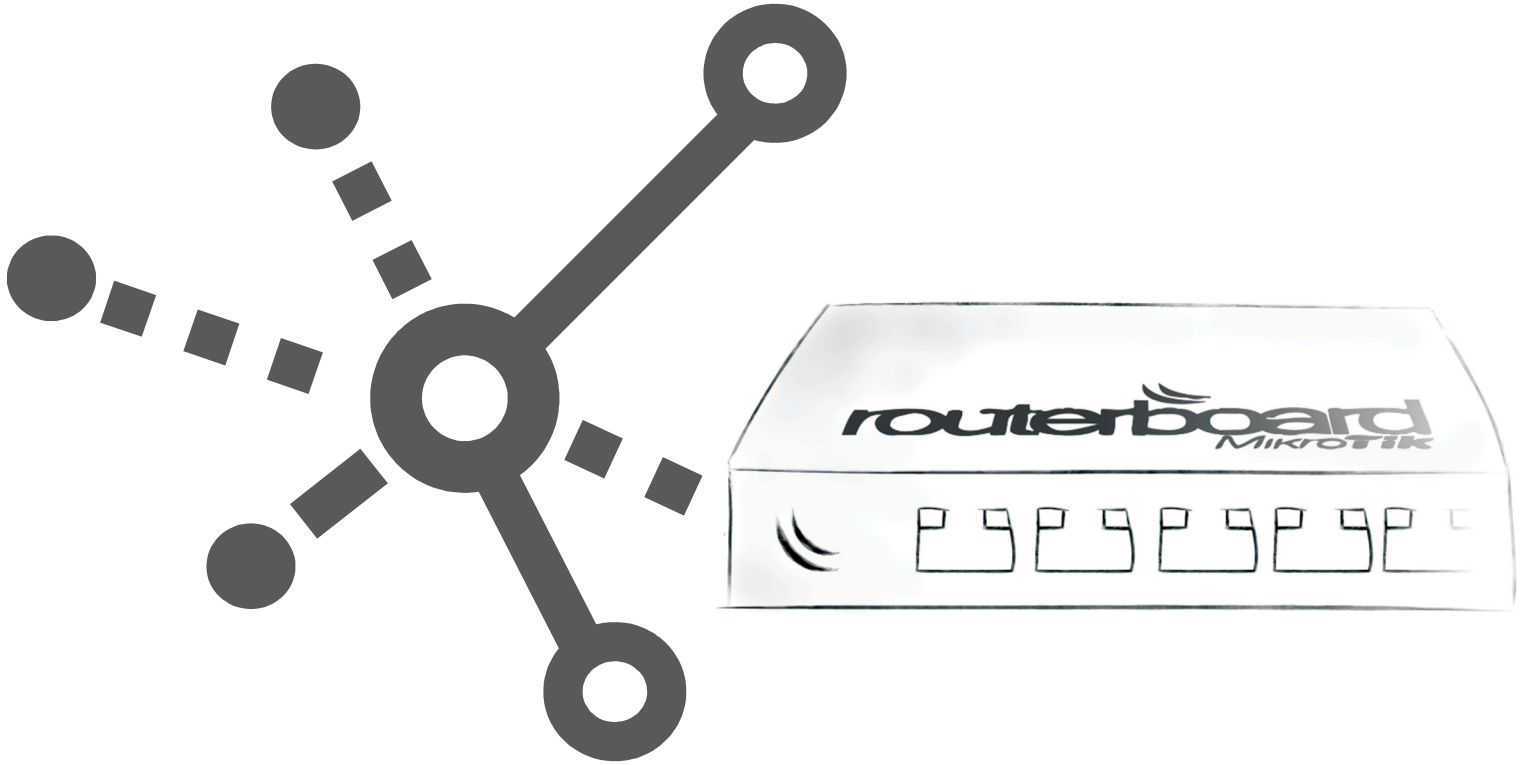
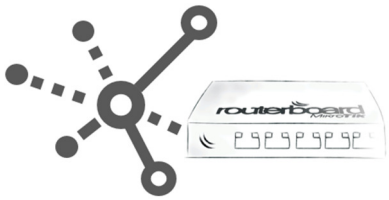
MUM Europe, Ljubljana 2016.03.25
Andis Arins / router.lv



How to choose the right VPN?

Presenter – Andis Arins

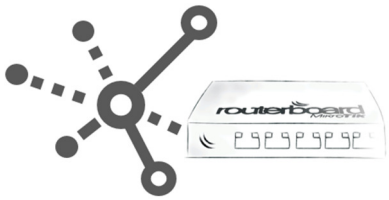


- MikroTik Consultant at www.router.lv
- MikroTik / Microsoft certified trainer
  - Member of the board in Latvian Internet Association
  - Review expert EU EC in future networking research

andis[at]router.lv

www.linkedin.com/in/andisarins

Focus of presentation



Virtual Private Networking aspects in perspective of Security / Performance / Flexibility

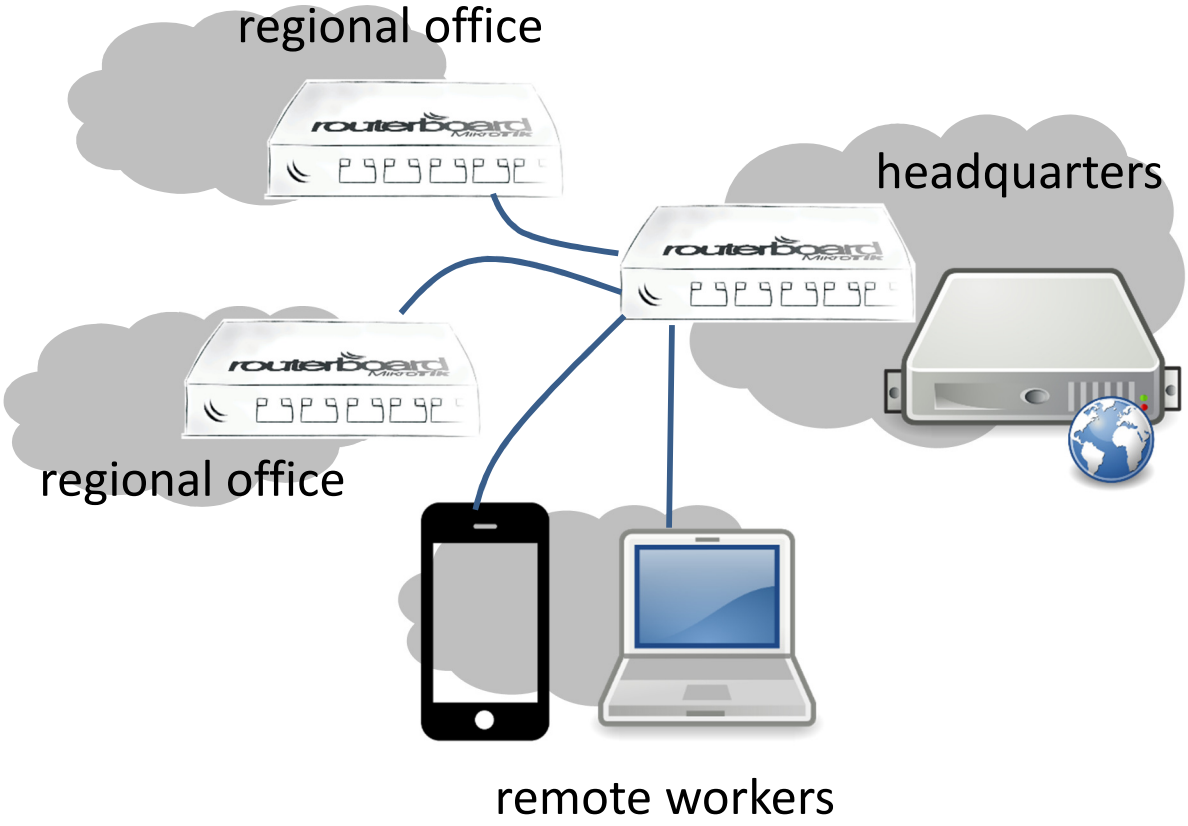
Why you want one ?

What RouterOS can offer?

How to pick the best one for you ?

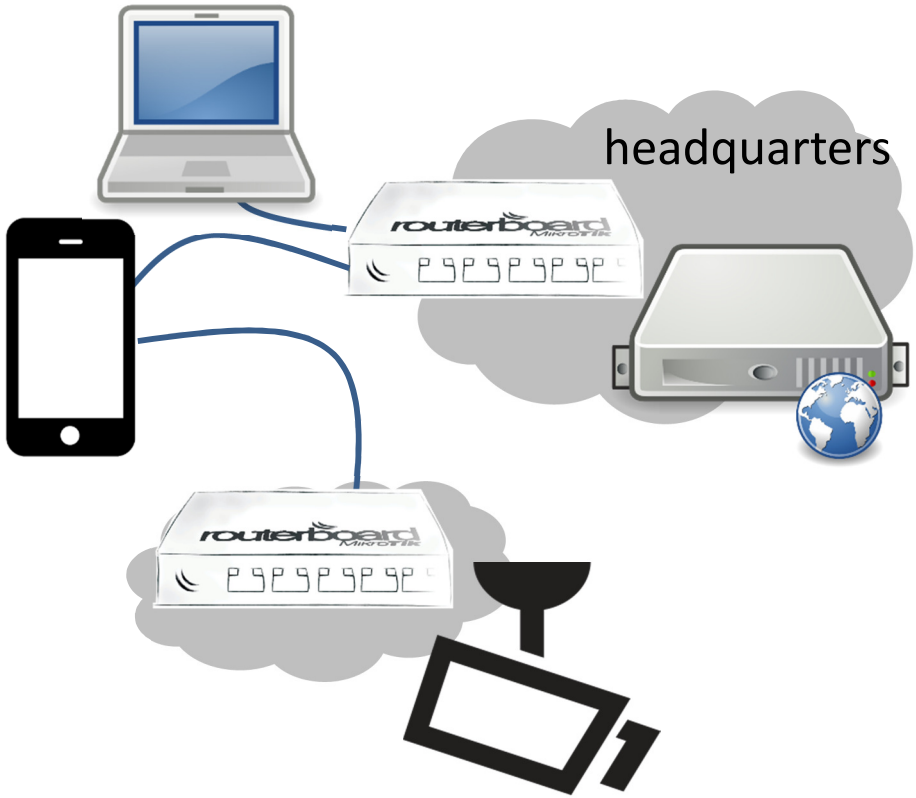
VPN user profiles

- road warriors
- corporate connections
- James Bonds

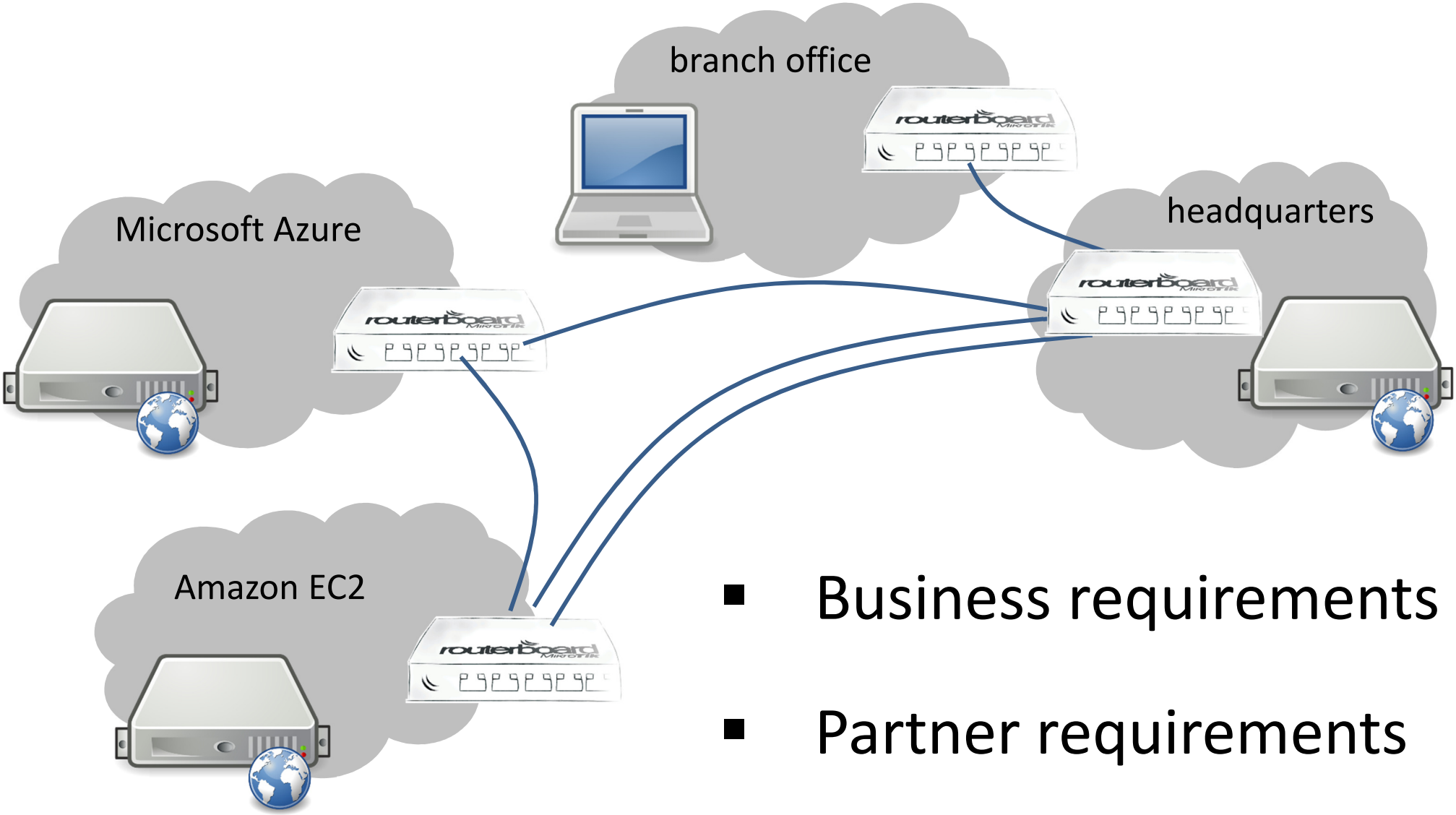


road warriors

- working from anywhere
- unpredictable network conditions

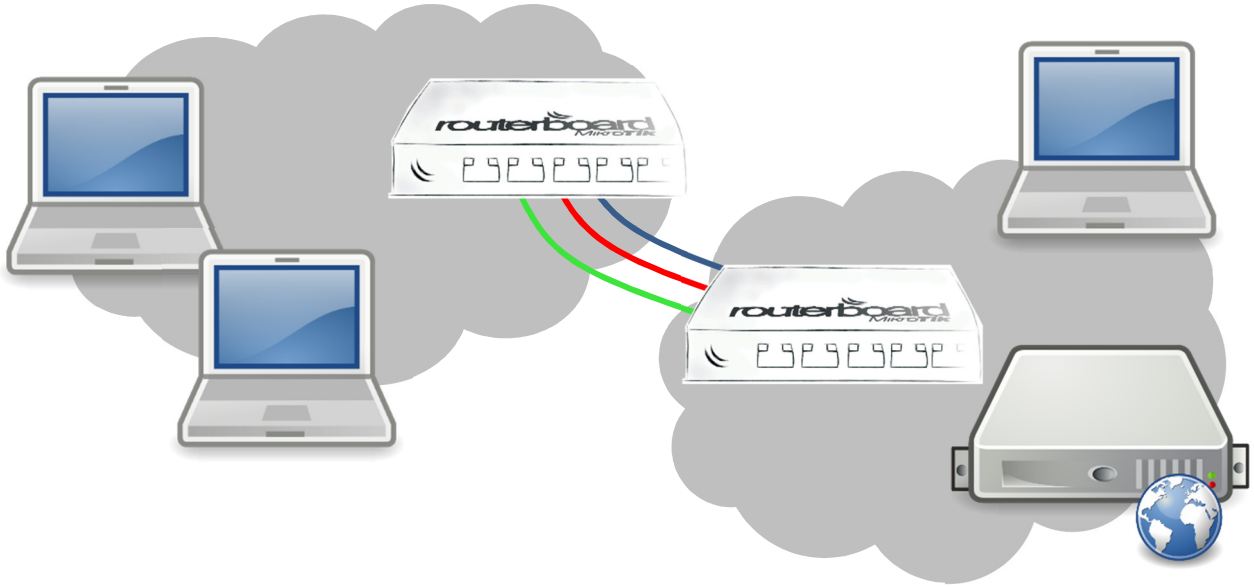


Corporate connections

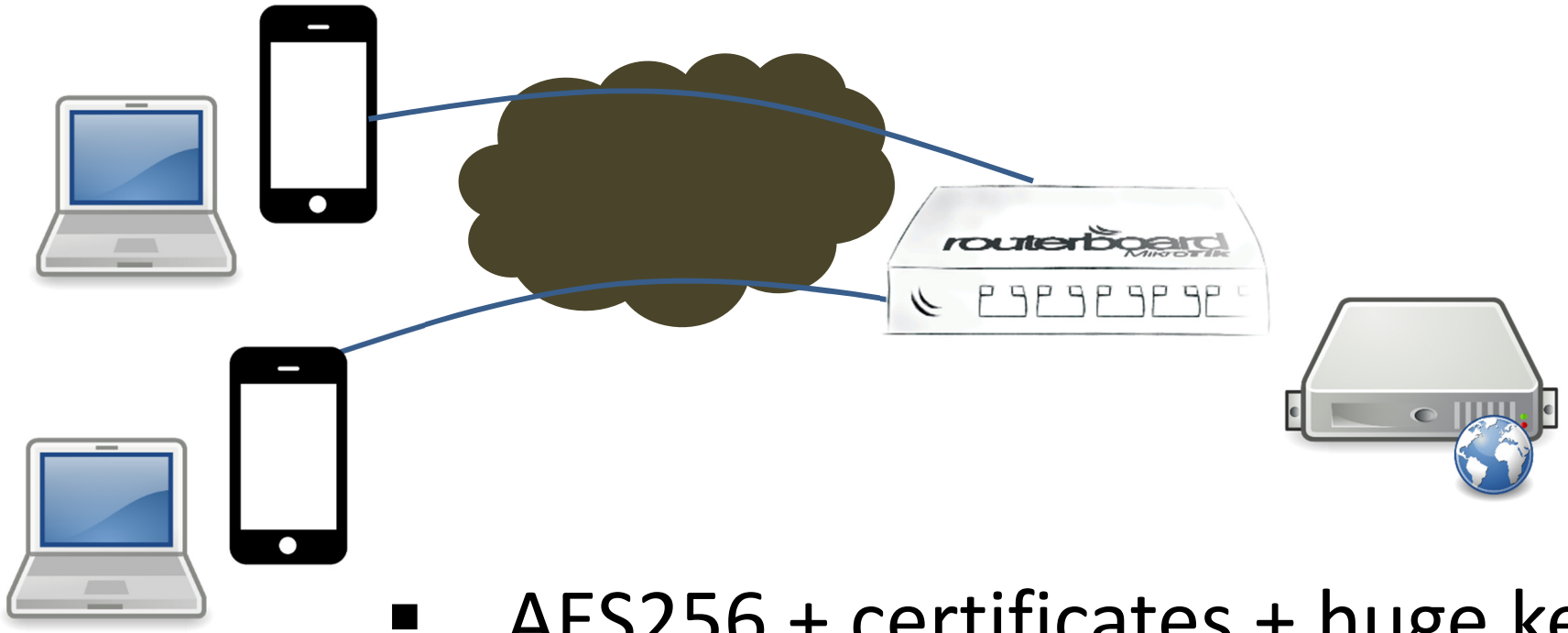


- Business requirements
- Partner requirements

Corporate connections



Serious encryption

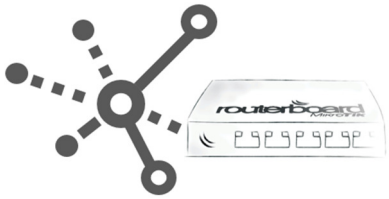


- AES256 + certificates + huge keys stored in safe hardware
- VPN over VPN

Critical functions

- Authentication
- Access control
- Confidentiality
- Data integrity

RouterOS VPN portfolio



PPPoE - Point-to-Point Protocol over Ethernet

PPTP – Point to Point Tunneling Protocol

L2TP - Layer 2 Tunneling Protocol

SSTP – Secure Socket Tunneling Protocol

OVPN – Open Source VPN

IPSEC - Internet Protocol Security

EoIP – Ethernet over IP

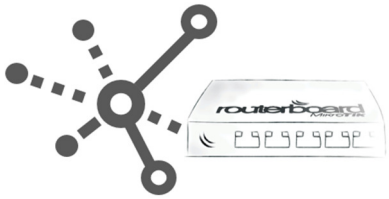
Does encryption still work?

Core cryptography elements:

- Algorithm
- Key (size)

Security is Only as Strong as the Weakest Link

Algoritms

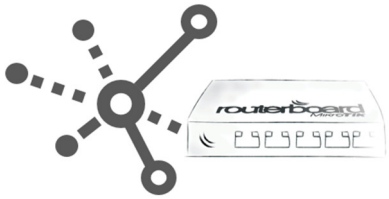


- **DES** (Data Encryption Standard) was once the standard crypto algorithm for encryption
- **MD5** has recently been found less secure than previously thought
- **RC4** (Rivest Cipher 4) - recent attacks :Royal Holloway, KU Leuven

AES (Advanced Encryption Standard) is the current preferred symmetric algorithm

IPSEC / SSTP between RouterOS / OVPN

Keys



Symmetric:
Key sizes of 128 bits (standard for SSL) are sufficient for most applications
Consider 256 bits for secure systems such as large financial transactions

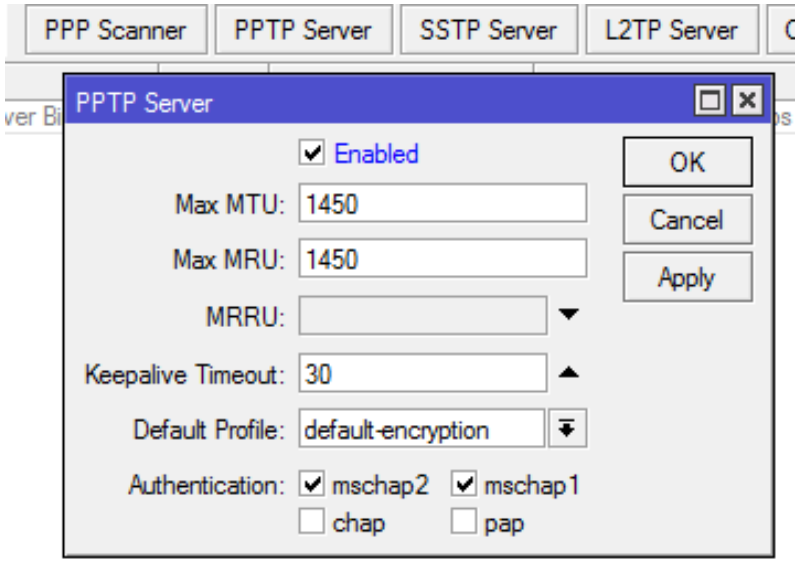
Symmetric-key encryption protocols should include message authentication

Asymmetric:
2048 bits should be considered for highly protected applications.
2048 / 4096 ?

Don’t use excessive key sizes unless you know you need them.

Point-to-Point Tunneling Protocol

PPTP is a available since the mid 1990s
requires /47 GRE and /6 TCP:1723



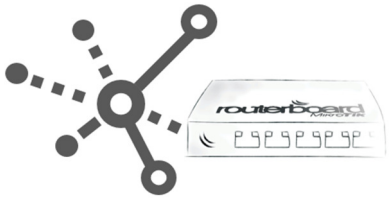
+ Pros

- client software on all platforms
- very easy to set up
- fast
- NAT friendly

- Cons

- not at all secure
- easy to block on firewalls

PPTP vulnerability



MPPE-128 encryption (which uses RC4 encryption with a 128bit key)

MITM attack to capture the handshake and any PPTP traffic after that offline crack of the handshake and derive the RC4 key

no forward secrecy - cracking one PPTP session is sufficient to crack all previous PPTP sessions using the same credentials.

https://github.com/moxie0/chapcrack

IP security (IPSec)

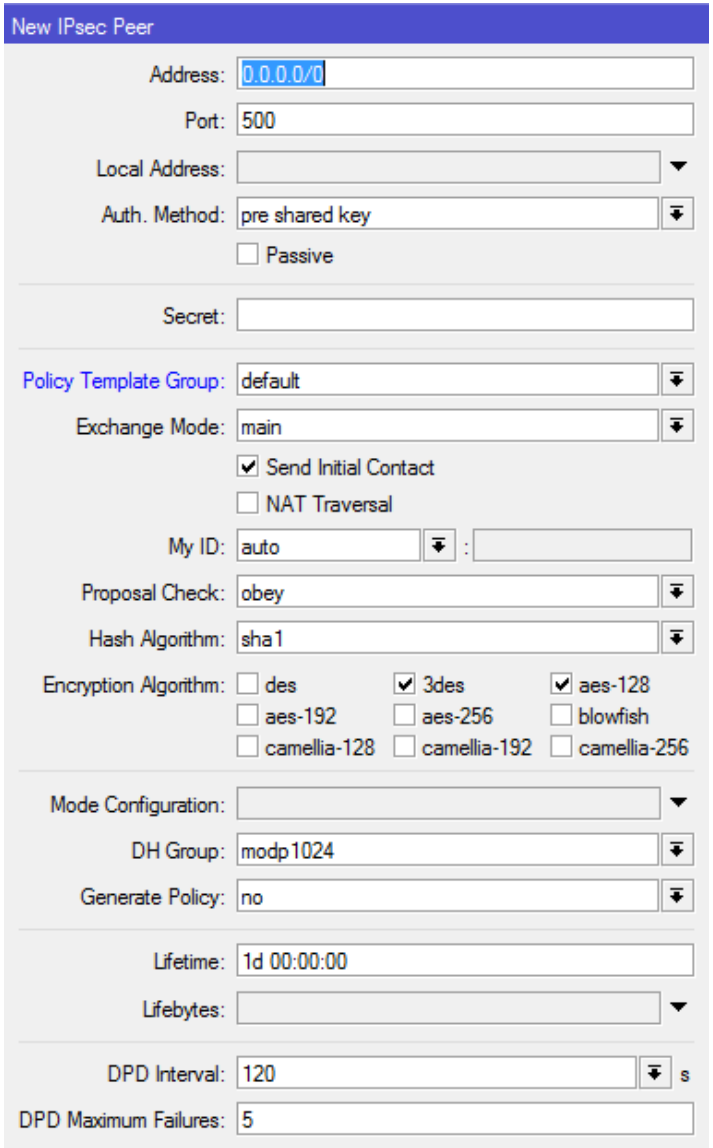
IPSec is set of encryption mechanisms,
two modes: transport/ tunnel
requires IKE /17 udp:500, ESP /50

+ Pros

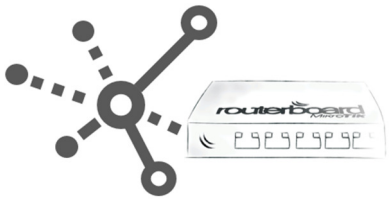
- considered very secure
- works together with other tunnels
- faster than OVPN/SSTP
- hardware support

- Cons

- struggle with restrictive firewalls
- problems with NAT
- complicated setup



L2TP/IPSec



The L2TP and IPsec protocols combine their best individual features to create a highly secure VPN client
requires IKE udp:500, ESP /50, udp:1701

+ Pros

- Clients in most modern OS
- faster than OVPN/SSTP
- Hardware support

- Cons

- struggle with restrictive firewalls
- larger overhead
- may be compromised by governments (unproven)

OpenVPN

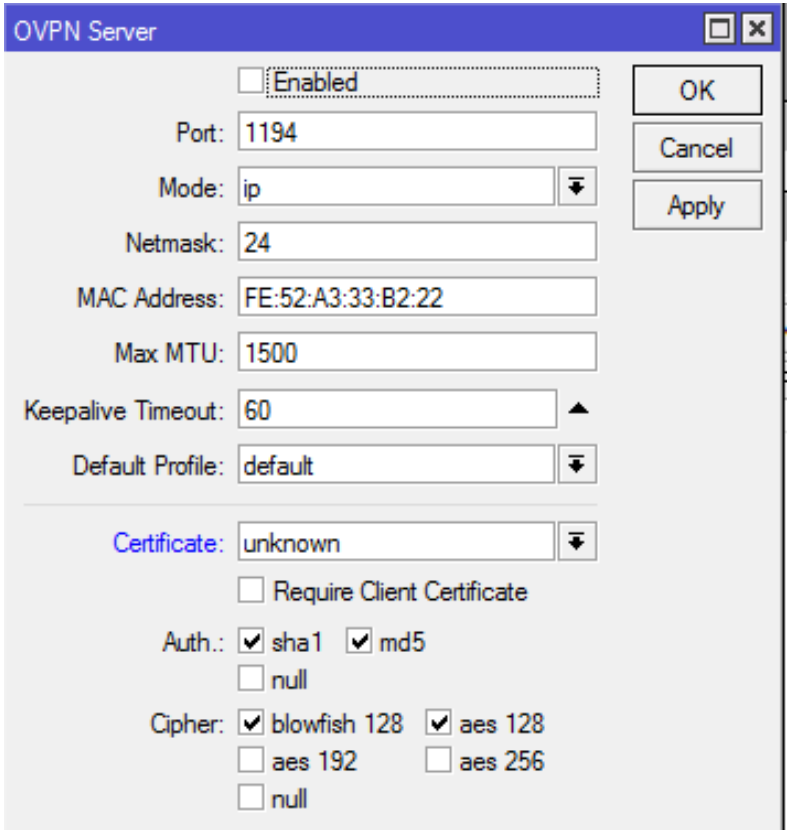
fairly new open source technology that uses the OpenSSL
requires tcp:1194 (can be changed)

+ Pros

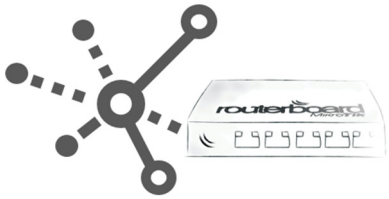
- Optional clients in most OS (OpenVPN Connect)
- Can bypass firewalls
- Open source
- NAT friendly

- Cons

- Needs third party software
- Certificates required



Secure Socket Tunneling Protocol



introduced by Microsoft in Windows Vista SP1, small chance to ever appear on Apple device. SSL v3 offers similar advantages to OpenVPN
requires tcp:443 (can be changed)

+ Pros

- very secure
- built-in client in MS Windows
- can bypass firewalls
- NAT friendly

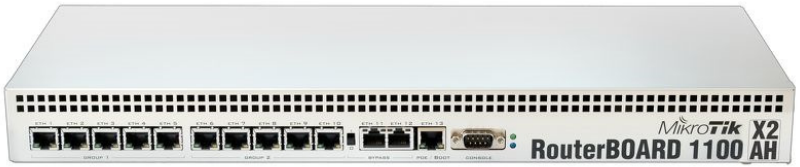
- Cons

- RouterOS <-> MS Windows can use only RC4
- Proprietary standard owned by Microsoft so cannot be independently audited for back doors and suchlike
- Overhead of PPP

VPN hardware acceleration

AES for IPSec, not for SSTP/OVPN

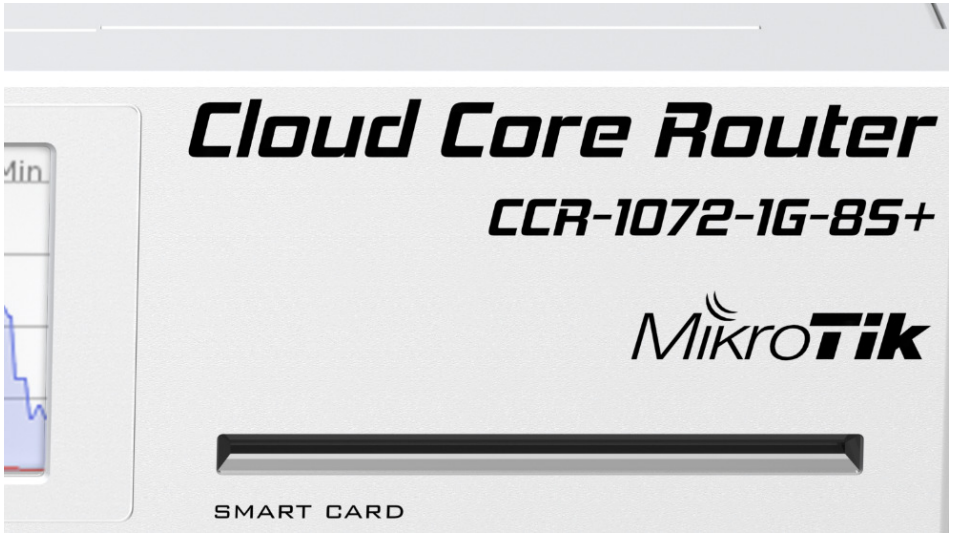
RB850



1100AHx2

Cloud Core Router (tile CPU family)

Smart Card slots



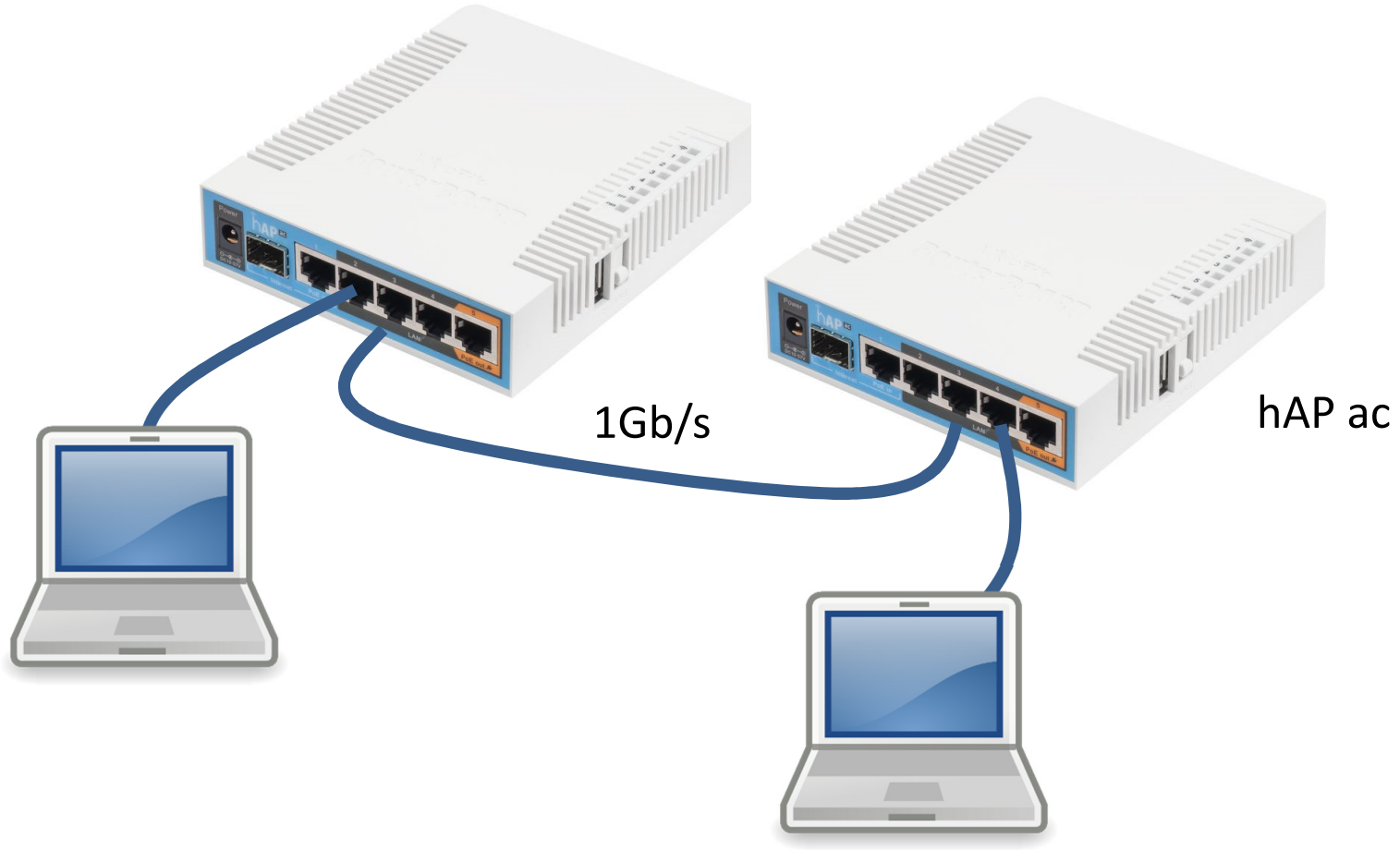
CCR 1072 – full size

CCR 1009 – sim factor

Tunnel characteristics

VPN type	Logical interface	Encrtiption	Authentication	Can be bridged
EoIP	+	-	-	+
IPIP	+	-	-	-
PPTP	+	+ MPPE128	-	with BCP
L2TP	+	+ MPPE128	-	with BCP
PPPoE	+	+ MPPE128	-	with BCP
SSTP	+	TLS (AES/RC4)	+ TLS	with BCP
OpenVPN	+	TLS (AES/BF)	+ TLS	with BCP
GRE	+	-	-	-
IPSec	-	+	+	-

Performance testbed



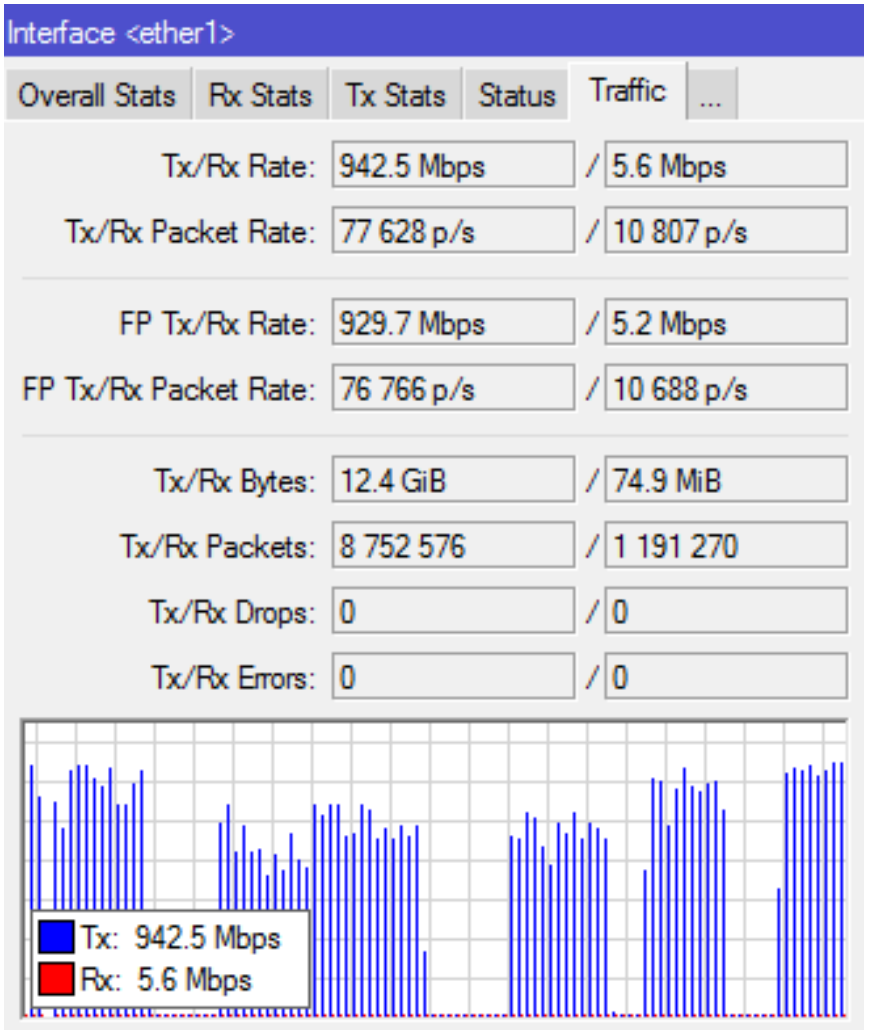
Testbed calibration

simple routing, no encryption, no fastpath

Transfer size: 1GB
Protocol: SMB3 over TCP

time: 9.938s
cpu ~ 35%

average bandwidth: 805 Mb/s
overhead: 4.3%

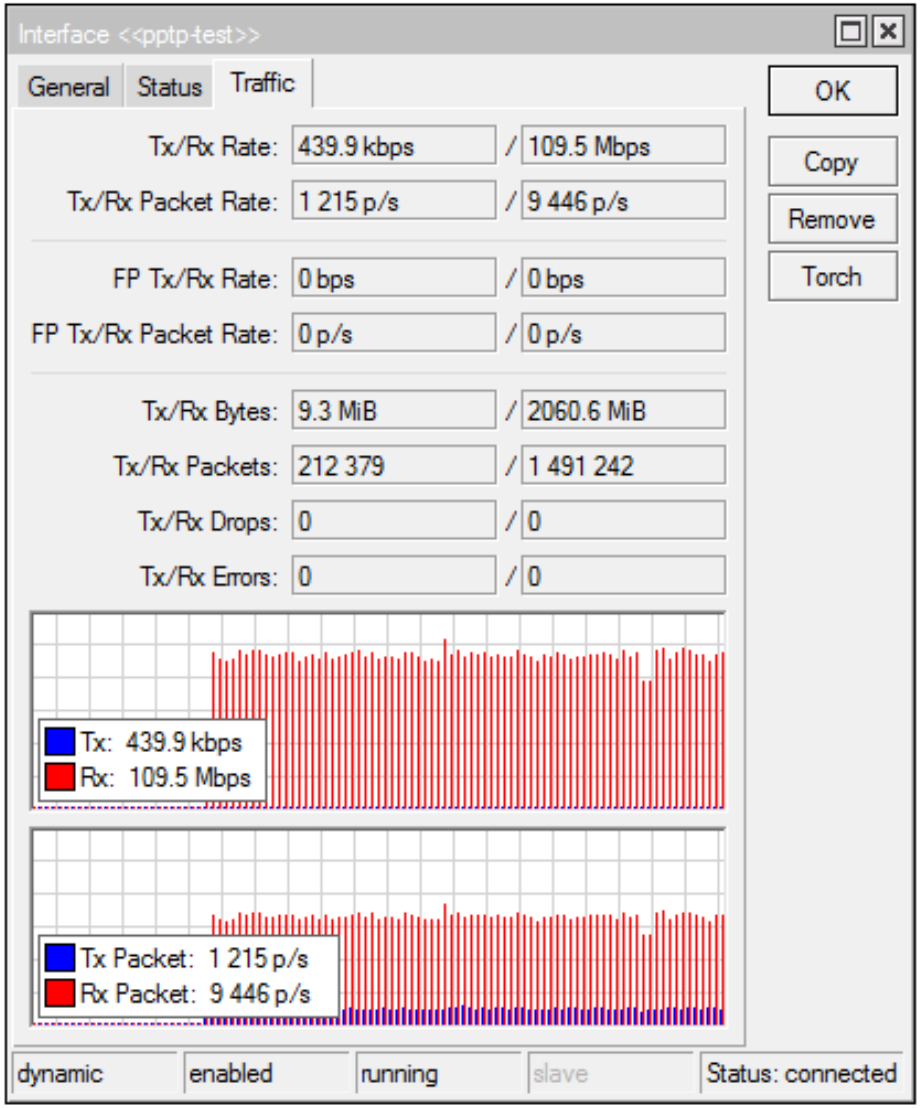


PPTP benchmark

PPTP, MPPE128 stateless

time: 9.938s
cpu ~ 99%

average bandwidth: 97.44 Mb/s
overhead: 7.2%



IPSec benchmark

Et...	Protocol	Src.	Dst.	VLAN Id	DSCP	Tx Rate	Rx Rate	Tx Pack...	Rx Pack
800 (ip)	50 (ipsec)	3.3.3.2	3.3.3.1			435.8 k...	48.4 Mbps	457	40
800 (ip)	6 (tcp)	2.2.2.9:445 (smb)	1.1.1.4:40457			0 bps	46.5 Mbps	0	40

IPSec, AES128 / SHA1 / pfs

time: 169.525s
cpu ~ 99%

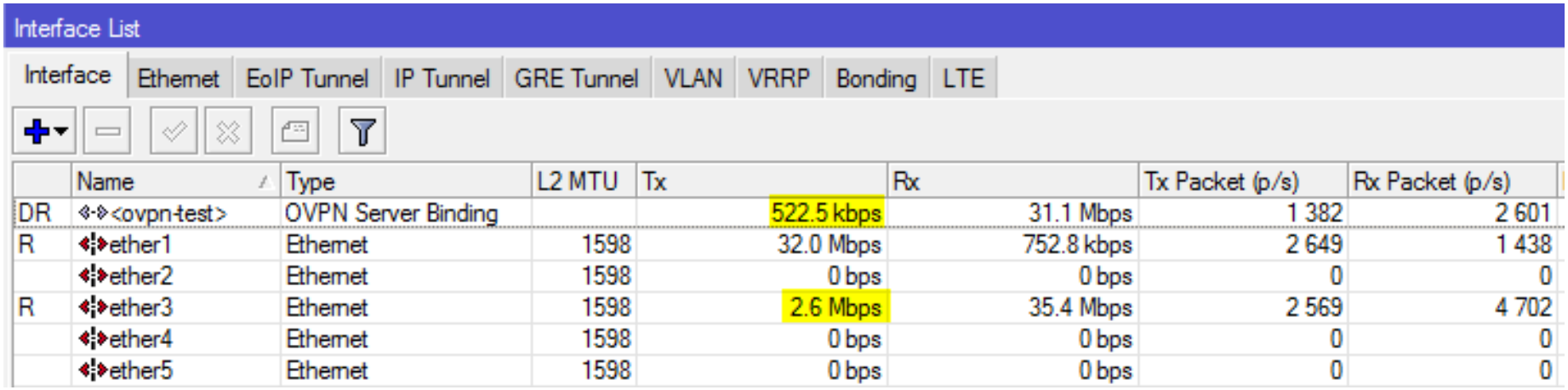
average bandwidth: 47.19 Mb/s
overhead: 8.3%

IPSec, AES256 / SHA1 / pfs

time: 203.436s
cpu ~ 99%

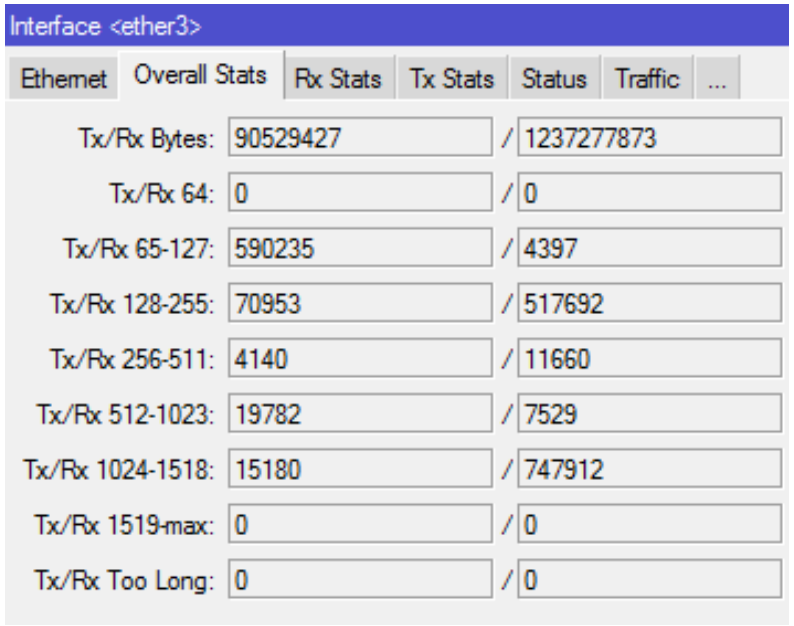
average bandwidth: 39.32 Mb/s
overhead: 8.3%

OVPN benchmark

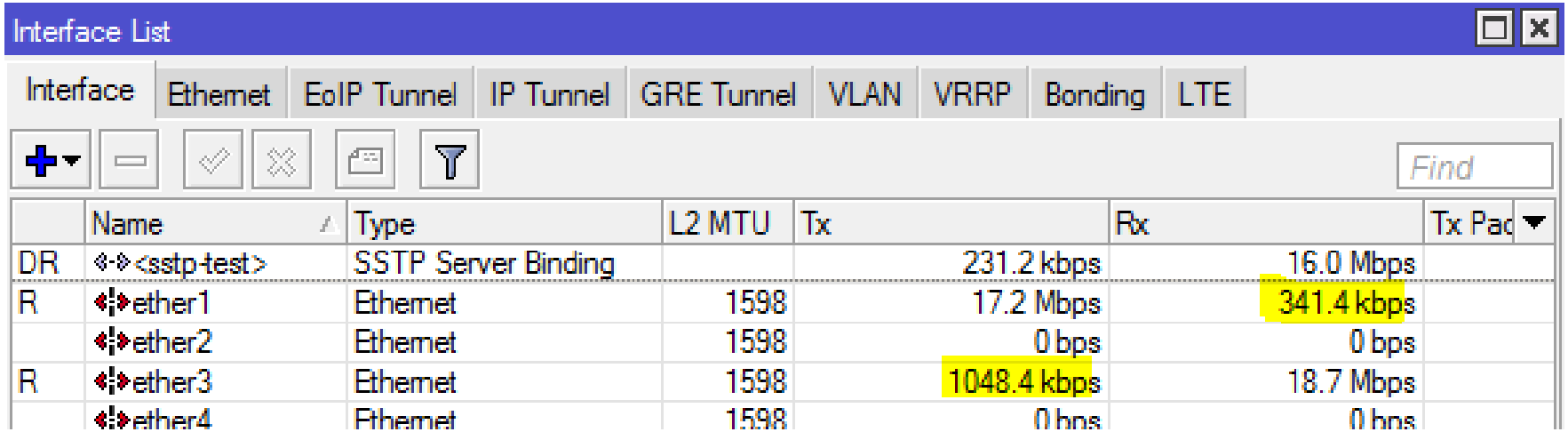


OVPN, AES-128-CBC/SHA1/ 2048 certificate
time: 325.66s
cpu ~ 65%
avarage bandwidth : 24.56 Mb/s

OVPN, AES-256-CBC/SHA1/ 2048 certificate
time: 357.94s
cpu ~ 70%
avarage bandwidth : 22.35 Mb/s
~15% overhead



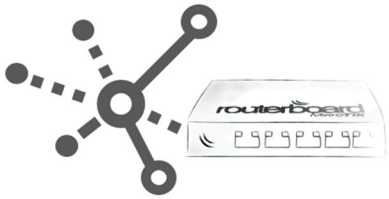
SSTP benchmark



SSTP, AES256-CBC (certificate/fps impact minimal)

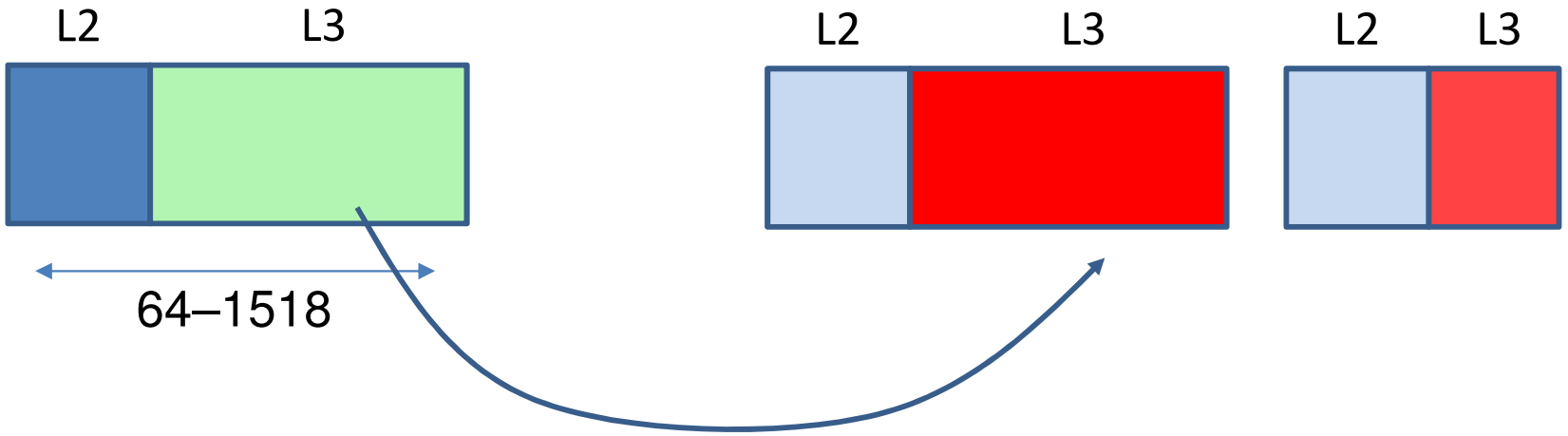
time: 533.887s
cpu ~ 50%
av.bandwidth : 15.00 Mb/s
overhead: 13%

Experimentation summary

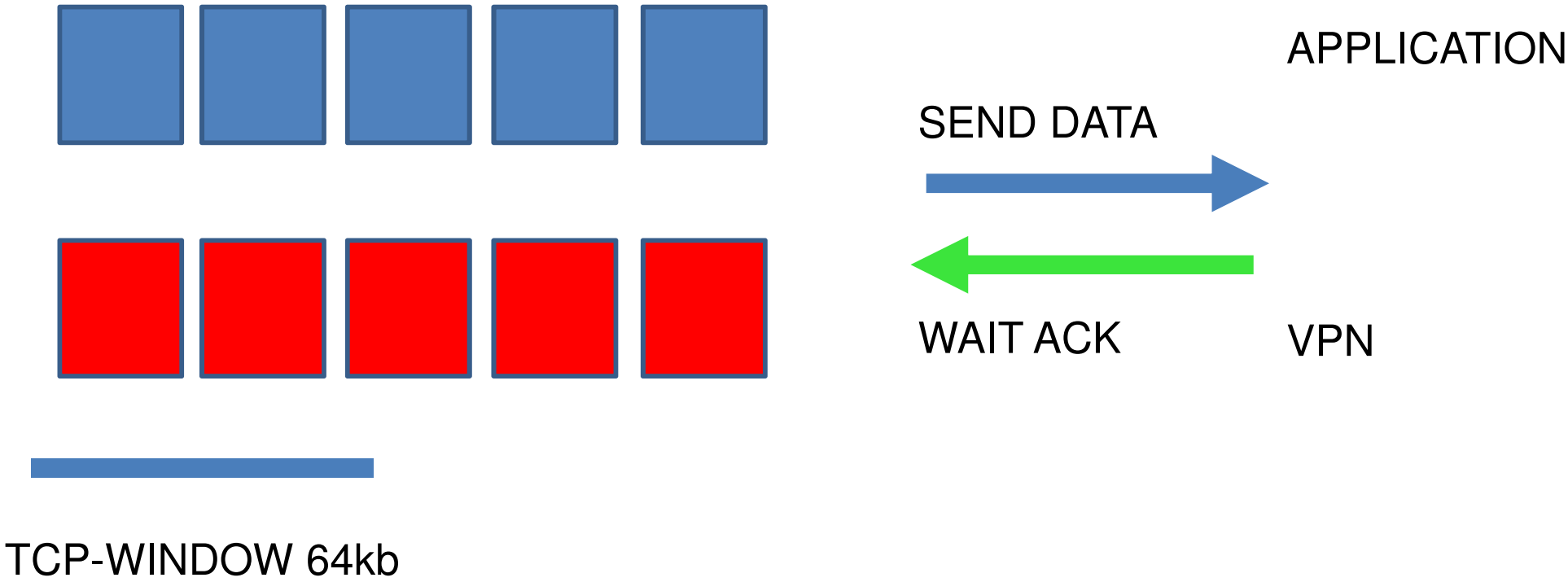


VPN	Measured Mb/s	Overhead	CPU
-	805	4.3%	35%
PPTP	97.5	7.2%	99%
IPSec	47	8.3%	99%
OVPN	25	15%	65%
SSTP	15	13%	50%

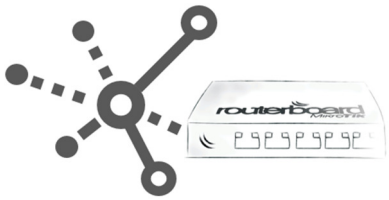
What happens to data packet



TCP over TCP problem



Conclusion – encryption works



- IPSEC – on CCR routers with routable IPs
- OVPN – primary choice for road warriors (its now time to switch from PPTP)
- SSTP – primary choice for MS Windows
- GRE-IPSEC to connect to Cisco

- Waiting for IKEv2

SXT-LTE IPv6

lmt

all IPv6 devices must support IPSec

SXT-LTE now can get IPv6 address.
This is a great potential for IPv6 VPNs in mobile world.

Thank You!