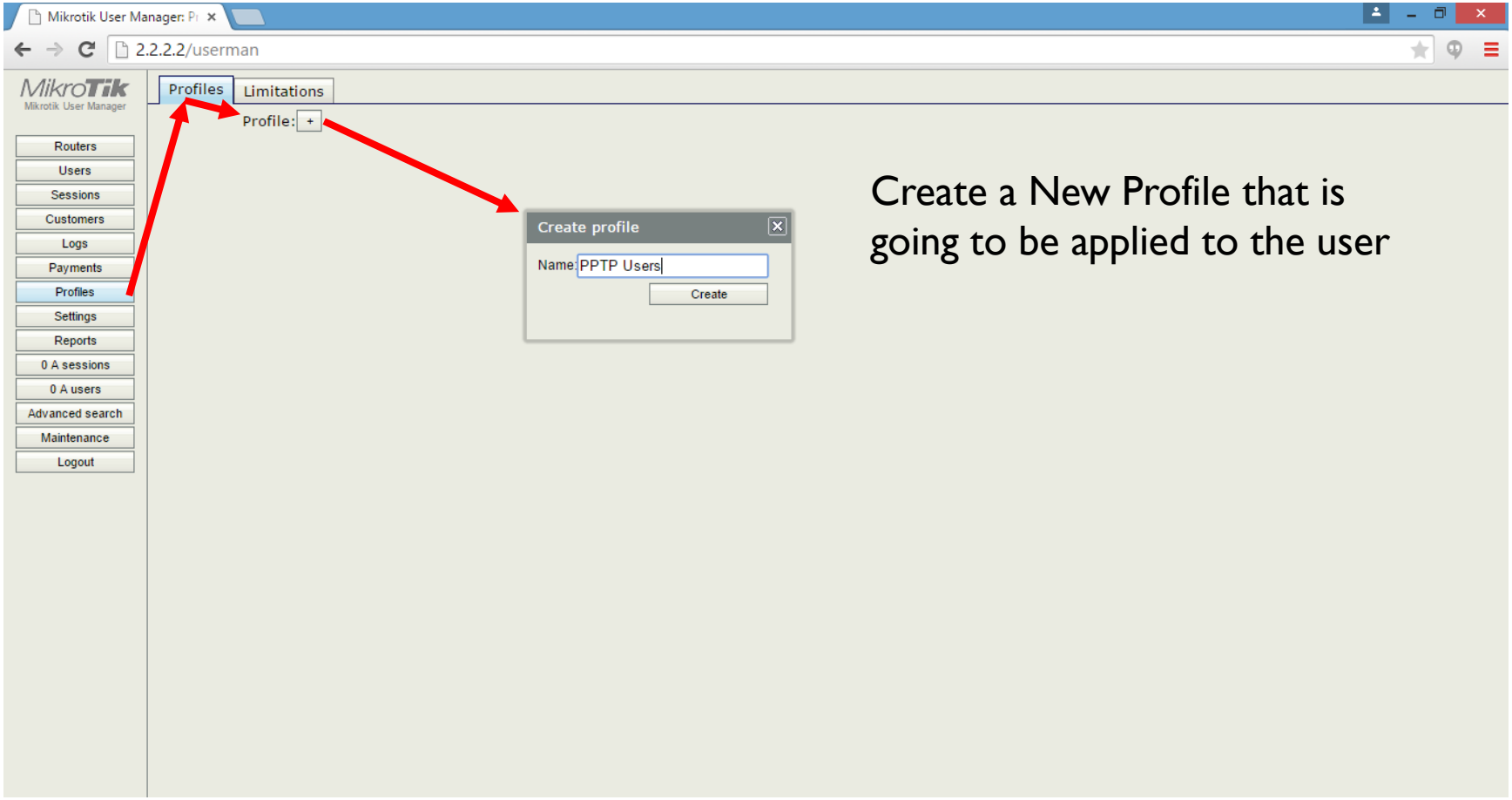
Default Login is admin
No password

Userman Settings – Step 1



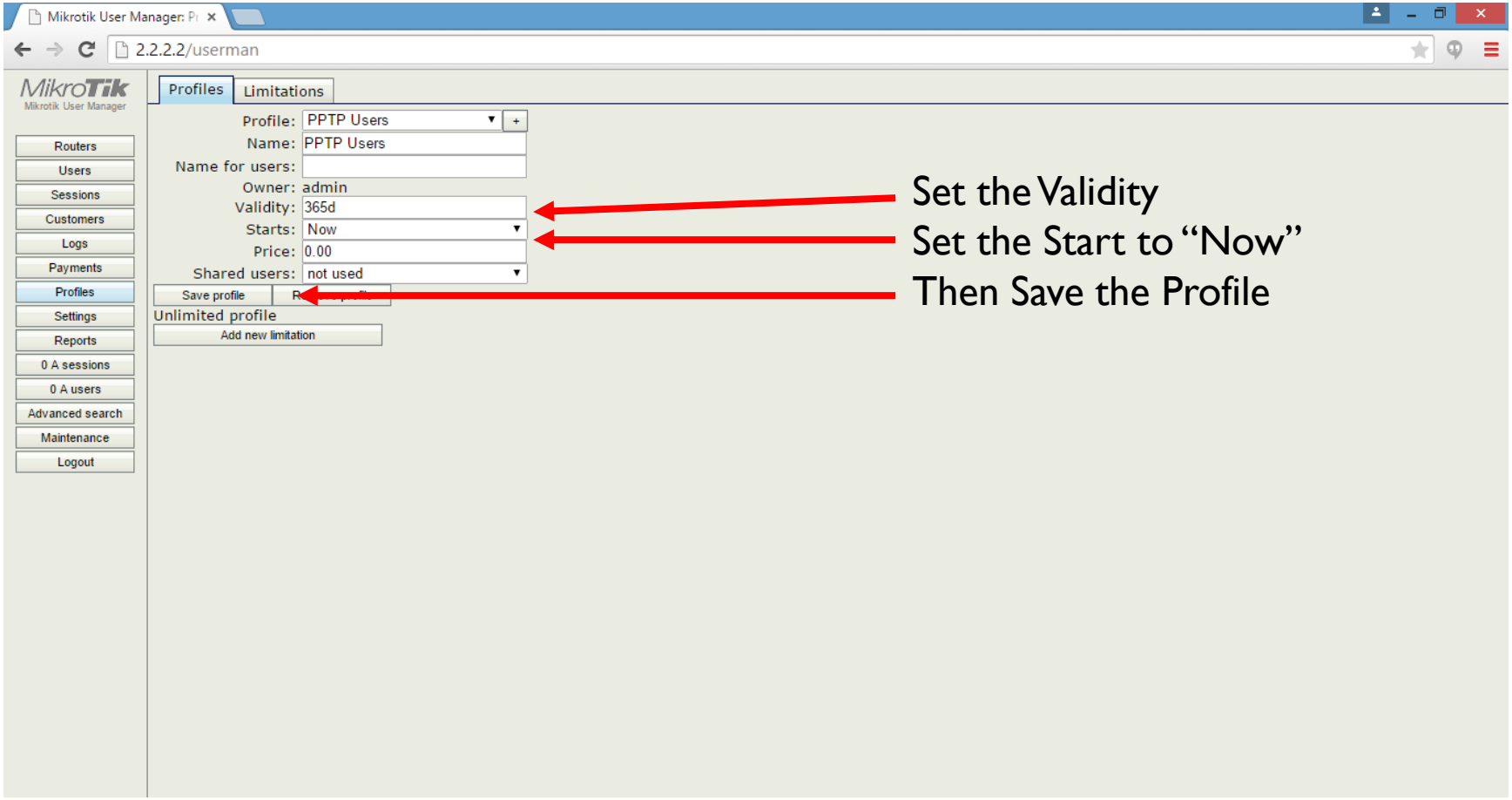
The RADIUS server has to know which routers (NAS Nodes) its talking to

Userman Settings – Step 2

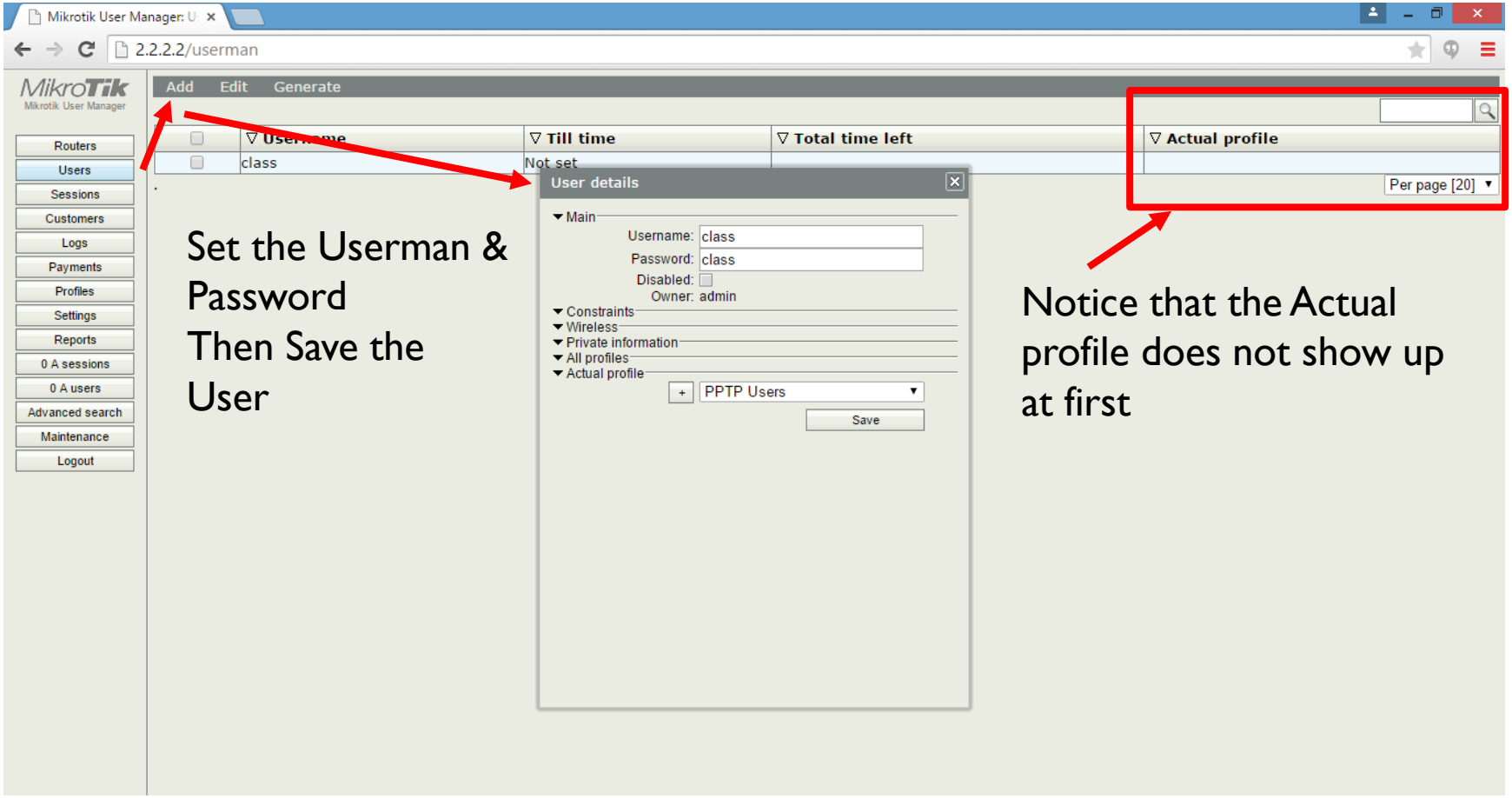


Create a New Profile that is going to be applied to the user

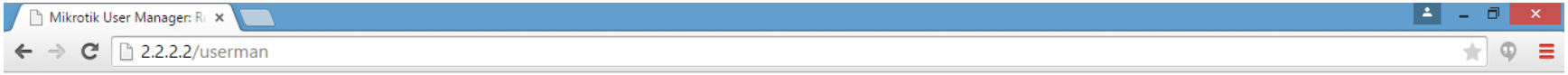
Userman Settings – Step 2 (Cont)



Userman Settings – Step 3

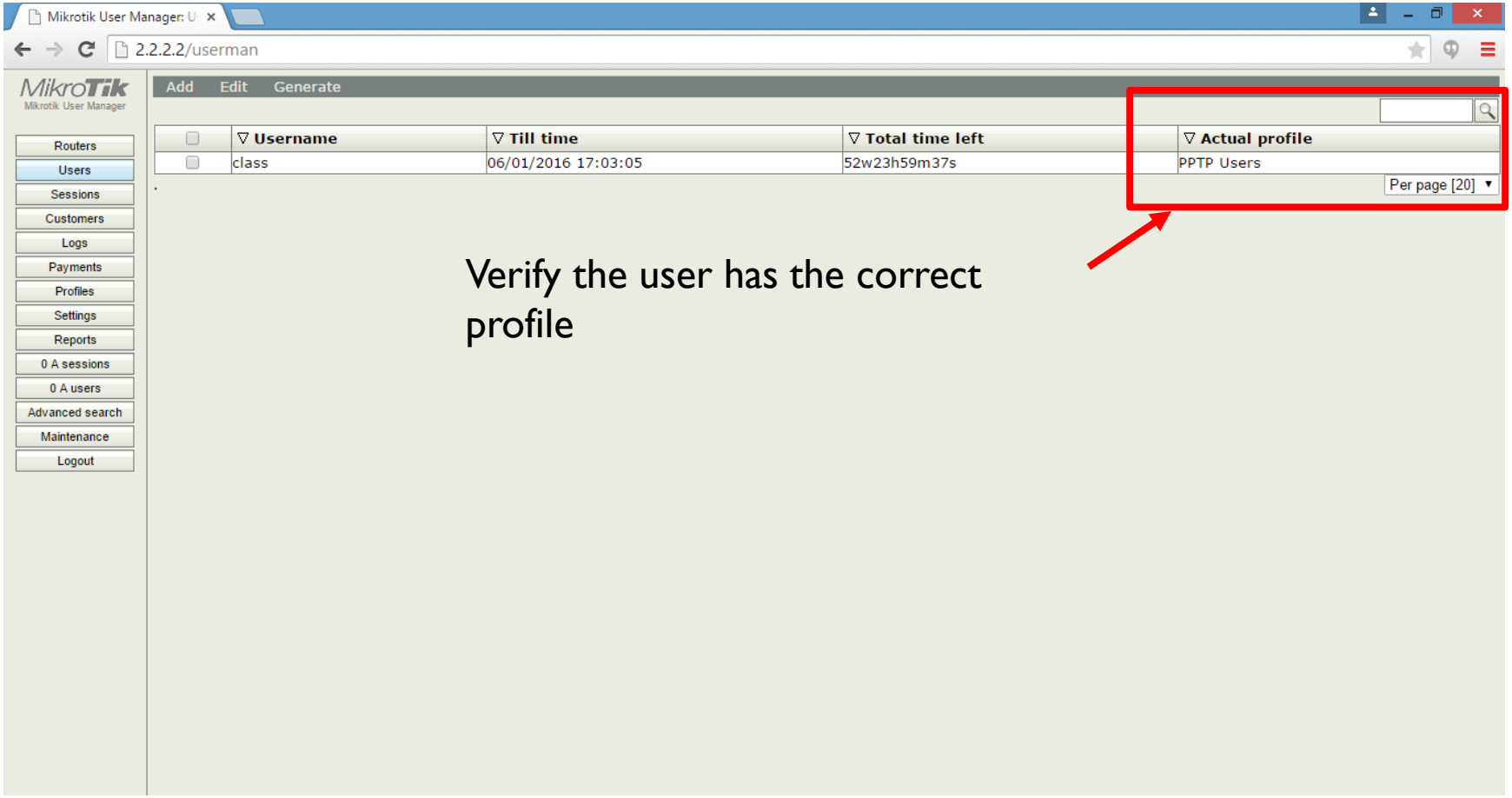


Userman Settings – Step 4

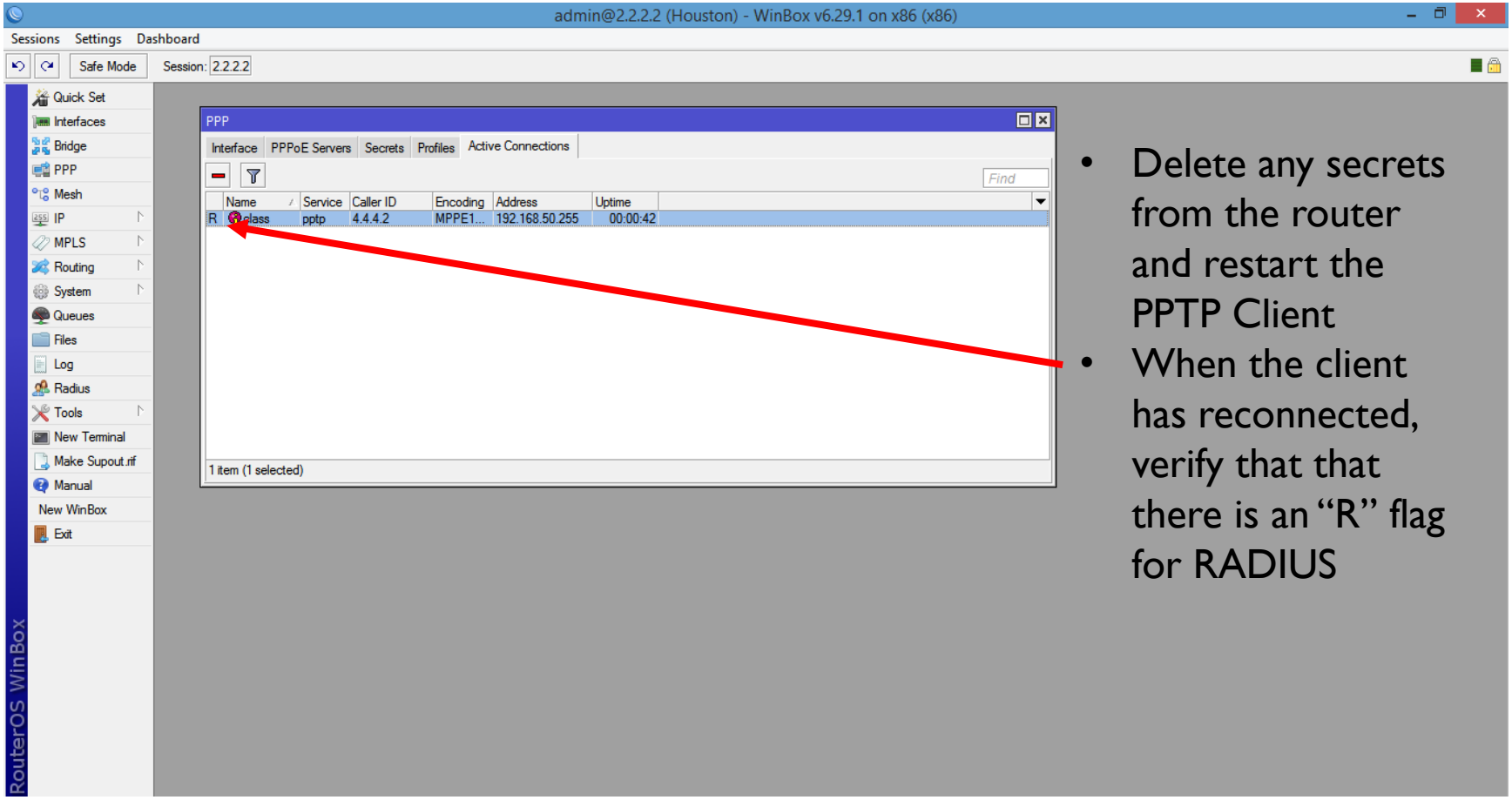


Log out and then log back in

Userman Settings



PPTP Client Settings



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

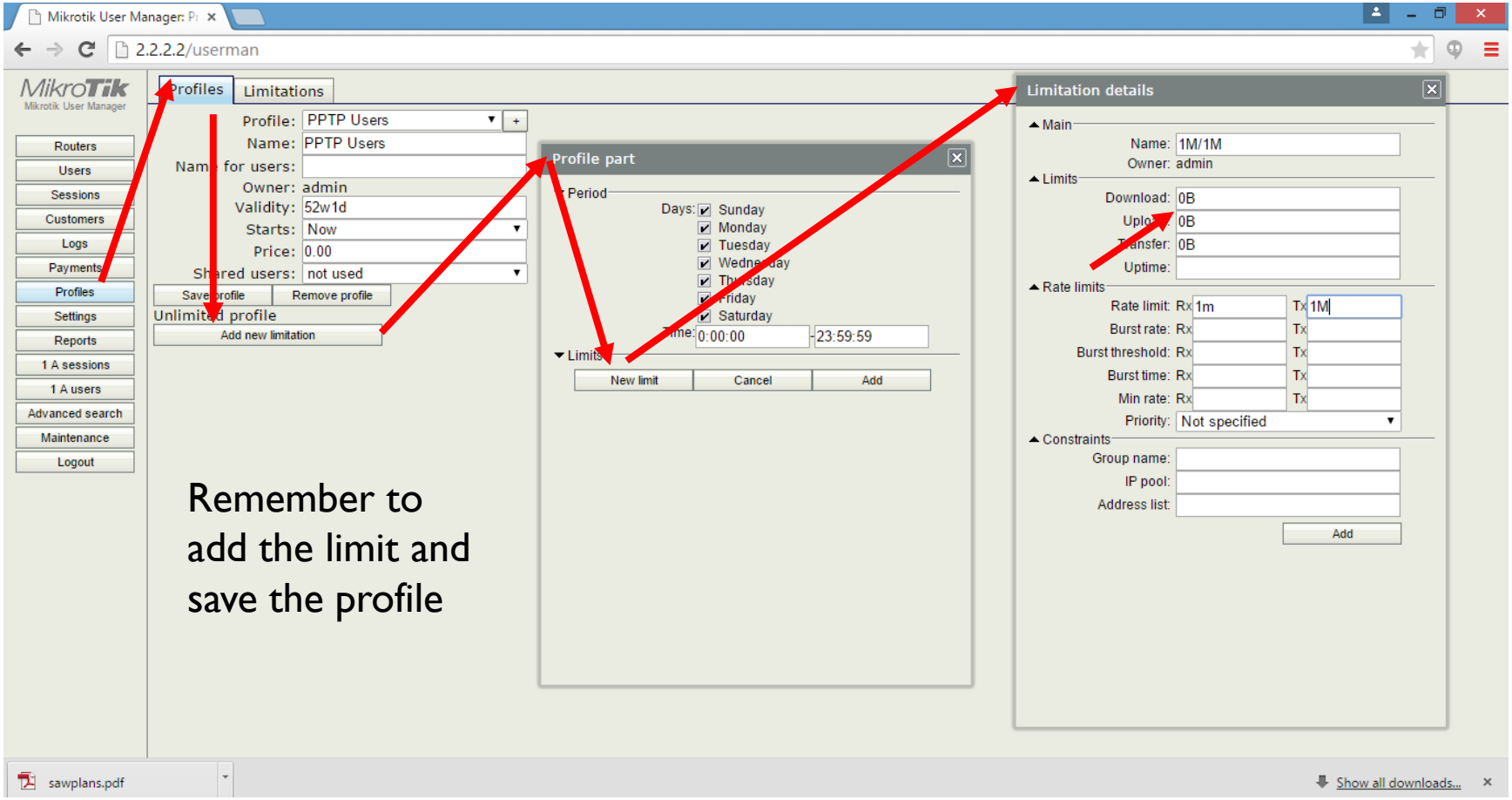
PPTP & RADIUS Lab

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

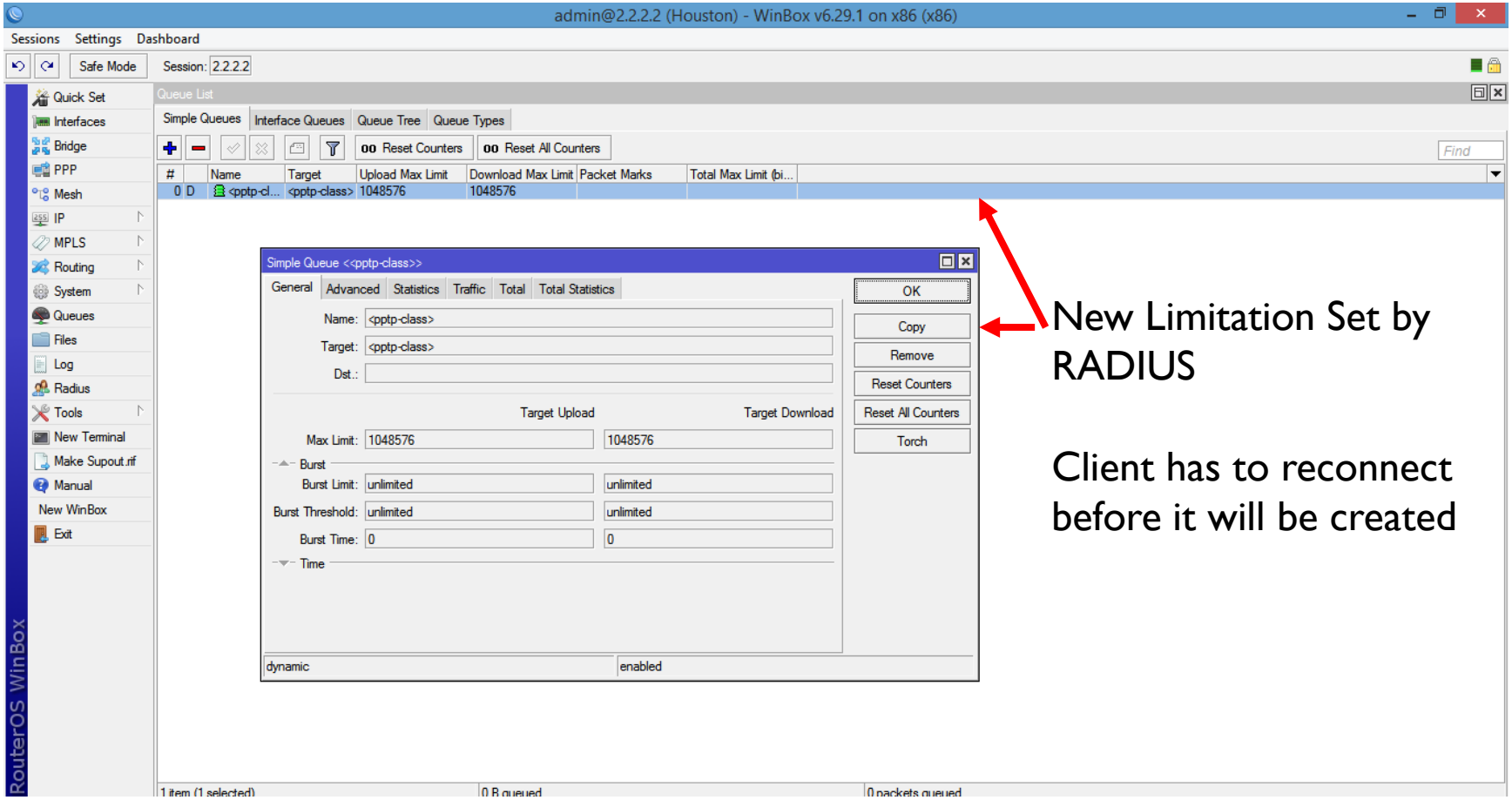
Adding Dynamic Queues

- Dynamically created queues can be added by utilizing the Limitations feature in the Usermanager Profile

Adding Dynamic Queues



Adding Dynamic Queues

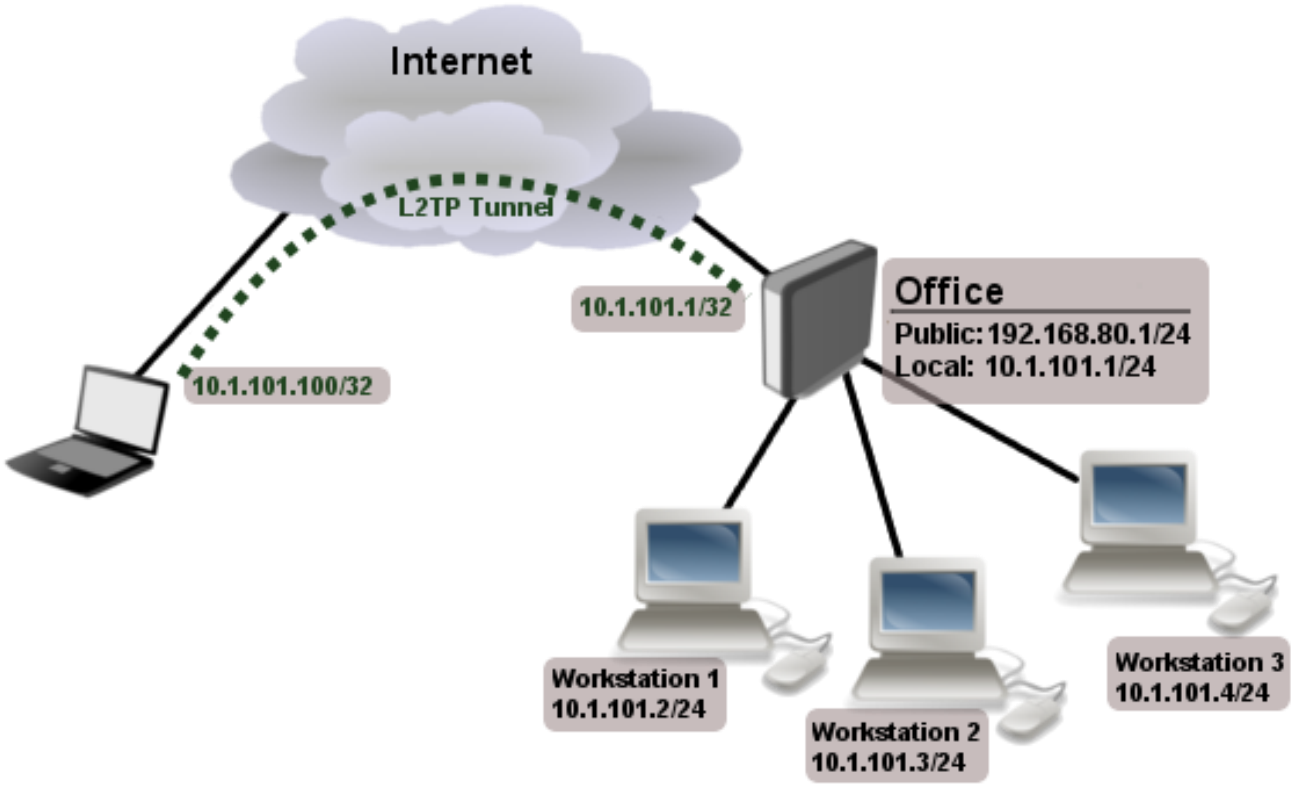


Dynamic Queue Lab

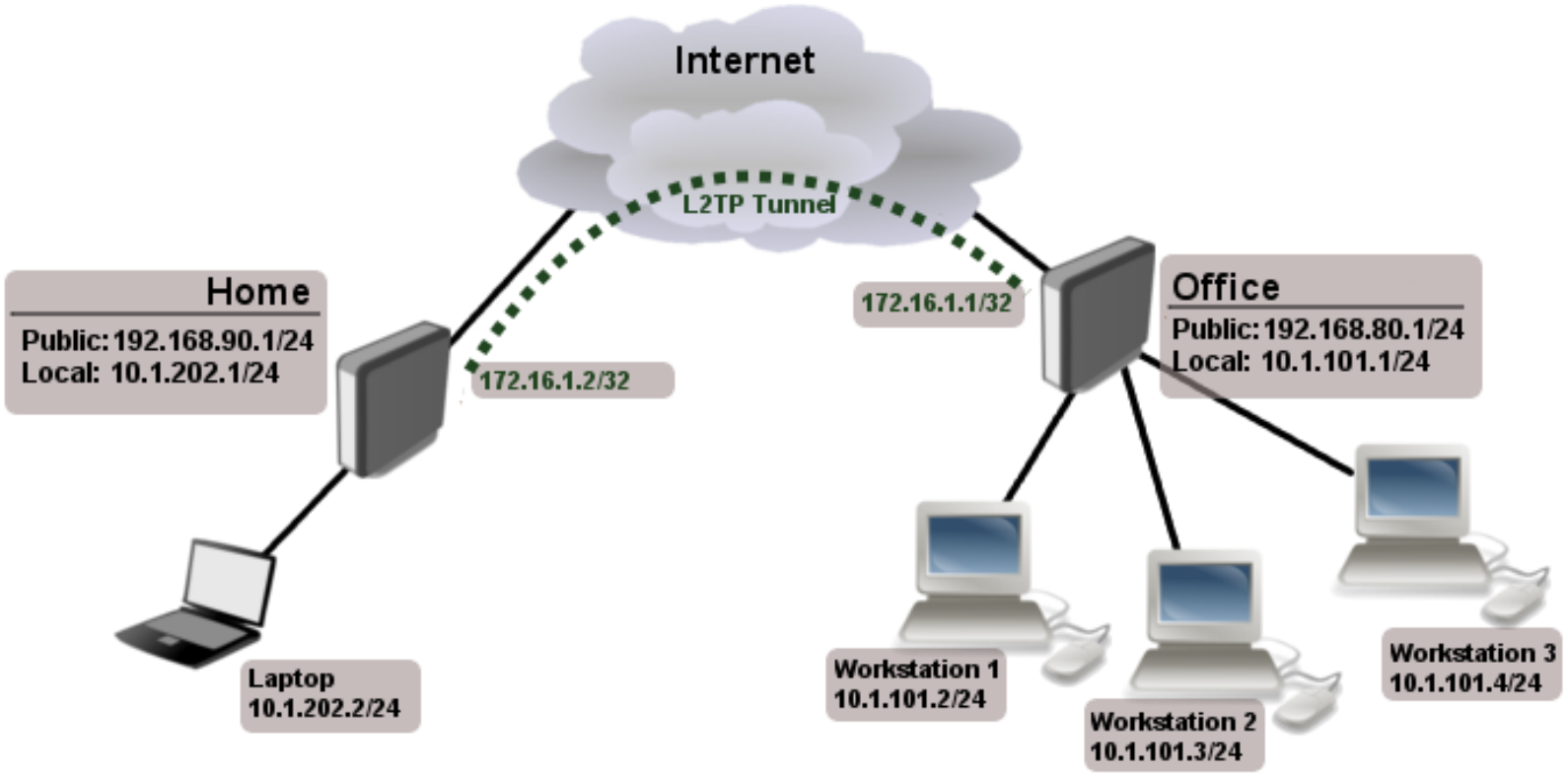
- Set a new limitation of 1 Meg up and 1 Med down and test with the bandwidth test tool. Remember to test to IP address of the tunnel and not the IP address of the router.
- Swap roles and test the other direction.

L2TP

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 verisionso Microsoft Windows, but is difficult to setup without IPSEC. Other tunnels are recommends for this application.

L2TP in MikroTik

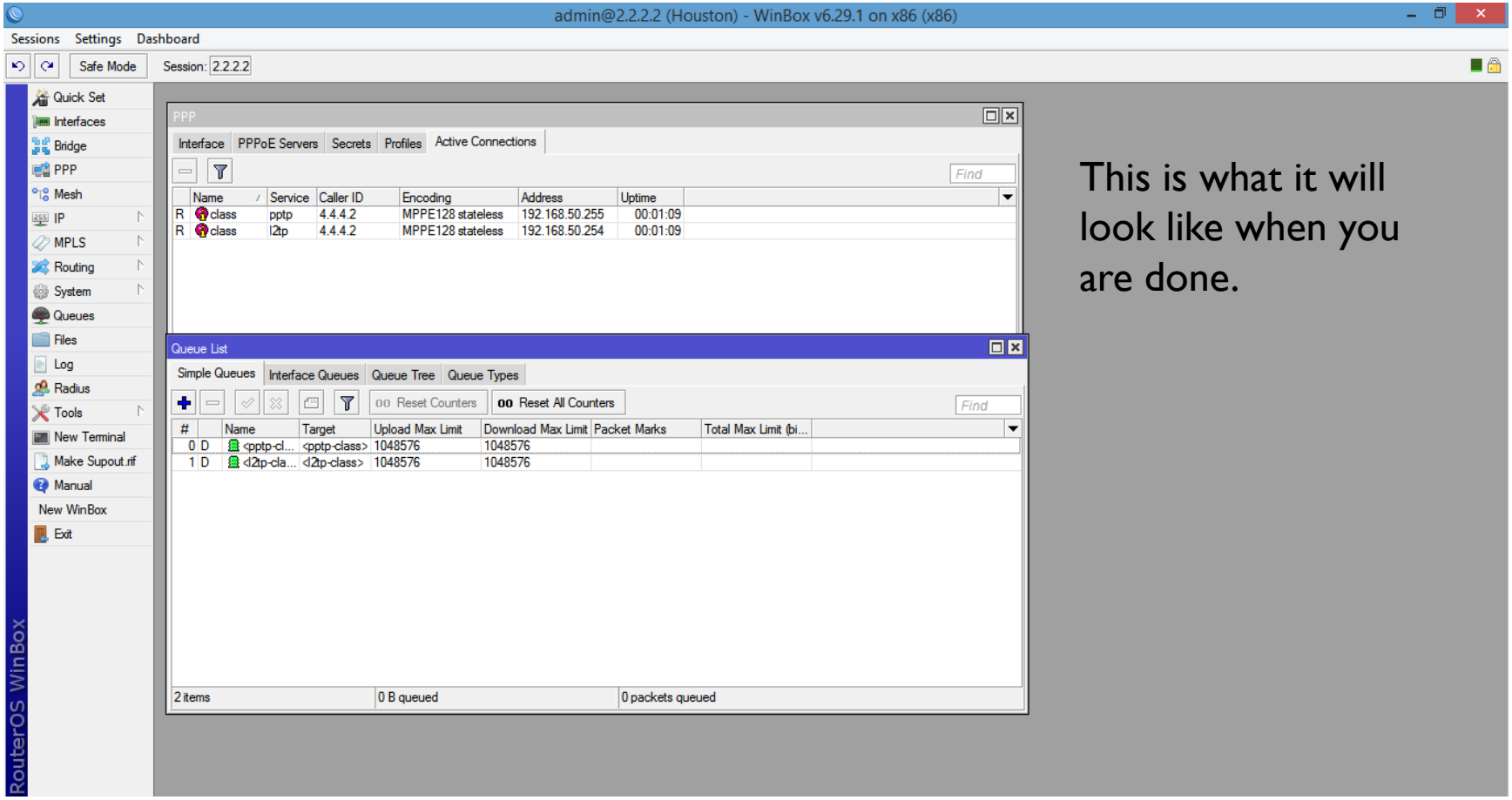
- Functionally, an L2TP is identically to the PPTP tunnel; exact same setup
- L2TP tunnels can be encrypted when both the server and client are MikroTik routers.
  - There can be limited connectivity with other OSs, but the results may be unpredictable.

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.

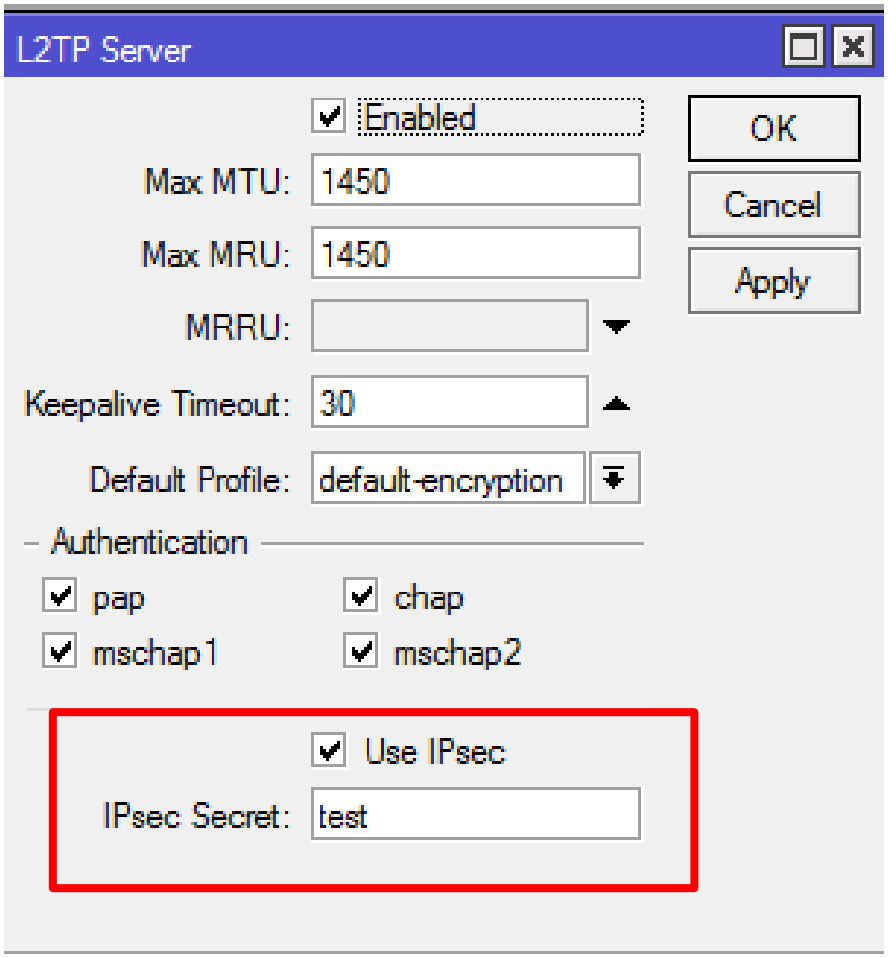
- Hint: You are going to have to modify the User in Usermanager for both tunnels to become active.

L2TP Lab



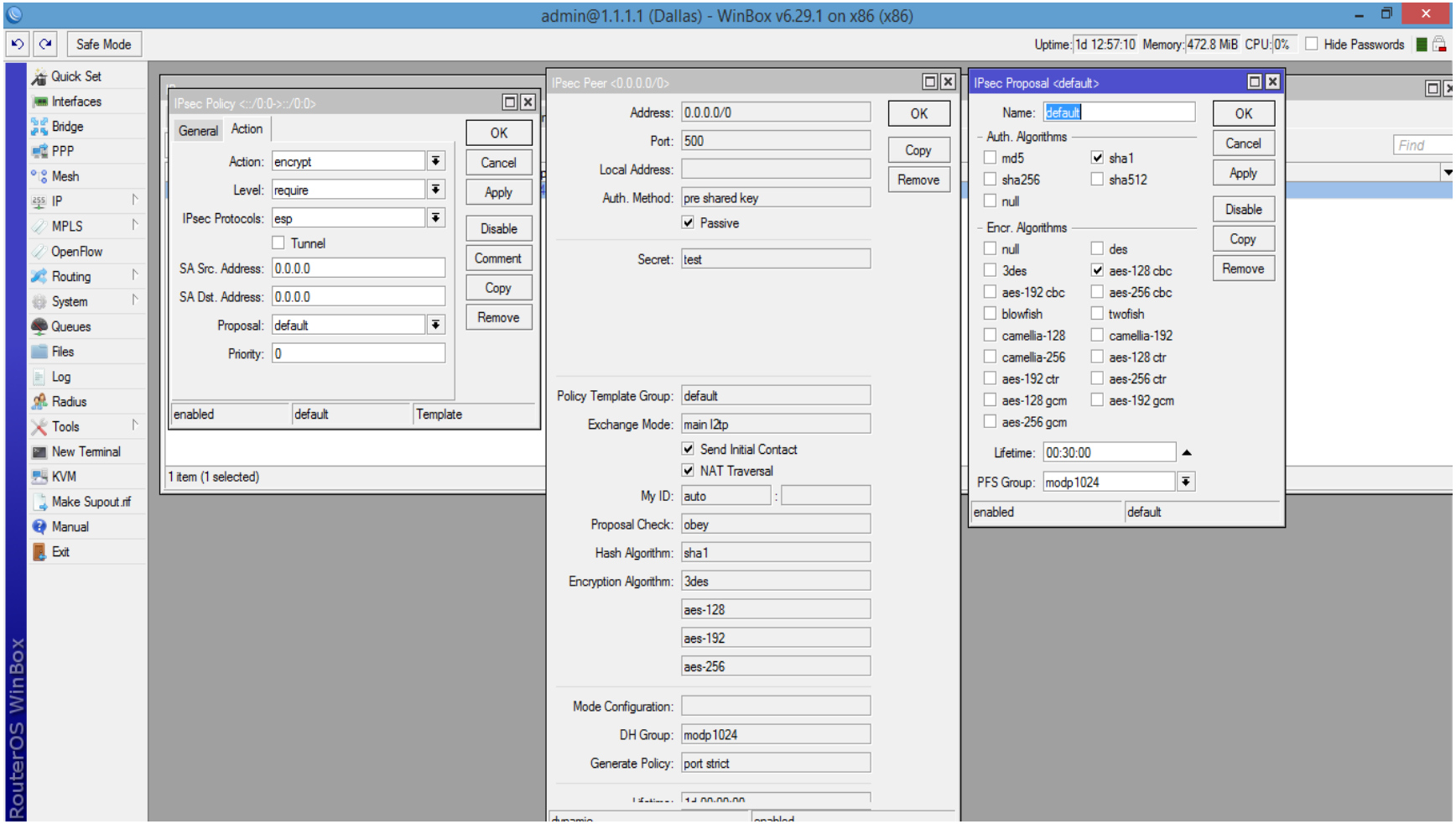
This is what it will look like when you are done.

L2TP & IPSEC



- 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


admin@1.1.1.1 (Dallas) - WinBox v6.29.1 on x86 (x86)
Safe Mode
Uptime: 1d 12:57:10 Memory: 472.8 MiB CPU: 0% Hide Passwords
Quick Set
Interfaces
Bridge
PPP
Mesh
IP
MPLS
OpenFlow
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
KVM
Make Supout.rif
Manual
Exit
RouterOS WinBox
IPsec Policy <::/0:0->::/0:0>
General
Action
Action: encrypt
Level: require
IPsec Protocols: esp
Tunnel
SA Src. Address: 0.0.0.0
SA Dst. Address: 0.0.0.0
Proposal: default
Priority: 0
OK
Cancel
Apply
Disable
Comment
Copy
Remove
enabled
default
Template
1 item (1 selected)
IPsec Peer <0.0.0.0/0>
Address: 0.0.0.0/0
Port: 500
Local Address:
Auth. Method: pre shared key
Passive
Secret: test
Policy Template Group: default
Exchange Mode: main l2tp
Send Initial Contact
NAT Traversal
My ID: auto
Proposal Check: obey
Hash Algorithm: sha1
Encryption Algorithm: 3des
aes-128
aes-192
aes-256
Mode Configuration:
DH Group: modp1024
Generate Policy: port strict
OK
Copy
Remove
IPsec Proposal <default>
Name: default
Auth. Algorithms
md5
sha1
sha256
sha512
null
Encr. Algorithms
null
des
3des
aes-128 cbc
aes-192 cbc
aes-256 cbc
blowfish
twofish
camellia-128
camellia-192
camellia-256
aes-128 ctr
aes-192 ctr
aes-256 ctr
aes-128 gcm
aes-192 gcm
aes-256 gcm
Lifetime: 00:30:00
PFS Group: modp1024
OK
Cancel
Apply
Disable
Copy
Remove
enabled
default
Find

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

Tunnel	Introduced	Layer	Port	Port can be changed	Default MTU	Authentication Protocols	Encryption Protocols	Encryption Level	Clients can call home	Bridging or BCP Supported
GRE	Oct 1994	3	N/A	No	1476	N/A	N/A	None	No	No
IPIP	Oct 1996	3	N/A	No	1500	N/A	N/A	None	No	No
VLAN	1998	2	N/A	No	1500	N/A	N/A	None	N/A	Yes
IPSEC	Nov 1998	3	UDP 500	Yes	N/A	None MD5 SHA1 SHA256 SHA512	None DES, 3DES, AES, Blowfish, Twofish, Camellia	None, 64bits, 128bit, 192bit, 256bit	Yes	No
PPPoE	Feb 1999	2	N/A	N/A	1480	PAP CHAP MSCHAP v1 MSCHAP v2	None MPPE 40bit MPPE 128bit	None or 40bit or 128bit	N/A	Yes
PPtP	July 1999	3	TCP 1723	No	1450	PAP CHAP MSCHAP v1 MSCHAP v2	None MPPE 40bit MPPE 128bit	None or 40bit or 128bit	Yes	Yes
L2TP	Aug 1999	3	UDP 1701	No	1450	PAP CHAP MSCHAP v1 MSCHAP v2	None MPPE 40bit MPPE 128bit	None or 40bit or 128bit	Yes	Yes
OVPN	May 2001	3	TCP 1194	Yes	1500	None MD5 SHA1	None Blowfish 128 AES 128 AES 192 AES 256	None 128bit, 192bit, or 256bit	Yes	Yes
EOIP	Sept 2002	3	N/A	No	1500	N/A	N/A	None	No	Yes
SSTP	Jan 2007	3	TCP 443	Yes	1500	PAP CHAP MSCHAP v1 MSCHAP v2 TLS 1.0	None MPPE 40bit MPPE 128bit TLS 1.0	None or 40bit or 128bit or 256bit	Yes	Yes

Tunnel Comparaison of Loss

Tunnel	Initial Bandwidth	With Tunnel	% of Loss
GRE	691M RX	195M RX	71.80%
IPIP	691M RX	204M RX	70.50%
VLAN	691M RX	582M RX	15.80%
IPSEC	691M RX	667M RX	3.50%
PPPoE	691M RX	94M RX	86.40%
PPtP	691M RX	61M RX	91.20%
L2TP	691M RX	59M RX	91.50%
OVPN	691M RX	29M RX	95.90%
EOIP	691M RX	190M RX	72.50%
SSTP	691M RX	29M RX	95.80%

End of Module