VPN and Tunnel concept with IP-in-IP tunnel configuration

Armenia MUM 2017

Presenter Information

Amin Hamidi Younessi

MikroTik Certified Trainer

: amin.younessi

: amin.younessi

: info@netrotik.com , aminyounessi@gmail.com

Presentation topics:

- Fundamentals of VPN technology.
- Benefits of Tunnels.
- Types of Tunnels.
- IP-in-IP configuration between MikroTik and Cisco Routers.

What is VPN?

- Virtual Private Network.
- VPN transmits data by means of tunneling.
- Both tunnel endpoints need to support the same protocol.
- Tunneling protocols are operate at either OSI layer 2 or layer3.

Benefits of Tunnels

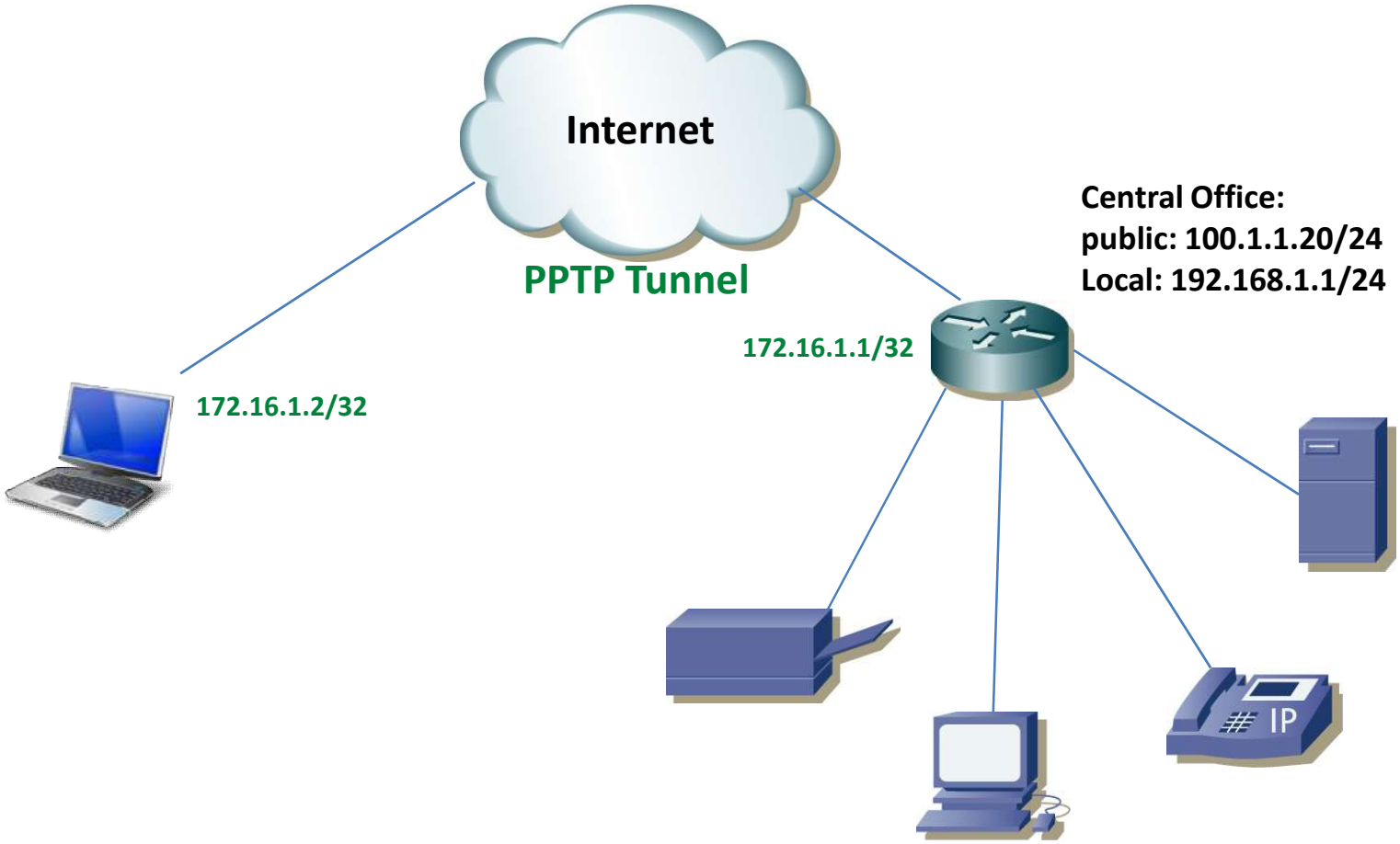
- Decrease cost.
- Scalability.
- Confidentiality.
- Authentication.
- Data Integrity.
- Anti-reply.

Two Main Types of Tunnels

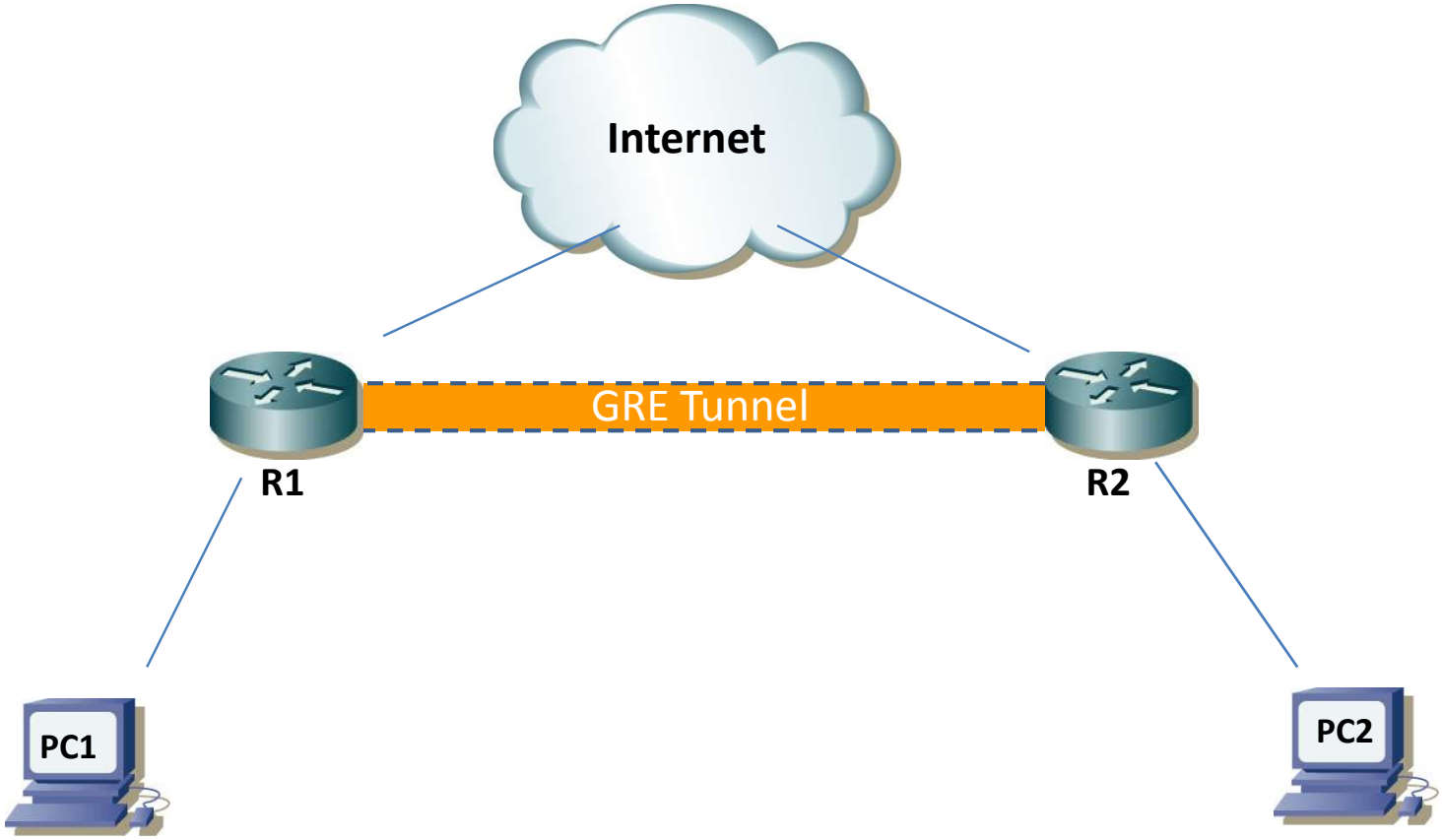
- Remote-access tunnels(as known as VPN)

- Site-to-site tunnels

Remote access sample



Site-to-site sample



Types of Tunnels:

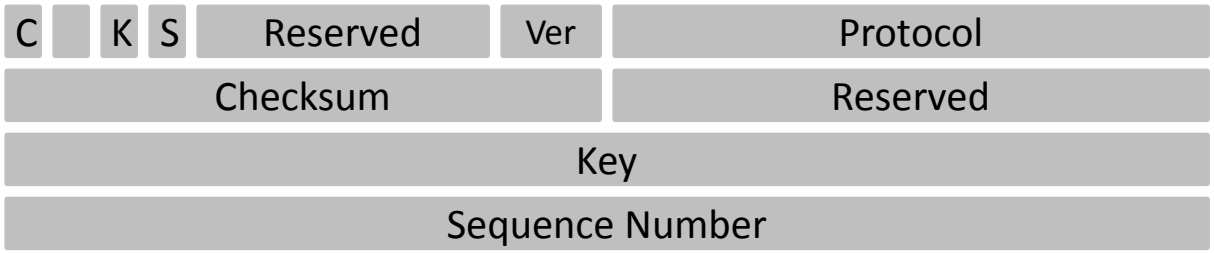
IPIP	GRE	EOIP	L2TP	PPTP
layer3 tunnel	layer 3 tunnel	layer 2 tunnel	layer 2 tunnel	layer2 tunnel
4 for ipv4 and 41 for ipv6	IP protocol number 47	IP protocol number 47	1701 UDP	1723 TCP

IP-in-IP Tunnel mechanism

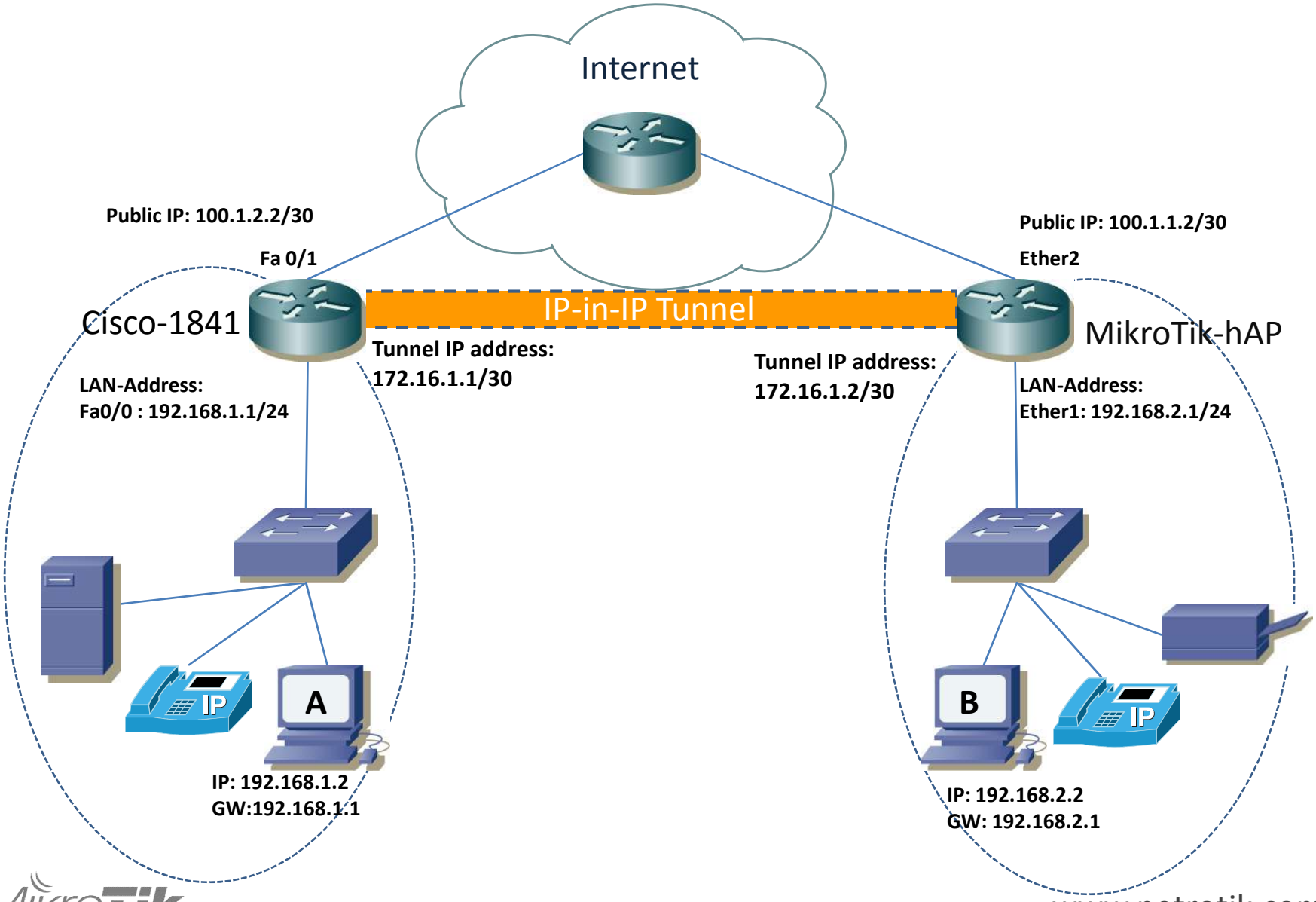
- The IPIP tunnel is a simple protocol that encapsulates IP packets in IP to make a tunnel between two routers.

GRE Tunnel mechanism

- The GRE header is variable in length, from 4 to 16 bytes, depending on which optional features have been enabled.



IP-in-IP tunnel Scenario



Steps:

- Configuring the IP addresses
  - MikroTik:

```
[admin@Mikrotik hAP] > ip address add address=192.168.2.1/24 interface=ether1 comment=LAN_ADDRESS
```

```
[admin@Mikrotik hAP] > ip address add address=100.1.1.2/30 interface=ether2 comment=WAN-ADDRESS
```

  - Cisco:

```
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly in
 duplex auto
 speed auto
end
```

```
interface FastEthernet0/1
 description R1<--->ISP
 ip address 100.1.2.2 255.255.255.252
 ip nat outside
 ip virtual-reassembly in
 duplex auto
 speed auto
end
```

- Add default route:
  - MikroTik:

```
[admin@Mikrotik hAP] > ip route add dst-address=0.0.0.0/0 gateway=100.1.1.1 comment="Default Route"
```

  - Cisco:

```
R1(config)#ip route
R1(config)#ip route 0.0.0.0 0.0.0.0 100.1.2.1
```

- Source NAT for direct clients to the internet
  - MikroTik :

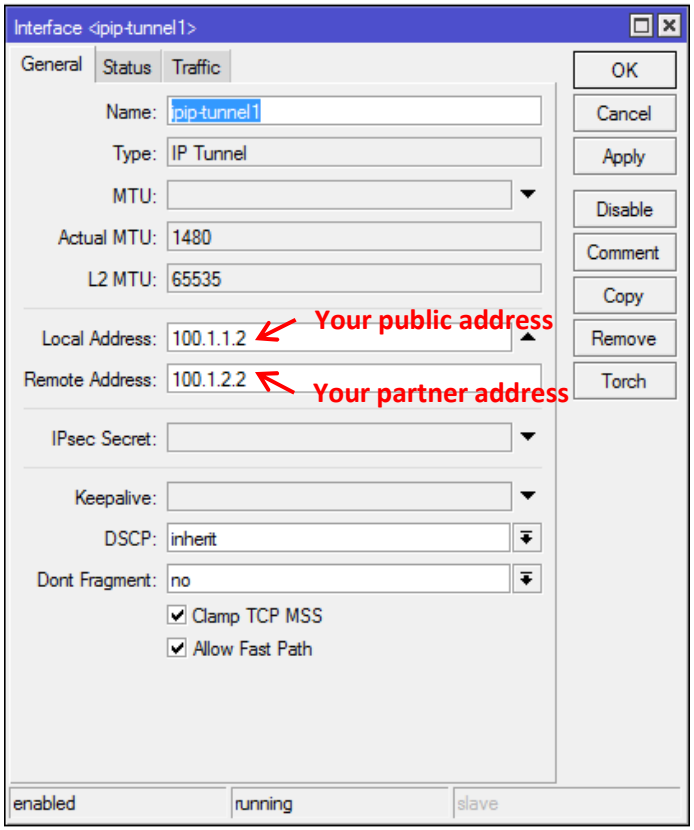
```
[admin@Mikrotik hAP] > ip firewall nat add chain=srcnat out-interface=ether2 action=src-nat to-addresses=100.1.1.2
```

  - Cisco

```
!
access-list 100 permit ip 192.168.1.0 0.0.0.255 any
!
```

```
R1(config)#
R1(config)#ip nat inside source list 100 interface FastEthernet0/1
```

- IPIP Tunnel configuration:

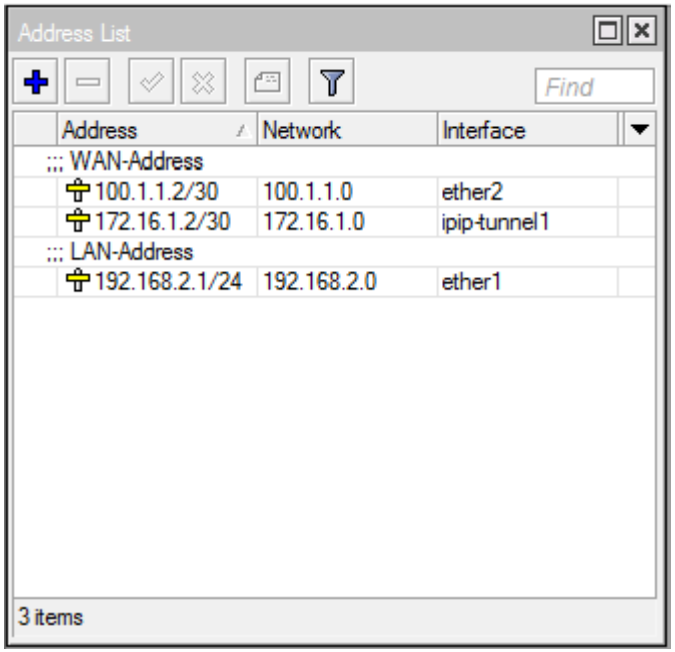



```
!
interface Tunnel100
 ip address 172.16.1.1 255.255.255.252
 tunnel source 100.1.2.2
 tunnel mode ipip
 tunnel destination 100.1.1.2
!
```

Your public address

Your partner address

- Setting IP address on tunnel interface




```
!
interface Tunnel100
 ip address 172.16.1.1 255.255.255.252
 tunnel source 100.1.2.2
 tunnel mode ipip
 tunnel destination 100.1.1.2
!
```

- Now it's time to verifying connections
  - ping pc A from pc B

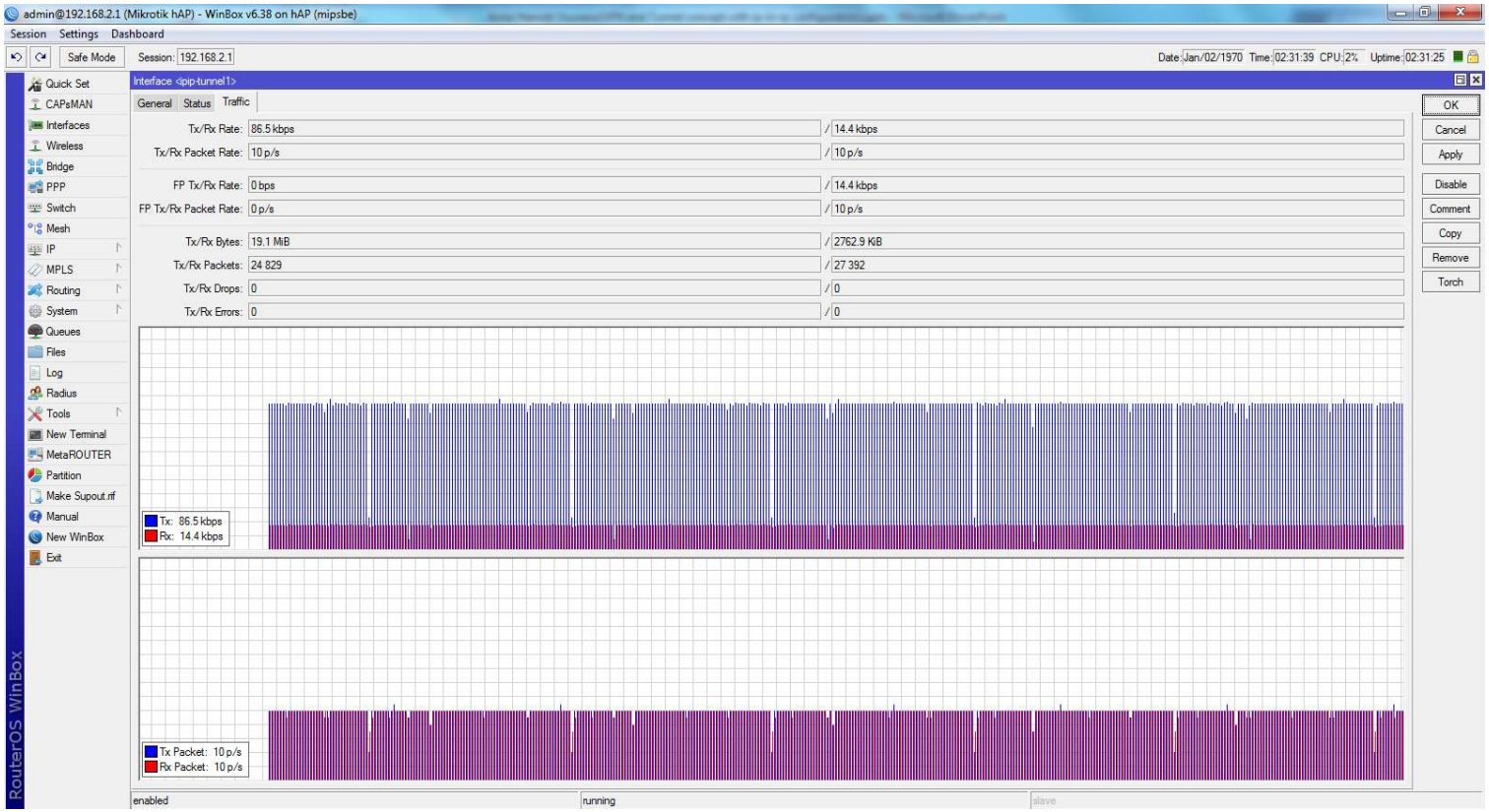
```
Administrator: C:\Windows\system32\cmd.exe - ping  192.168.2.2 -t

C:\Users\amin>ping 192.168.2.2 -t

Pinging 192.168.2.2 with 32 bytes of data:
Reply from 192.168.2.2: bytes=32 time=1ms TTL=126
Reply from 192.168.2.2: bytes=32 time=1ms TTL=126
Reply from 192.168.2.2: bytes=32 time=1ms TTL=126
Reply from 192.168.2.2: bytes=32 time=1ms TTL=126
Reply from 192.168.2.2: bytes=32 time=1ms TTL=126
Reply from 192.168.2.2: bytes=32 time=1ms TTL=126
Reply from 192.168.2.2: bytes=32 time=1ms TTL=126
Reply from 192.168.2.2: bytes=32 time=1ms TTL=126
Reply from 192.168.2.2: bytes=32 time=1ms TTL=126
Reply from 192.168.2.2: bytes=32 time=1ms TTL=126
Reply from 192.168.2.2: bytes=32 time=1ms TTL=126
```

  - Trace route result from pc B

```
C:\Users\amin>tracert -d 192.168.2.2

Tracing route to 192.168.2.2 over a maximum of 30 hops

  1     1 ms    <1 ms    <1 ms  192.168.1.1
  2     1 ms    <1 ms    <1 ms  172.16.1.2
  3     1 ms    <1 ms    <1 ms  192.168.2.2

Trace complete.
```

Other side of tunnel

- Look at Tunnel Traffic



Summary

There is an increasing demand nowadays to connect to internal networks from distant locations. Employees often need to connect to internal private networks over the Internet (which is by nature insecure) from home, hotels, airports or from other external networks. Security becomes a major consideration when staff or business partners have constant access to internal networks from insecure external locations.

VPN (Virtual Private Network) technology provides a way of protecting information being transmitted over the Internet, by allowing users to establish a virtual private “tunnel” to securely enter an internal network, accessing resources, data and communications via an insecure network such as the Internet.

Thank you