
SERTINET, C.A.
RIF: J-29920648-2

GRE OVER IPSEC CON ALTA DISPONIBILIDAD USANDO LOS PROTOCOLOS VRRP Y OSPF

SERTINET, C.A.
RIF: J-29920648-2

Ponente

Nelson López

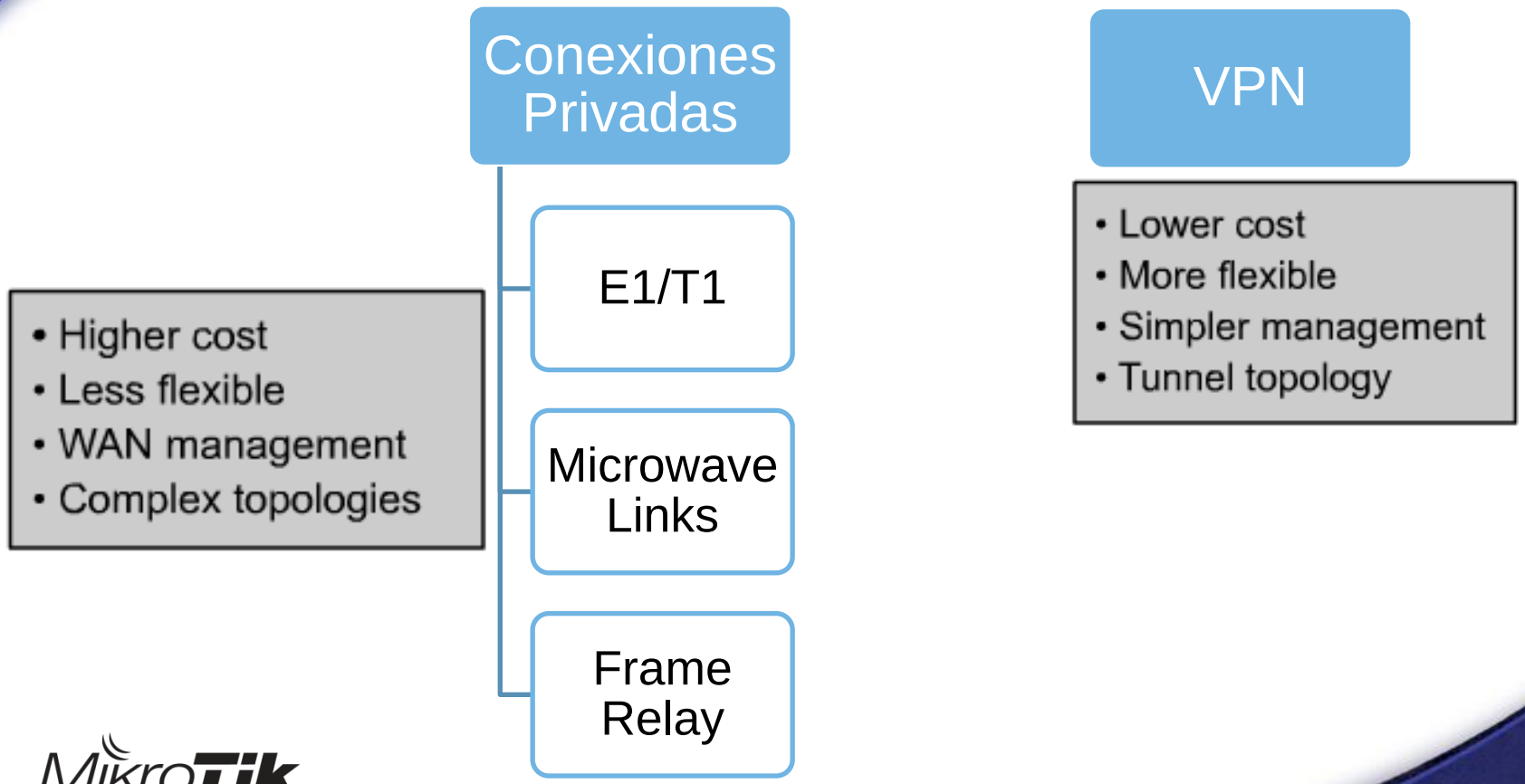
- País de origen : Venezuela
- Ingeniero de Telecomunicaciones
- CCNA, CCNA SECURITY
- MTCNA, MTCTCE
- 6 años de experiencia en Networking
- CEO / CTO de SERTINET, C.A

AGENDA

- Conceptos y tipos de VPN
- GRE (estructura, características, debilidades)
- IPSEC (conceptos, ISAKMP, Fases)
- Características de Alta Disponibilidad
- VRRP (concepto, características)
- Caso de éxito - Implementación
- Preguntas y Respuestas

MikroTik

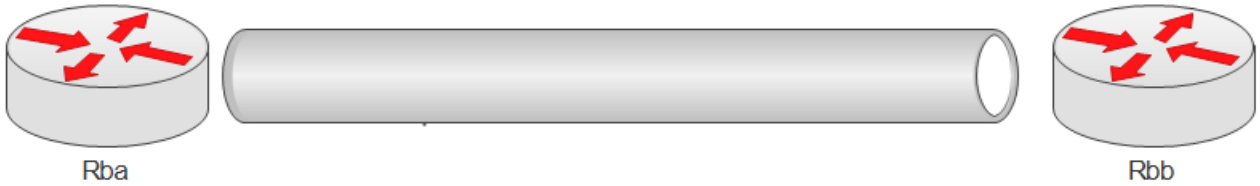
¿Cómo podemos conectar 2 Sucursales remotas?



MikroTik

¿Qué significa VPN?

VIRTUAL NETWORK → TUNNELING

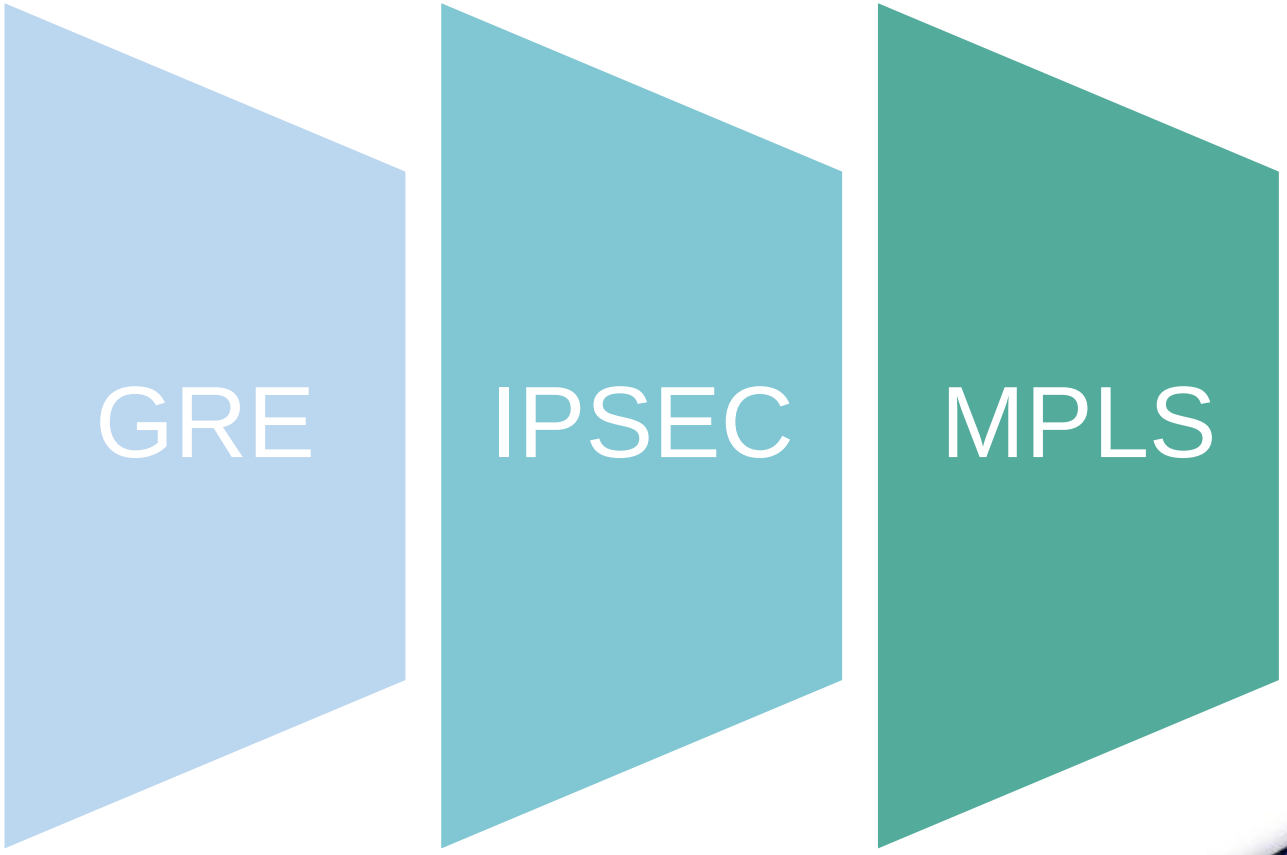


Virtual: Information within a private network is transported over a public network

PRIVATE NETWORK → ENCRYPTION

Private: The traffic is encrypted to keep the data confidential

Lawyer 3 VPN



MikroTik

Generic Routing Encapsulation (GRE)

Es un protocolo de túnel que fue originalmente desarrollado por Cisco. Se puede encapsular una amplia variedad de protocolos ha partir de la creación de un enlace virtual punto a punto.

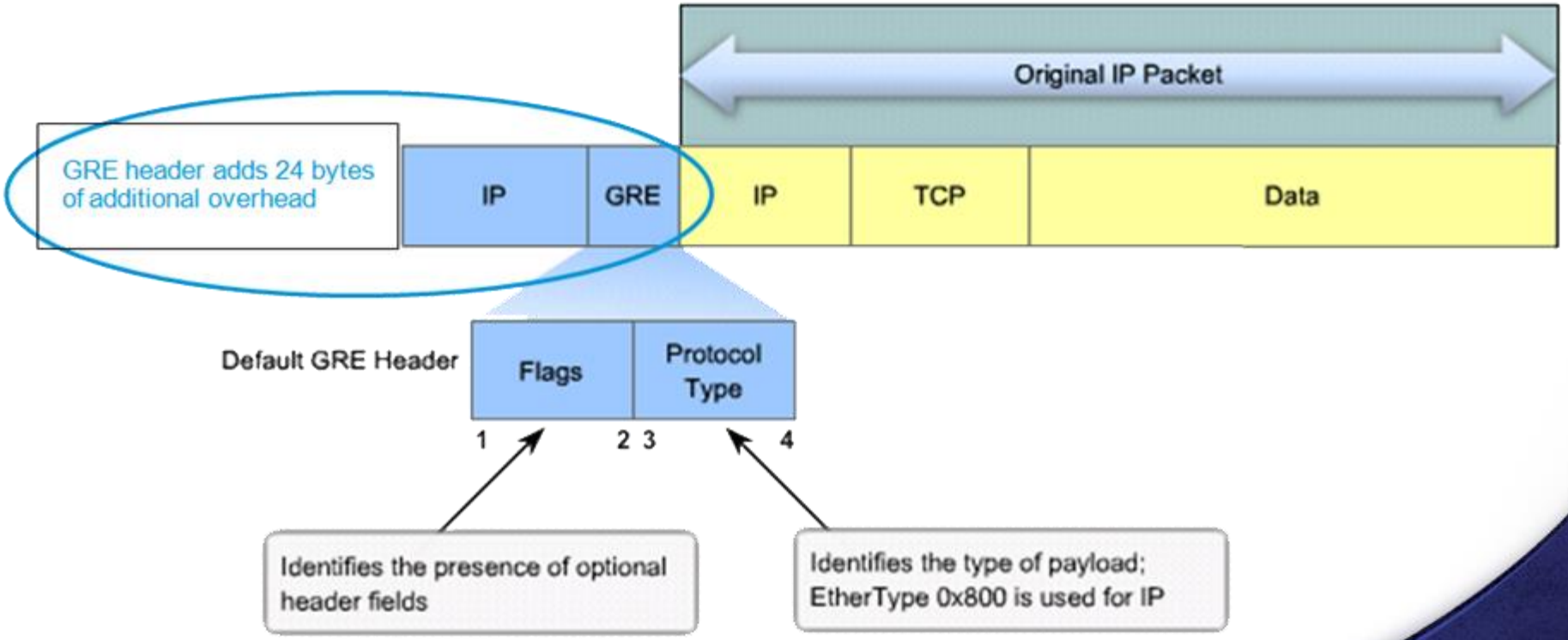
Sub-menu: /interface gre
Standards: GRE RFC 1701

GRE tunnel agrega 24 byte de Sobre Cabecera (4-byte gre header + 20-byte IP header).

GRE interface IP MTU es (1500-24) =**1476**.

MikroTik

Generic Routing Encapsulation (GRE)



MikroTik

GRE FRAGMENTACIÓN

DF (Don´t Fragment) bit (DF = 0)

1. 1500
2. 44 1476
3. 68 1500
4. Forward to GRE tunnel peer
5. De-capsulate GRE packets
6. Forward fragments to Host
7. Host reassembles data packet

Data packet (DF bit not set)

Fragment data packet

GRE encapsulate packets

68 1500

44 1476

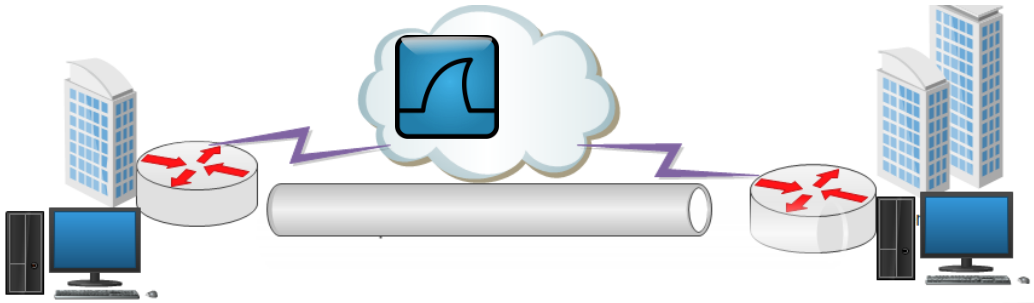
44 1476

1500

GRE DEBILIDADES

- GRE por si sólo no encrypta, la información
- Puede ser fácilmente monitoreado con un Sniffer como Wireshark.

```
102 148.834373000 192.168.1.10 192.168.2.10 SMB2 222 Ioctl Response FSCTL_PIPE_TRANSCEIVE File: MsFteWds
⊞ Frame 102: 222 bytes on wire (1776 bits), 222 bytes captured (1776 bits) on interface 0
⊞ Ethernet II, Src: CadmusCo_d4:b2:dd (08:00:27:d4:b2:dd), Dst: c4:01:1e:9c:00:00 (c4:01:1e:9c:00:00)
⊞ Internet Protocol Version 4, Src: 200.44.32.1 (200.44.32.1), Dst: 190.202.94.1 (190.202.94.1)
⊟ Generic Routing Encapsulation (IP)
  ⊞ Flags and Version: 0x0000
    Protocol Type: IP (0x0800)
⊞ Internet Protocol Version 4, Src: 192.168.1.10 (192.168.1.10), Dst: 192.168.2.10 (192.168.2.10)
⊞ Transmission Control Protocol, Src Port: 445 (445), Dst Port: 49159 (49159), Seq: 4177, Ack: 7264, Len: 144
⊞ NetBIOS Session Service
⊞ SMB2 (Server Message Block Protocol version 2)
```



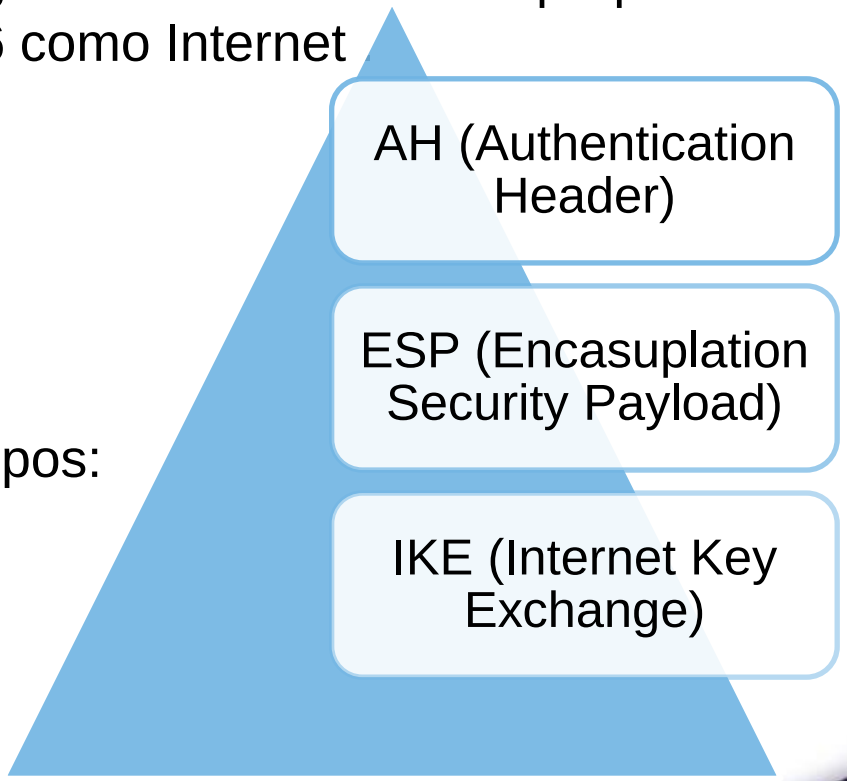
MikroTik

¿Cuándo deberías usar GRE ó IPSEC?

Internet Protocol Security (IPSEC)

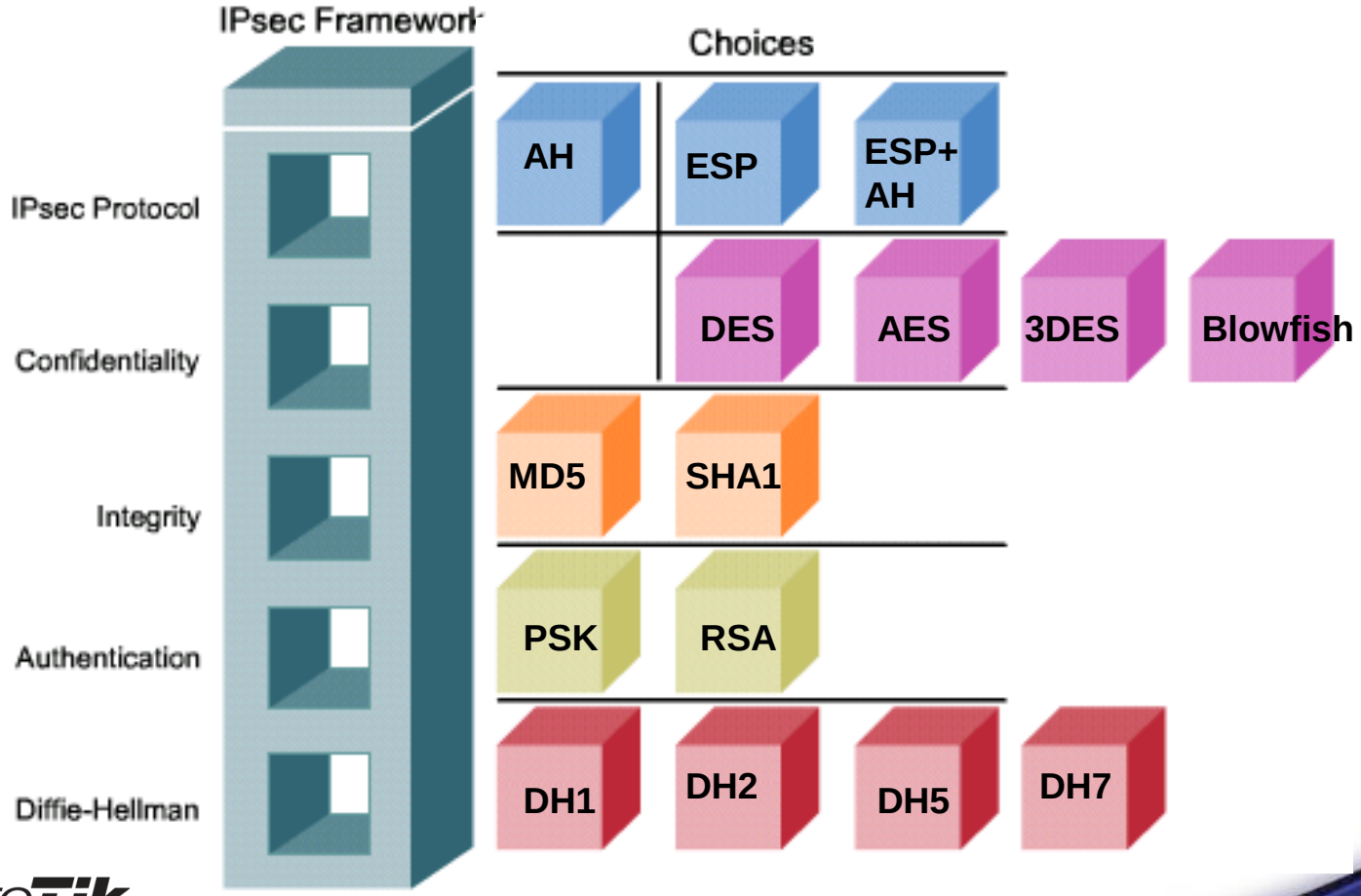
IPSEC es un conjunto de protocolos definidos por la Internet Engineering Task Force (IETF) para asegurar el intercambio de paquetes a través de redes sin protección IP / IPv6 como Internet .

Mikrotik divide IPSEC in 3 Grupos:



MikroTik

IPSEC Framework



MikroTik

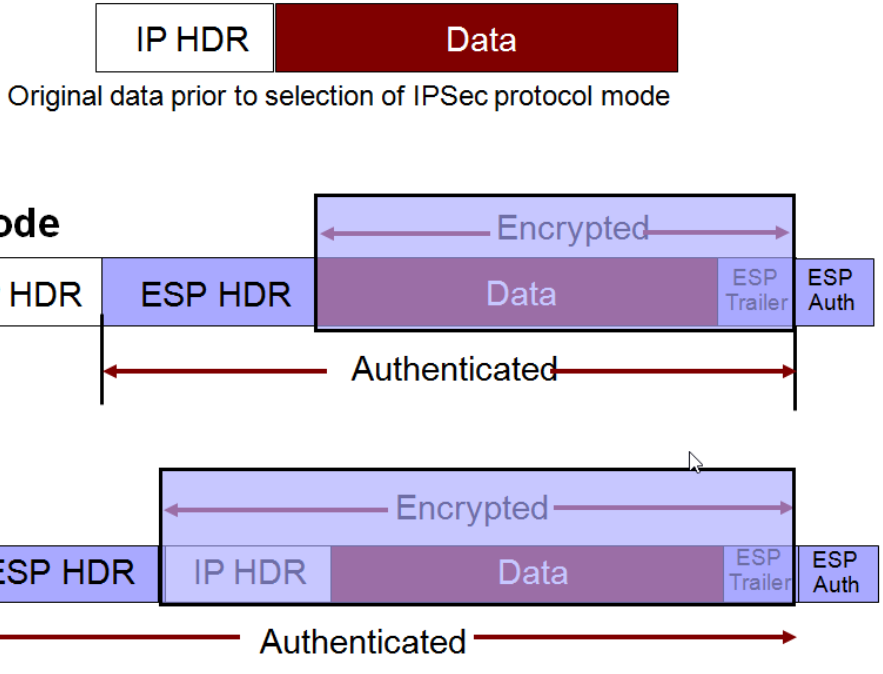
Encapsulating Security Payload (ESP)

Transport mode

Normalmente sólo se utiliza, cuando otro protocolo de túnel (Ejemplo GRE) para encapsular primero el paquete de datos IP, IPSec se utiliza para proteger los paquetes del túnel GRE.

Tunnel mode:

El modo de túnel se usa con redes privadas virtuales (VPN) , donde los hosts de una red protegida envían paquetes a hosts en una red protegida diferente a través de un par de compañeros de IPsec



Internet Key Exchange Protocol (IKE)

Phase1

- Authentication Method
- DH Group
- Encryption Algorithm
- Hash Algoritm
- NAT-T
- DPD &Lifetime (Optional)

Está fase cada opción debe ser igual en Ambos Peers

Phase2

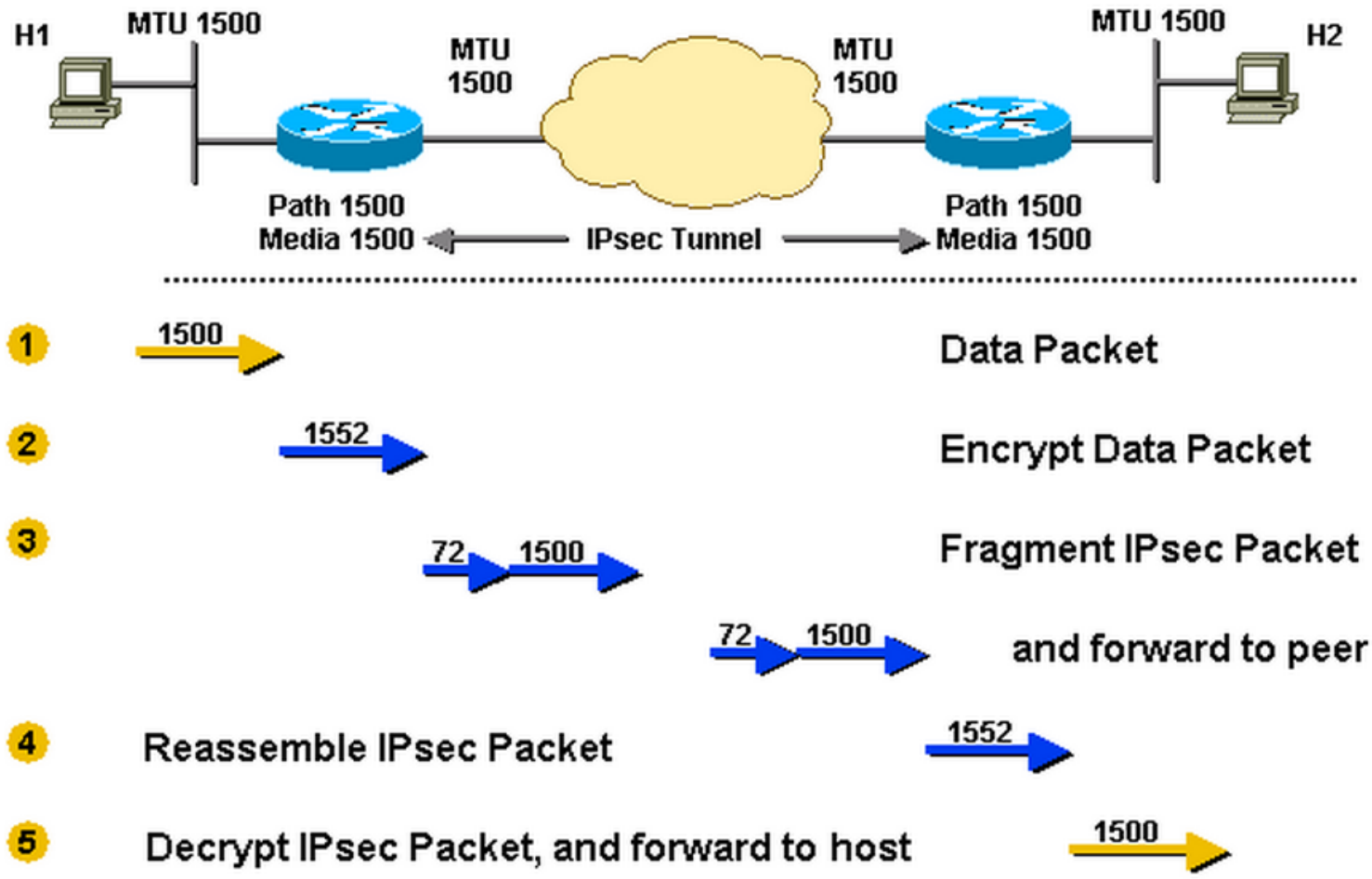
- Ipsec Protocol
- Mode (Tunnel /Transport)
- Authentication Method
- PFS (DH)
- Lifetime

Está fase cada opción debe ser igual en Ambos Peers

MikroTik

IPSEC FRAGMENTACIÓN

OverHead 52 – 58 Bytes (Encapsulating Security Payload (ESP) and ESP authentication (ESPauth)) per packet.



GRE OVER IPSEC

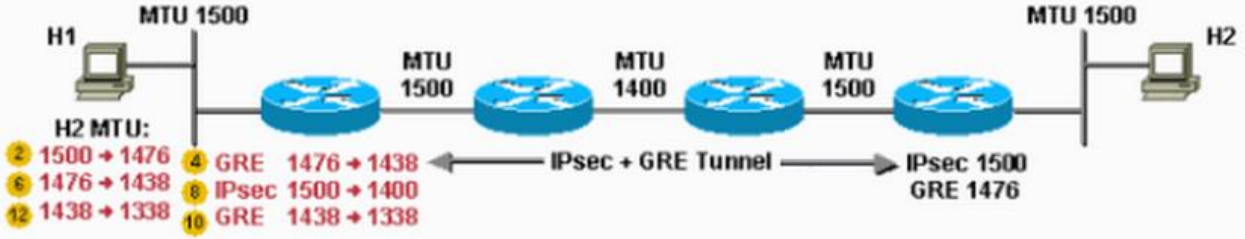
Original Payload (IP +Data)

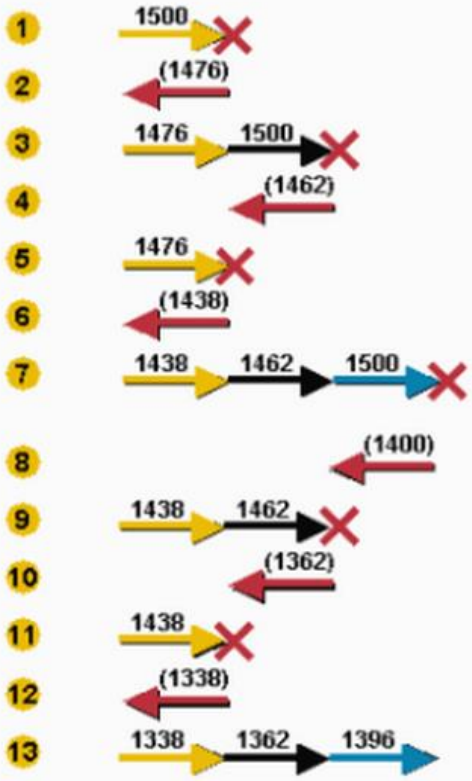
| GRE | Original Payload |

ESP | Encrypt (GRE | Original Payload |)

Tunnel Combination	Specific MTU Needed	Recommended MTU
GRE + IPsec (Transport mode)	1440 bytes	1400 bytes
GRE + IPsec (Tunnel mode)	1420 bytes	1400 bytes

GRE OVER IPSEC FRAGMENTACIÓN





1. Data Packet dropped by GRE
2. ICMP Error to Host (code=3, type=4)
3. Data Packet; GRE Packet dropped by IPsec
4. ICMP Error to GRE
5. Data Packet dropped by GRE
6. ICMP Error to Host
7. Data Packet; GRE Packet; IPsec Packet dropped by Intermediate router
8. ICMP Error to IPsec
9. Data Packet; GRE Packet dropped by IPsec
10. ICMP Error to GRE
11. Data Packet dropped by GRE
12. ICMP Error to Host
13. Data Packet; GRE Packet; IPsec Packet finally gets through

/ip ipsec peer

GRE OVER IPSEC FRAGMENTACIÓN

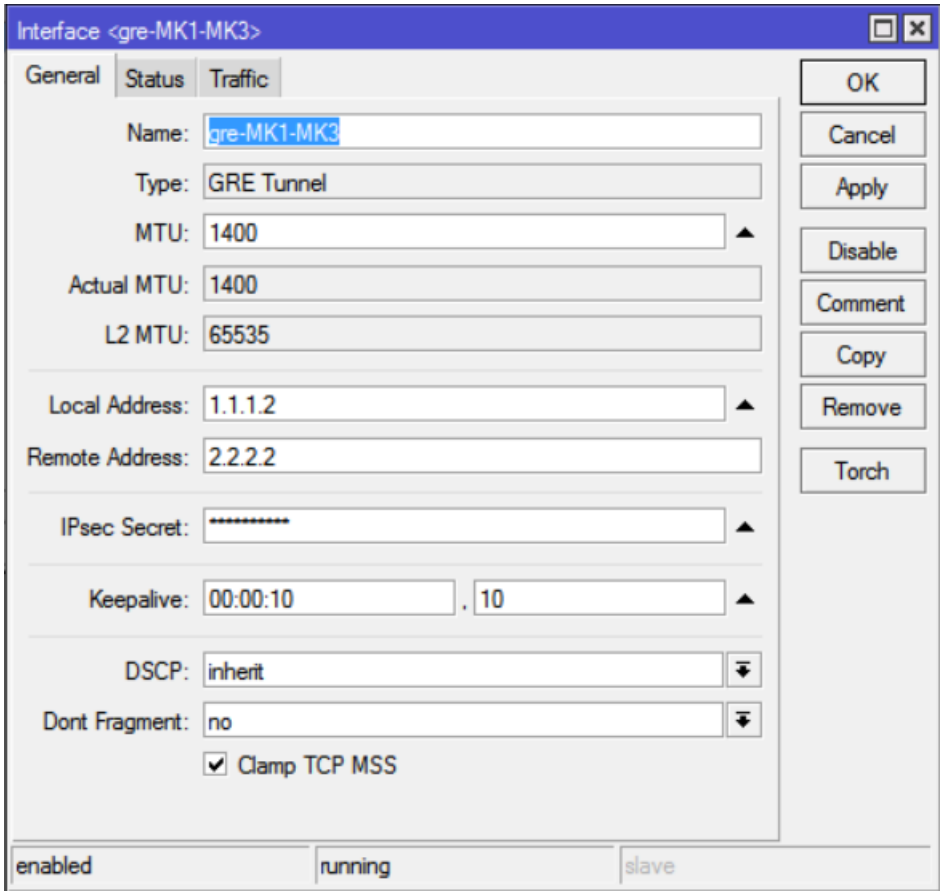
Packet Sniffer Packets

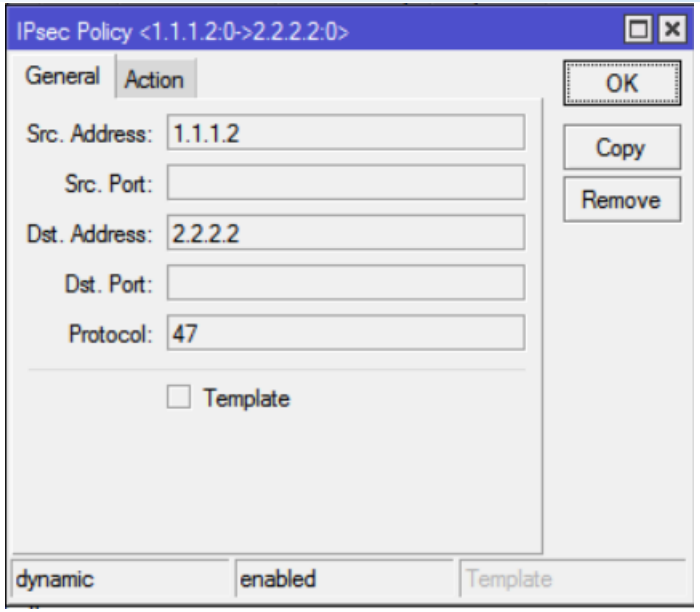
MTU

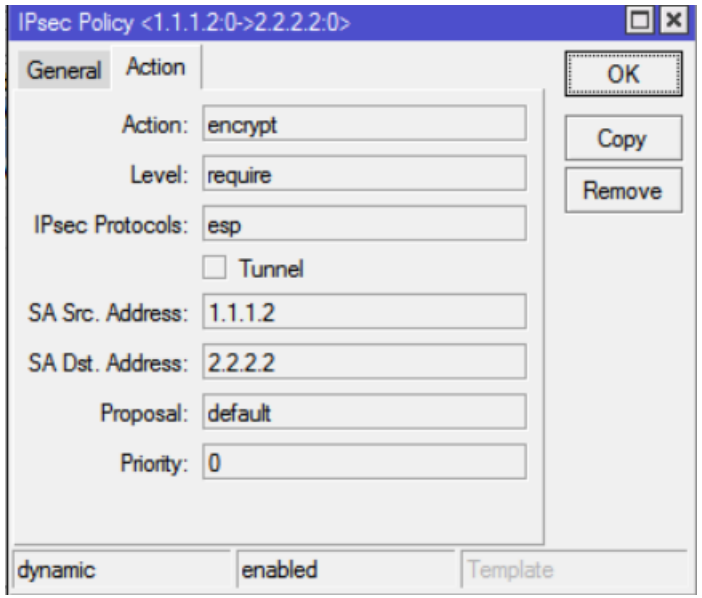
Find

Time...	Interface	Direction	Src. Address	Src. Port	Dst. Address	Dst. Port	Prot...	IP Protocol	Size
0.814	gre-MK1-MK3	tx	10.82.16.100		10.82.20.100		204...	1 (icmp)	1396
0.814	gre-MK1-MK3	tx	10.82.16.100		10.82.20.100		204...	1 (icmp)	1396
0.814	gre-MK1-MK3	tx	10.82.16.100		10.82.20.100		204...	1 (icmp)	1396
0.814	gre-MK1-MK3	tx	10.82.16.100		10.82.20.100		204...	1 (icmp)	1396
0.815	gre-MK1-MK3	tx	10.82.16.100		10.82.20.100		204...	1 (icmp)	1396
0.815	gre-MK1-MK3	tx	10.82.16.100		10.82.20.100		204...	1 (icmp)	1396
0.815	gre-MK1-MK3	tx	10.82.16.100		10.82.20.100		204...	1 (icmp)	1396
0.815	gre-MK1-MK3	tx	10.82.16.100		10.82.20.100		204...	1 (icmp)	1396
0.815	gre-MK1-MK3	tx	10.82.16.100		10.82.20.100		204...	1 (icmp)	1396
0.815	gre-MK1-MK3	tx	10.82.16.100		10.82.20.100		204...	1 (icmp)	1396
0.815	gre-MK1-MK3	tx	10.82.16.100		10.82.20.100		204...	1 (icmp)	1396
0.816	gre-MK1-MK3	tx	10.82.16.100		10.82.20.100		204...	1 (icmp)	1396
0.816	gre-MK1-MK3	tx	10.82.16.100		10.82.20.100		204...	1 (icmp)	1396
0.816	gre-MK1-MK3	tx	10.82.16.100		10.82.20.100		204...	1 (icmp)	1396
0.816	gre-MK1-MK3	tx	10.82.16.100		10.82.20.100		204...	1 (icmp)	1396
0.816	gre-MK1-MK3	tx	10.82.16.100		10.82.20.100		204...	1 (icmp)	1396
0.816	gre-MK1-MK3	tx	10.82.16.100		10.82.20.100		204...	1 (icmp)	1396
0.817	gre-MK1-MK3	tx	10.82.16.100		10.82.20.100		204...	1 (icmp)	636
0.840	gre-MK1-MK3	rx	10.82.20.100		10.82.16.100		204...	1 (icmp)	1396
0.840	gre-MK1-MK3	rx	10.82.20.100		10.82.16.100		204...	1 (icmp)	1396
0.840	gre-MK1-MK3	rx	10.82.20.100		10.82.16.100		204...	1 (icmp)	1396
0.840	gre-MK1-MK3	rx	10.82.20.100		10.82.16.100		204...	1 (icmp)	1396
0.840	gre-MK1-MK3	rx	10.82.20.100		10.82.16.100		204...	1 (icmp)	1396
0.840	gre-MK1-MK3	rx	10.82.20.100		10.82.16.100		204...	1 (icmp)	1396

GRE OVER IPSEC CONFIGURACION

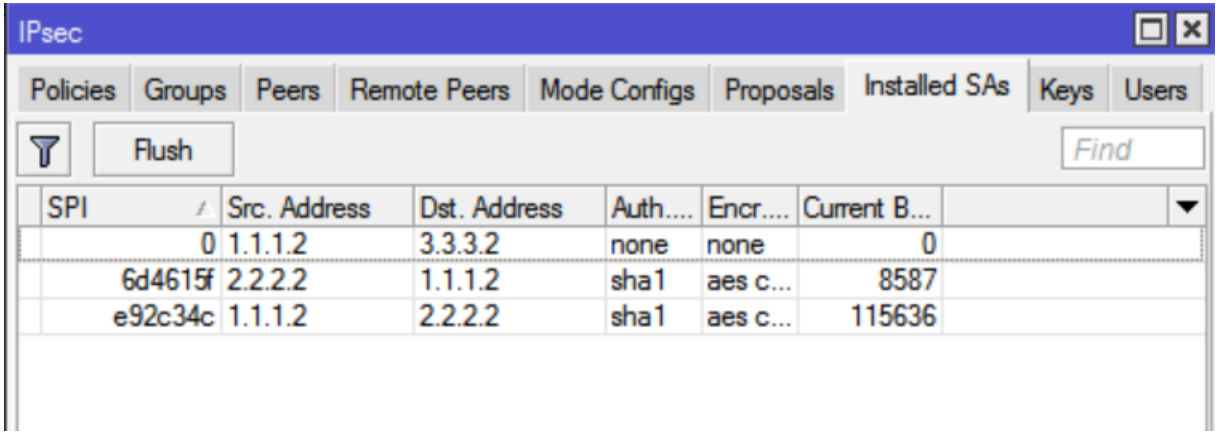






GRE OVER IPSEC CONFIGURACION

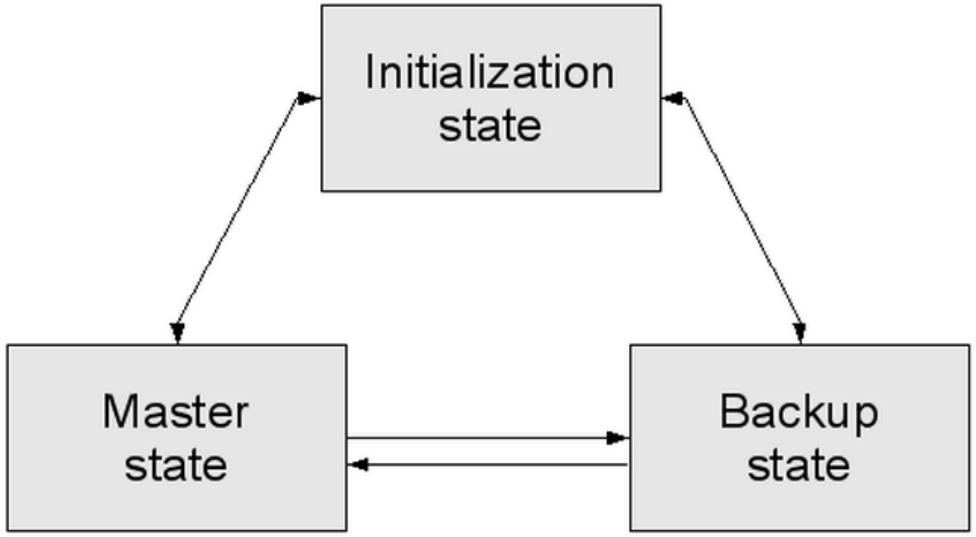
```
[admin@MK1] > ip ipsec peer print
Flags: X - disabled, D - dynamic
 0  D ;;; gre-MK1-MK3
      address=2.2.2.2/32 local-address=1.1.1.2 passive=no port=500
      auth-method=pre-shared-key secret="warcry1986" generate-policy=no
      policy-template-group=default exchange-mode=main send-initial-contact=yes
      nat-traversal=yes proposal-check=obey hash-algorithm=sha1
      enc-algorithm=3des,aes-128 dh-group=modp1024 lifetime=1d lifebytes=0
      dpd-interval=2m dpd-maximum-failures=5

 1  D ;;; gre-MK1-MK4
      address=3.3.3.2/32 local-address=1.1.1.2 passive=no port=500
      auth-method=pre-shared-key secret="warcry1986" generate-policy=no
      policy-template-group=default exchange-mode=main send-initial-contact=yes
      nat-traversal=yes proposal-check=obey hash-algorithm=sha1
      enc-algorithm=3des,aes-128 dh-group=modp1024 lifetime=1d lifebytes=0
      dpd-interval=2m dpd-maximum-failures=5
```



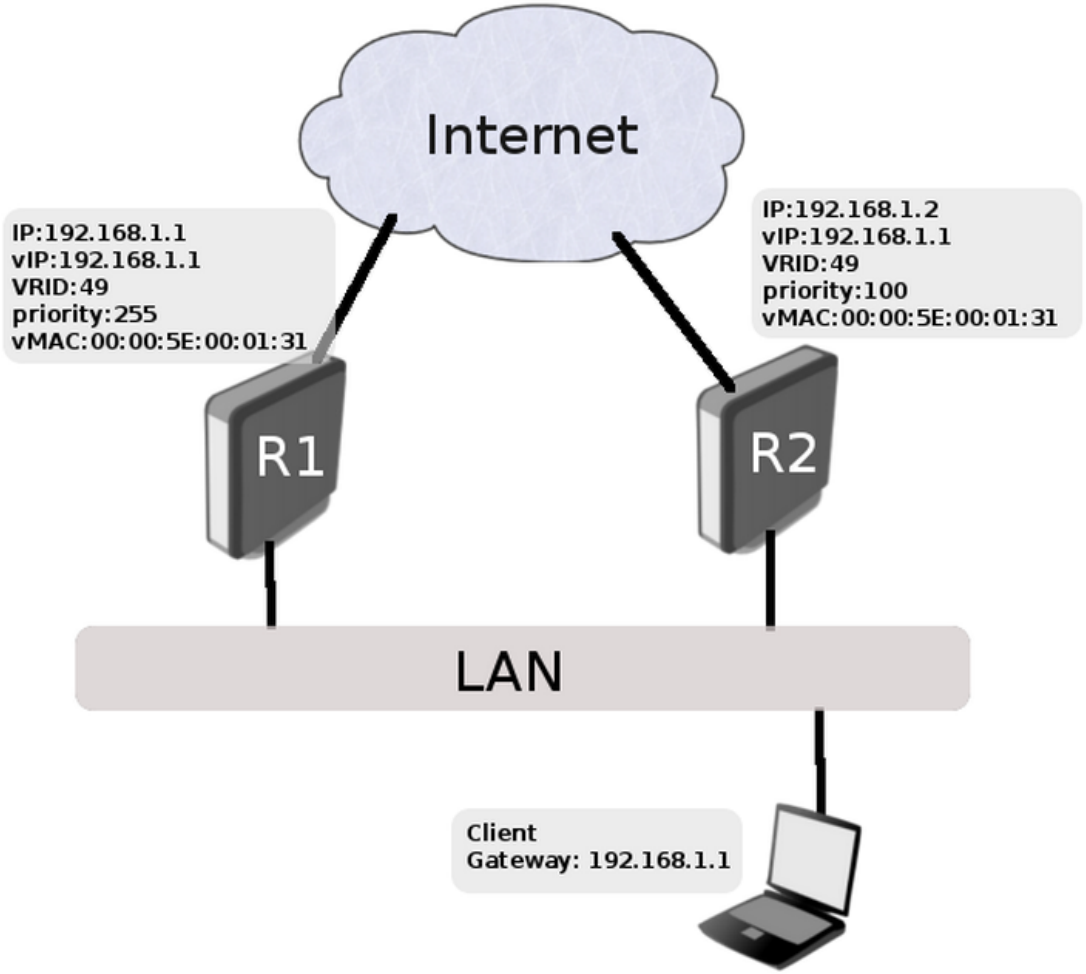
ALTA DISPONIBILIDAD

Virtual Router Redundancy Protocol (VRRP)

Es un protocolo de redundancia no propietario definido en el RFC 3768 diseñado para aumentar la disponibilidad de la puerta de enlace por defecto dando servicio a máquinas en la misma subred. El aumento de fiabilidad se consigue mediante el anuncio de un router virtual como una puerta de enlace por defecto en lugar de un router físico.



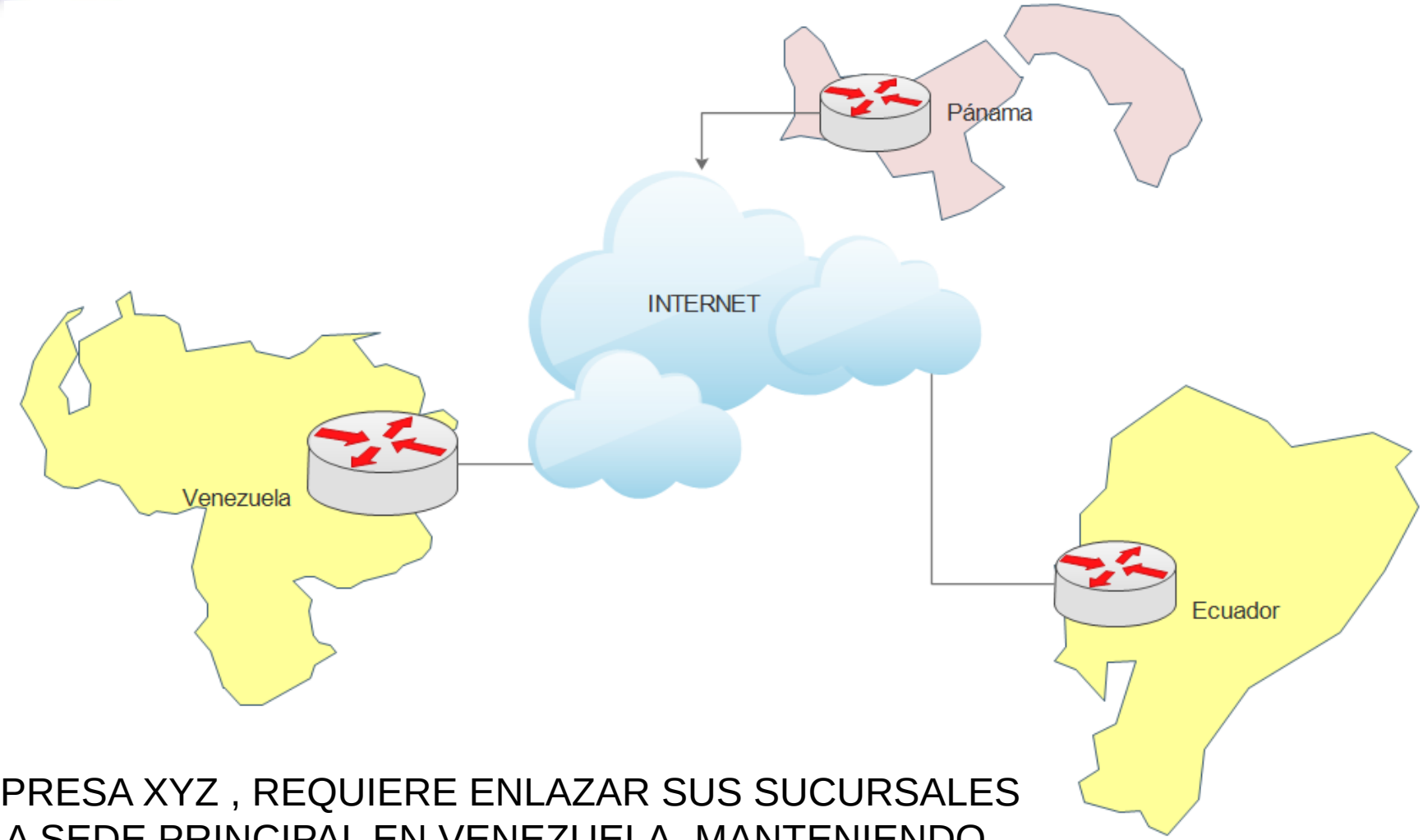
Virtual Router Redundancy Protocol (VRRP)



Soportado por distintas Marcas de Tecnología

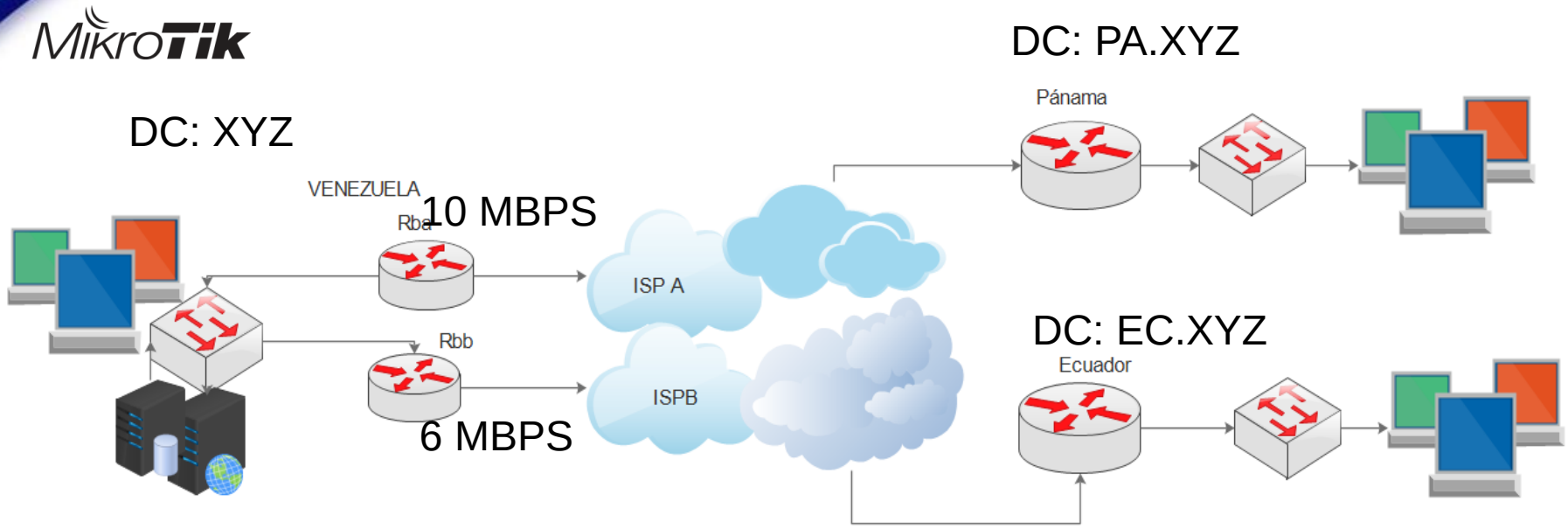
Tiempo detección de Falla de 3 Segundos.

ESCENARIO



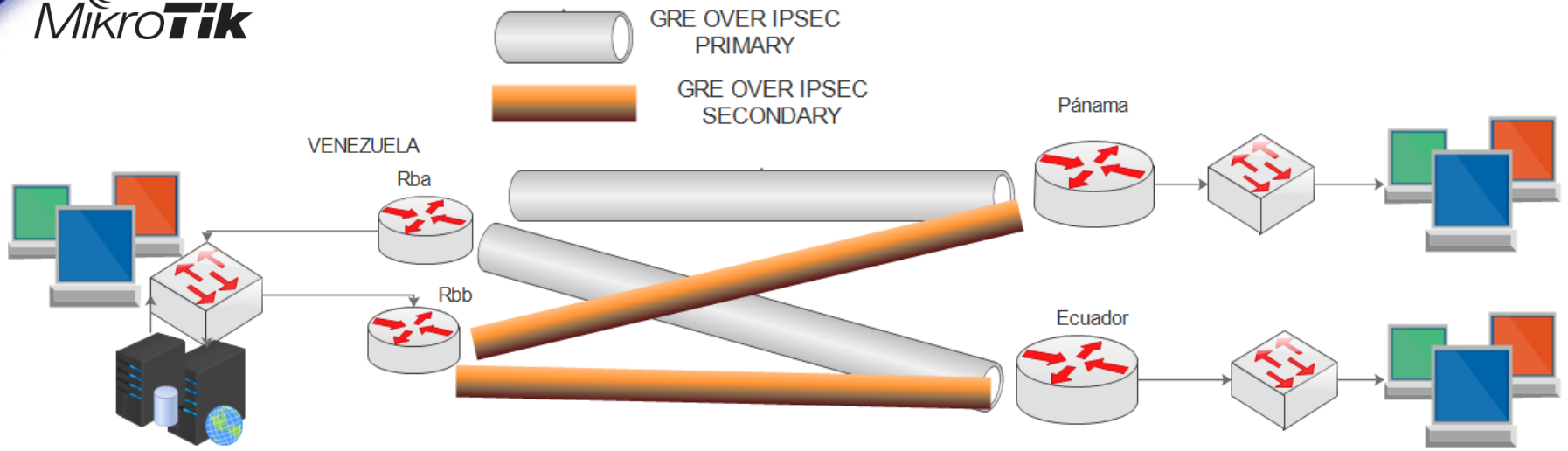
LA EMPRESA XYZ , REQUIERE ENLAZAR SUS SUCURSALES CON LA SEDE PRINCIPAL EN VENEZUELA, MANTENIENDO CONECTIVIDAD A LOS SERVICIOS Y SEGURIDAD EN LA DATA EN MOVIMIENTO.

SOLUCIÓN PLANTEADA



- GRE OVER IPSEC , PARA FUTURO CRECIMIENTO
- OSPF COMO PROTOCOLO DE ENRUTAMIENTO
- ESTRUCTURA DE LA RED
- ALTA DISPONIBILIDAD EN EL GATEWAY PARA VENEZUELA
- TOPOLOGÍA HUB AND SPOKE

SOLUCIÓN PLANTEADA



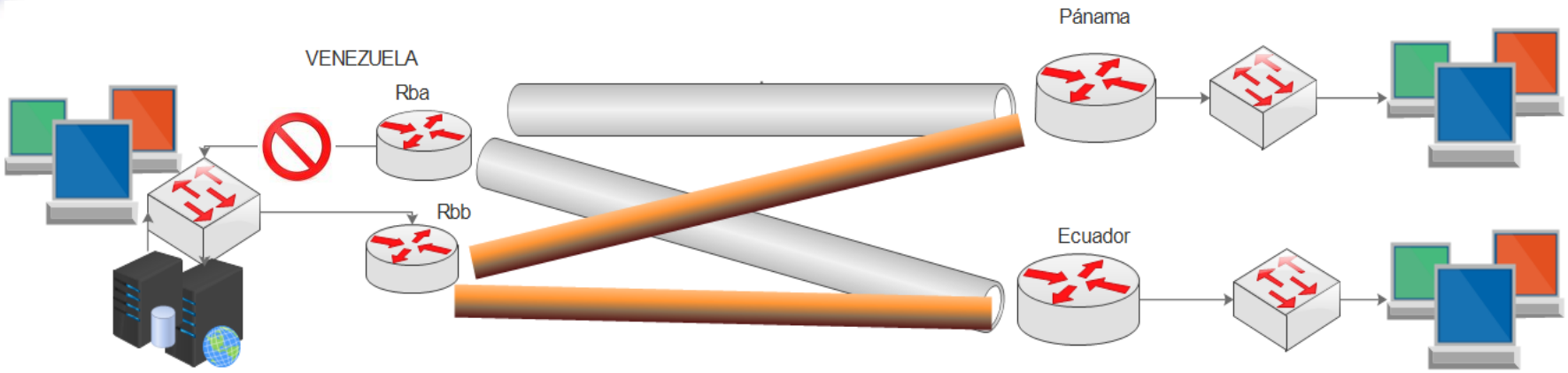

```
#
/interface gre
add ipsec-secret=warcry1986 !keepalive local-address=1.1.1.2 mtu=1400 name=\
    gre-MK1-MK3 remote-address=2.2.2.2
add ipsec-secret=warcry1986 !keepalive local-address=1.1.1.2 mtu=1400 name=\
    gre-MK1-MK4 remote-address=3.3.3.2
```

Ejemplo Rba

```
/interface gre
add ipsec-secret=warcry1986 !keepalive local-address=4.4.4.2 mtu=1400 name=\
    gre-Mk2-MK3 remote-address=2.2.2.2
add ipsec-secret=warcry1986 !keepalive local-address=4.4.4.2 mtu=1400 name=\
    gre-Mk2-Mk4 remote-address=3.3.3.2
```

Ejemplo Rbb

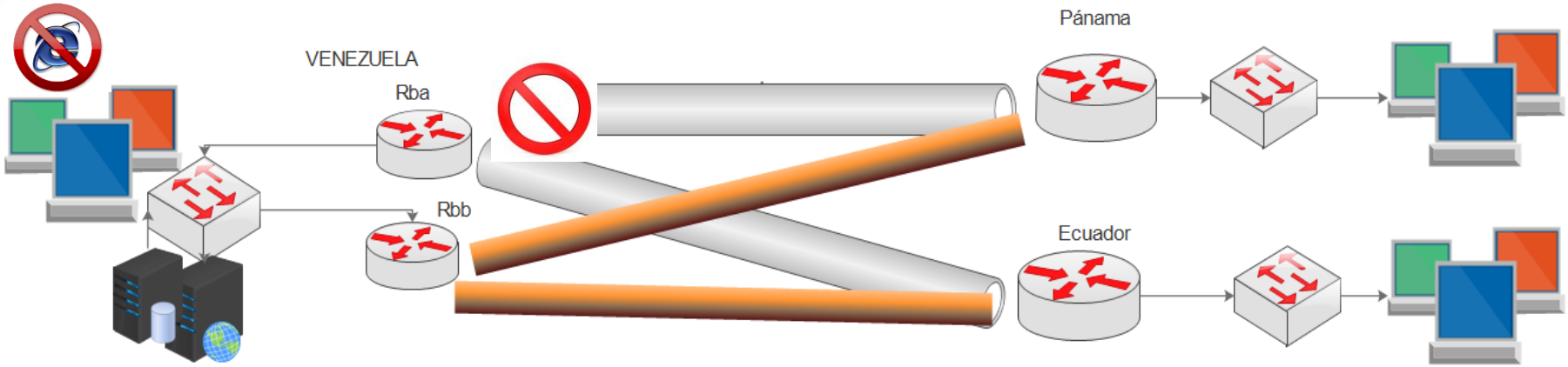
PUNTOS DE FALLA



SI EL ROUTER A ES EL MASTER DE LA CONFIGURACIÓN PLANTEADA AUTOMATICAMENTE DESPUÉS DE 3s EL ROUTER B TOMA SU LUGAR COMO GATEWAY DE LA RED Y OSPF CON TIEMPOS DE **1s HELLO 4s DEAD** ACTUALIZA SU TABLA ENRUTAMIENTO

MikroTik

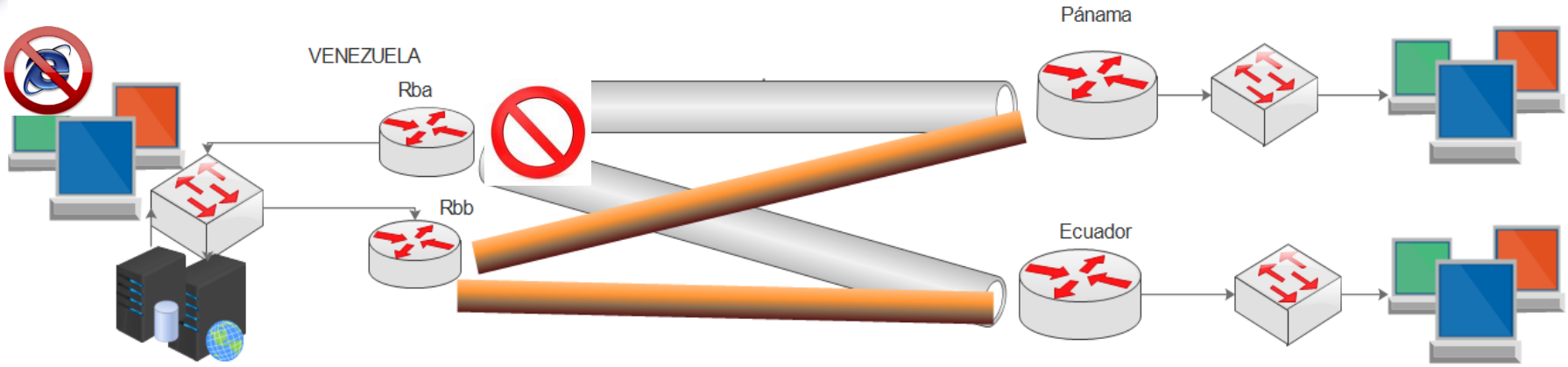
PUNTOS DE FALLA

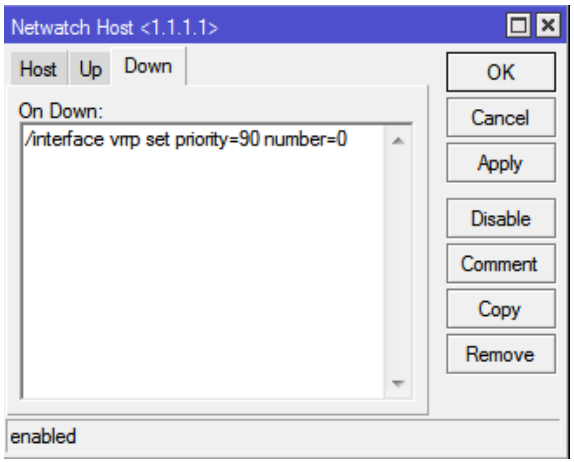


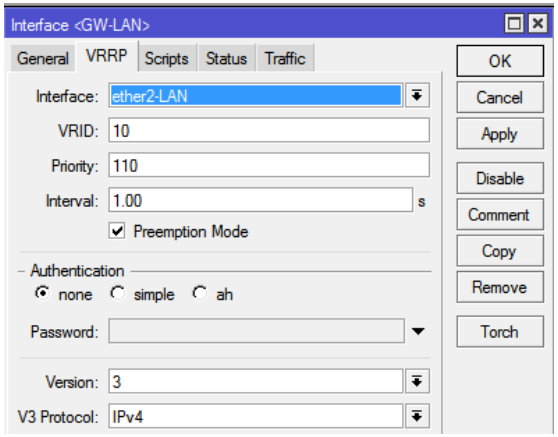
INTERNET DEL ISP A : Automáticamente los Túneles GRE pierden su conectividad y por ende OSPF actualiza su tabla de enrutamiento.
Para este escenario las Sucursales mantendrán conectividad con los Sistemas de la red de Venezuela, pero curiosamente la red de Venezuela no tendrá acceso al Internet.

MikroTik

PUNTOS DE FALLA







MikroTik

RECORDANDO

- CONFIGURAR CONEXIÓN DE INTERNET
- DEFINIR DIRECCIONAMIENTO (GRE – RED LAN)
- CREAR INTERFAZ GRE (IP ORIGEN – IP DESTINO)
- DEFINIR CONEXIÓN DE IPSEC
- ESTABLECER RUTAS DE OSPF
- CONFIGURAR VRRP
- OBJECT TRACK CON NETWATCH

BIBLIOGRAFIA CONSULTADA

http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/WAN_and_MAN/P2P_GRE_IPSec/P2P_GRE/2_p2pGRE_Phase2.html

http://www.cisco.com/c/en/us/support/docs/ip/generic-routing-encapsulation-gre/25885-pmtud-ipfrag.html

http://wiki.mikrotik.com/wiki/Main_Page

¿PREGUNTAS?

MUCHAS GRACIAS POR SU ATENCIÓN

Contacto:

+584120398717 / +584128380796

nelsont86@gmail.com

nelt_12@hotmail.com

http://ve.linkedin.com/in/lopeztheis

MikroTik