



SERTI  NET, C.A.

RIF: J-29920648-2



Mikrotik User Meeting - Colombia

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

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

¿Cómo podemos conectar 2 Sucursales remotas?

Conexiones Privadas

- Higher cost
- Less flexible
- WAN management
- Complex topologies

E1/T1

Microwave Links

Frame Relay

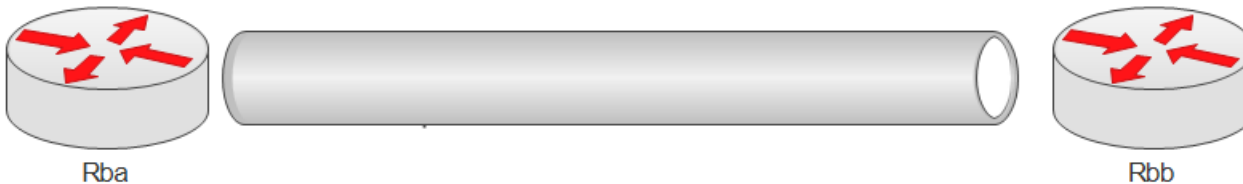
VPN

- Lower cost
- More flexible
- Simpler management
- Tunnel topology

¿Qué significa VPN?

MikroTik

VIRTUAL NETWORK → TUNNELING



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

PRIVATE NETWORK → ENCRYPTION



ENCRYPT

DECRYPT

Private: The traffic is encrypted to keep the data confidential

Lawyer 3 VPN



GRE



IPSEC



MPLS



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

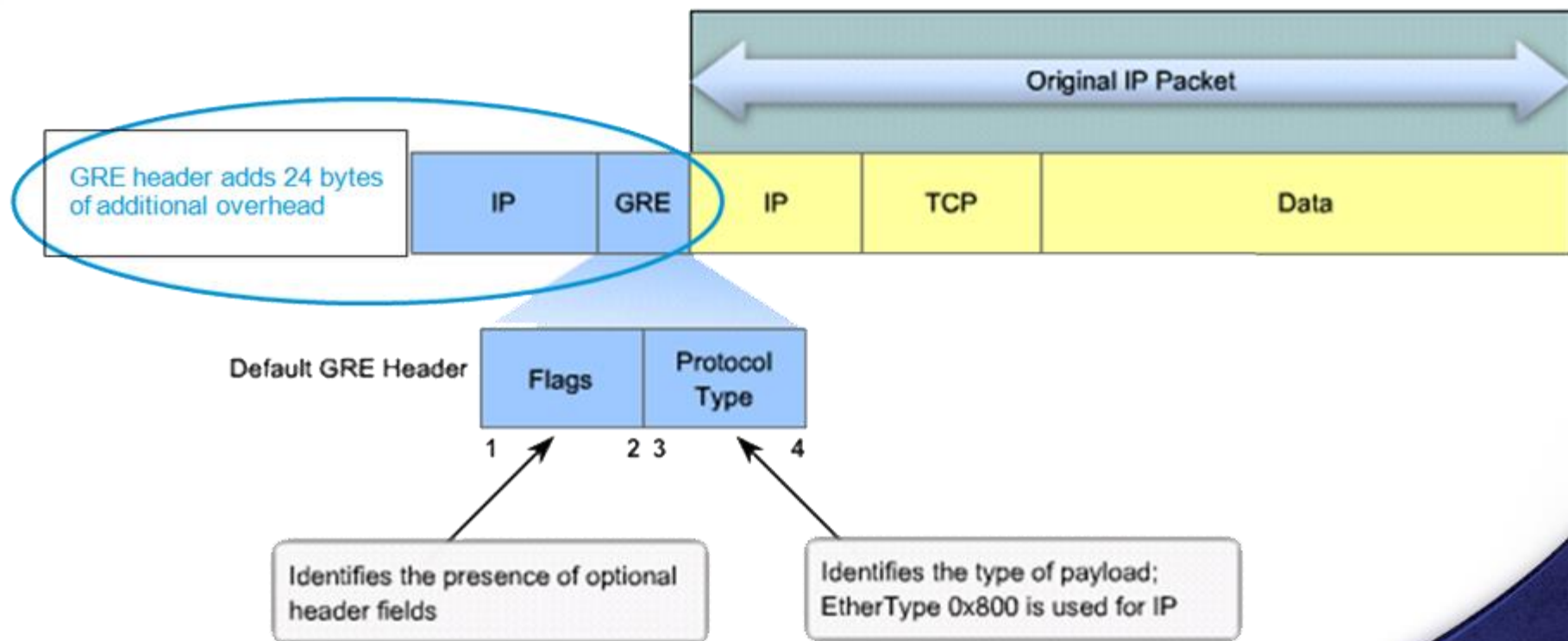
Standards: GRE [RFC 1701](#)

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

GRE interface IP MTU es $(1500-24) = \mathbf{1476}$.



Generic Routing Encapsulation (GRE)



GRE FRAGMENTACIÓN

DF (Don't Fragment) bit (DF = 0)

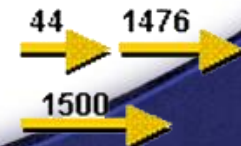
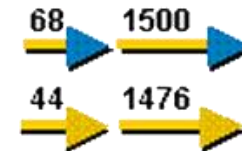


- 1 1500 →
- 2 44 1476 →
- 3 68 1500 →
- 4 Forward to GRE tunnel peer
- 5 De-capsulate GRE packets
- 6 Forward fragments to Host
- 7 Host reassembles data packet

Data packet (DF bit **not** set)

Fragment data packet

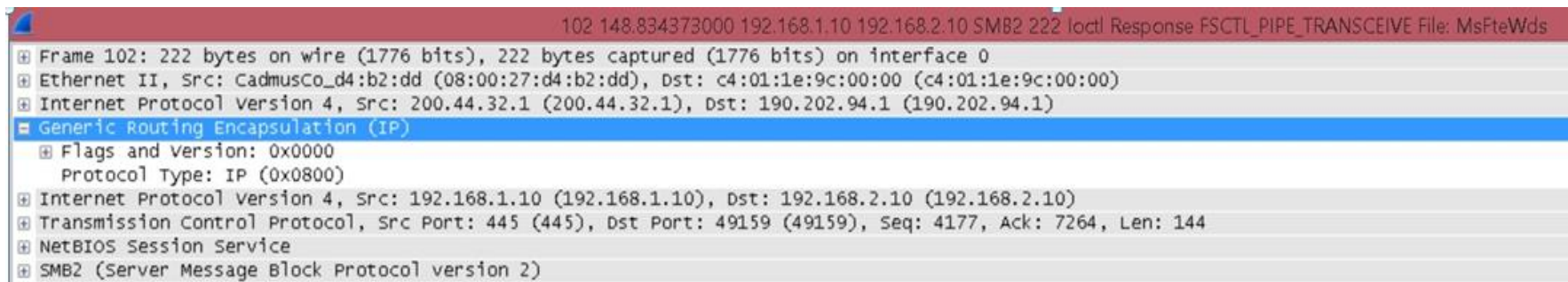
GRE encapsulate packets



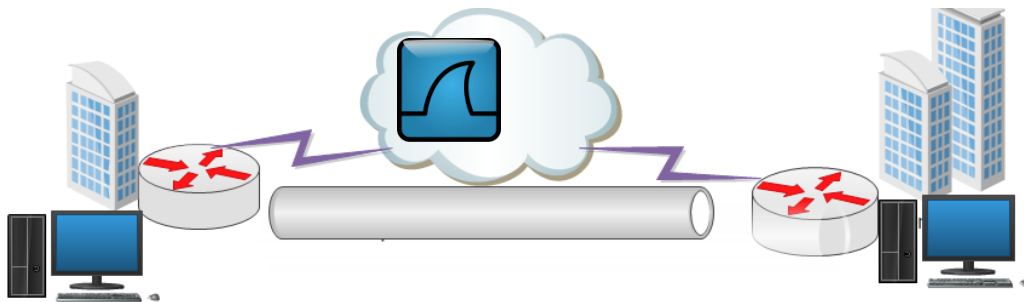


GRE DEBILIDADES

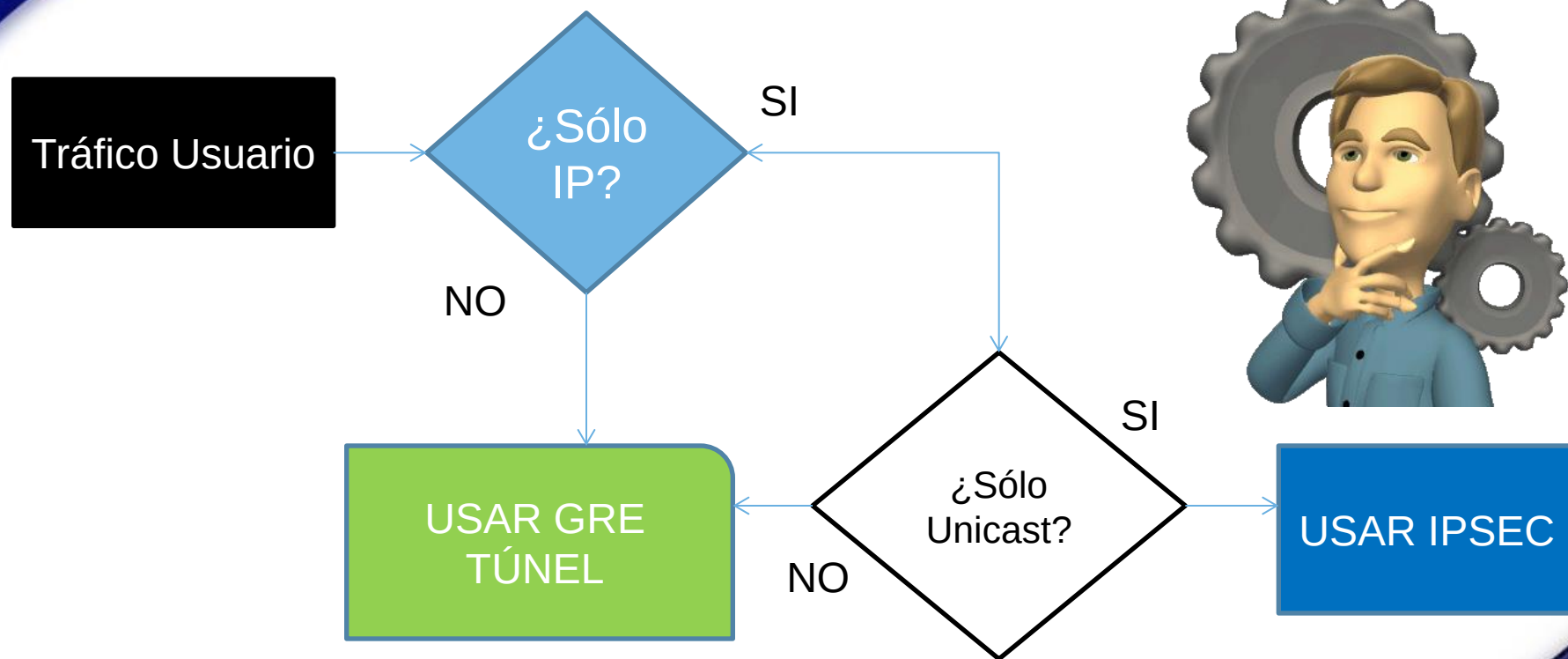
- GRE por si sólo no encrypta, la información
- Puede ser fácilmente monitoreado con un Sniffer como Wireshark.



MikroTik



¿Cuándo deberías usar GRE ó IPSEC?

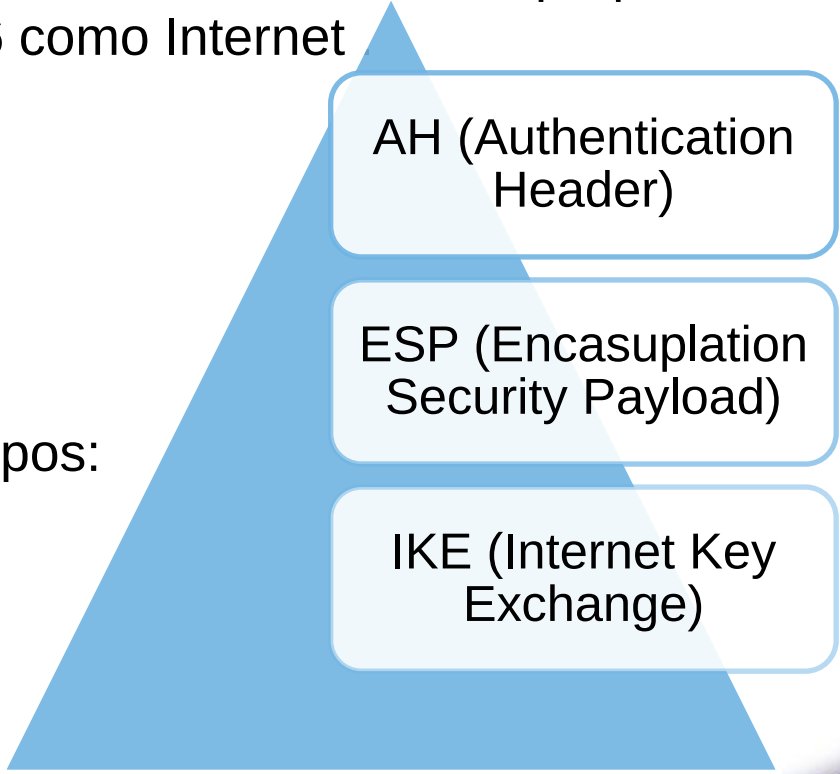




Internet Protocol Security (IPSEC)

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:

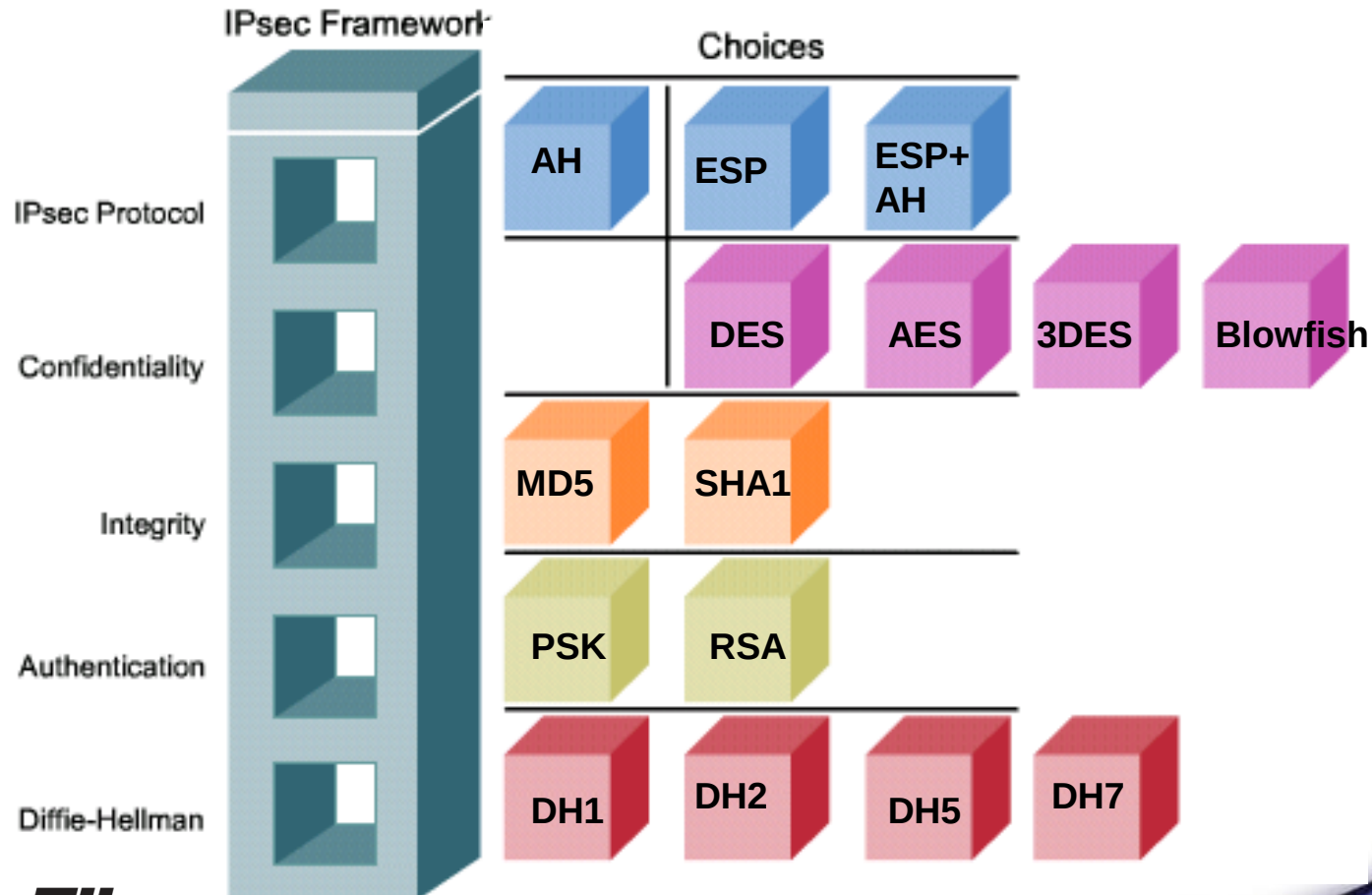


AH (Authentication Header)

ESP (Encapsulation Security Payload)

IKE (Internet Key Exchange)

IPSEC Framework





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.

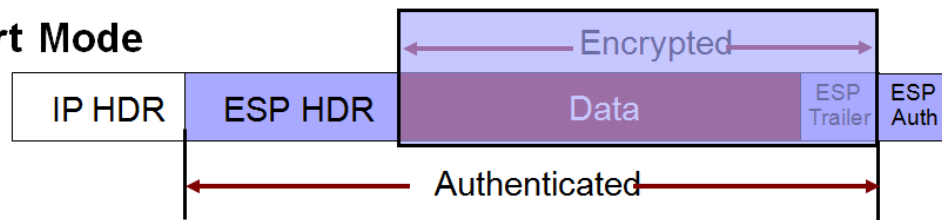
Tunnel mode:

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

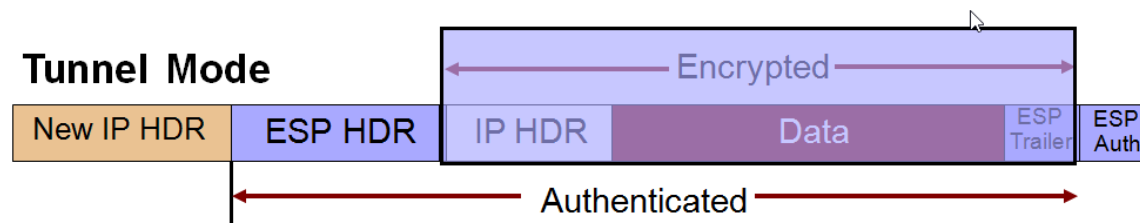


Original data prior to selection of IPSec protocol mode

Transport Mode



Tunnel Mode





Internet Key Exchange Protocol (IKE)

Phase1

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

Está fase cada opción debe ser igual en Ambos Peers



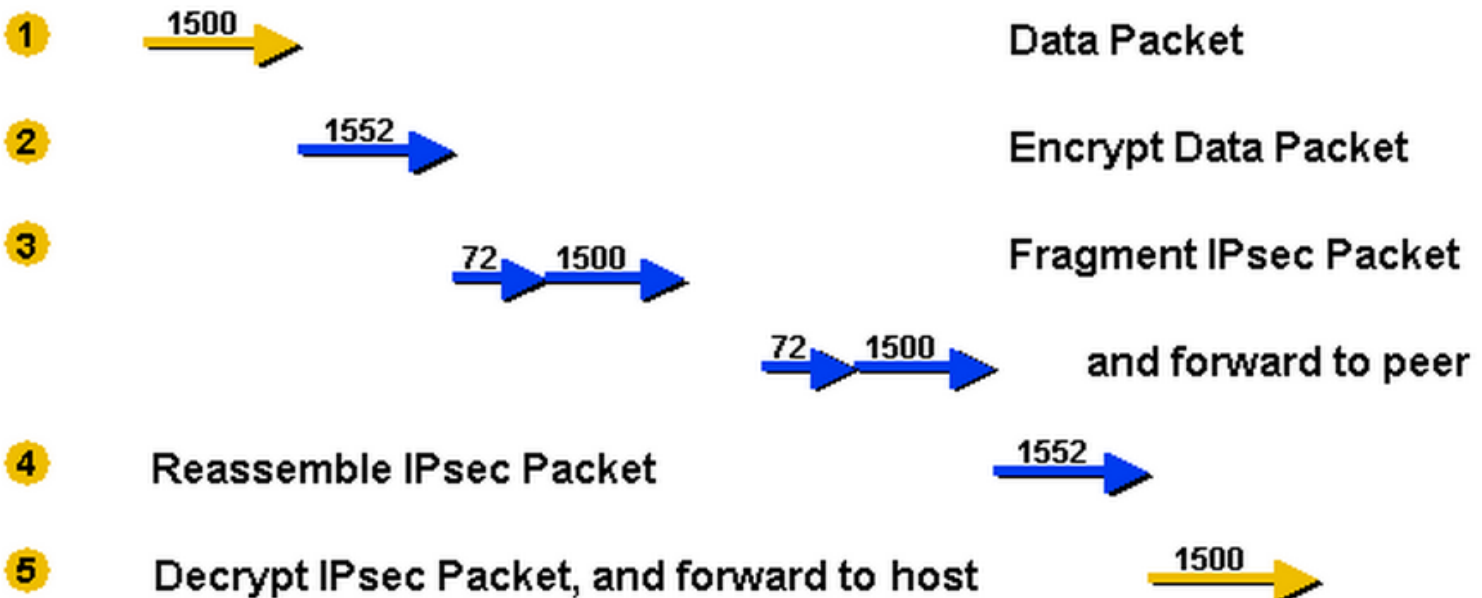
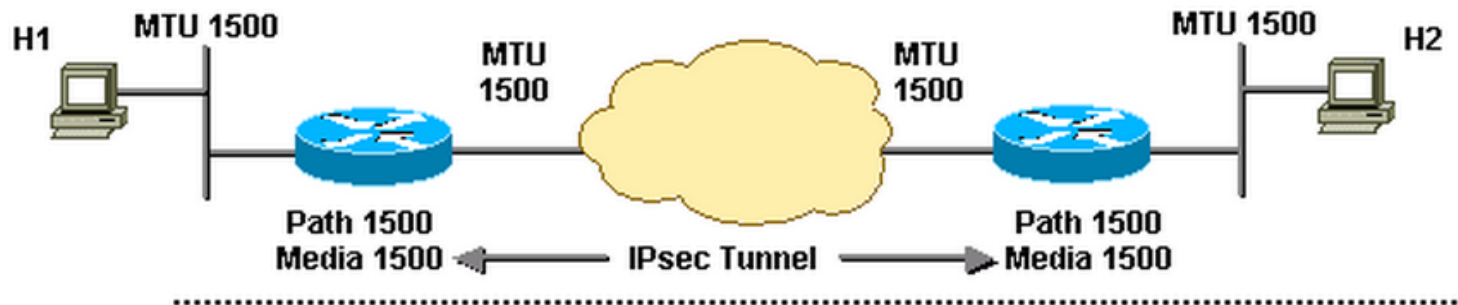
Phase2

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

Está fase cada opción debe ser igual en Ambos Peers

IPSEC FRAGMENTACIÓN

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



GRE OVER IPSEC

Original Payload (IP
+Data)



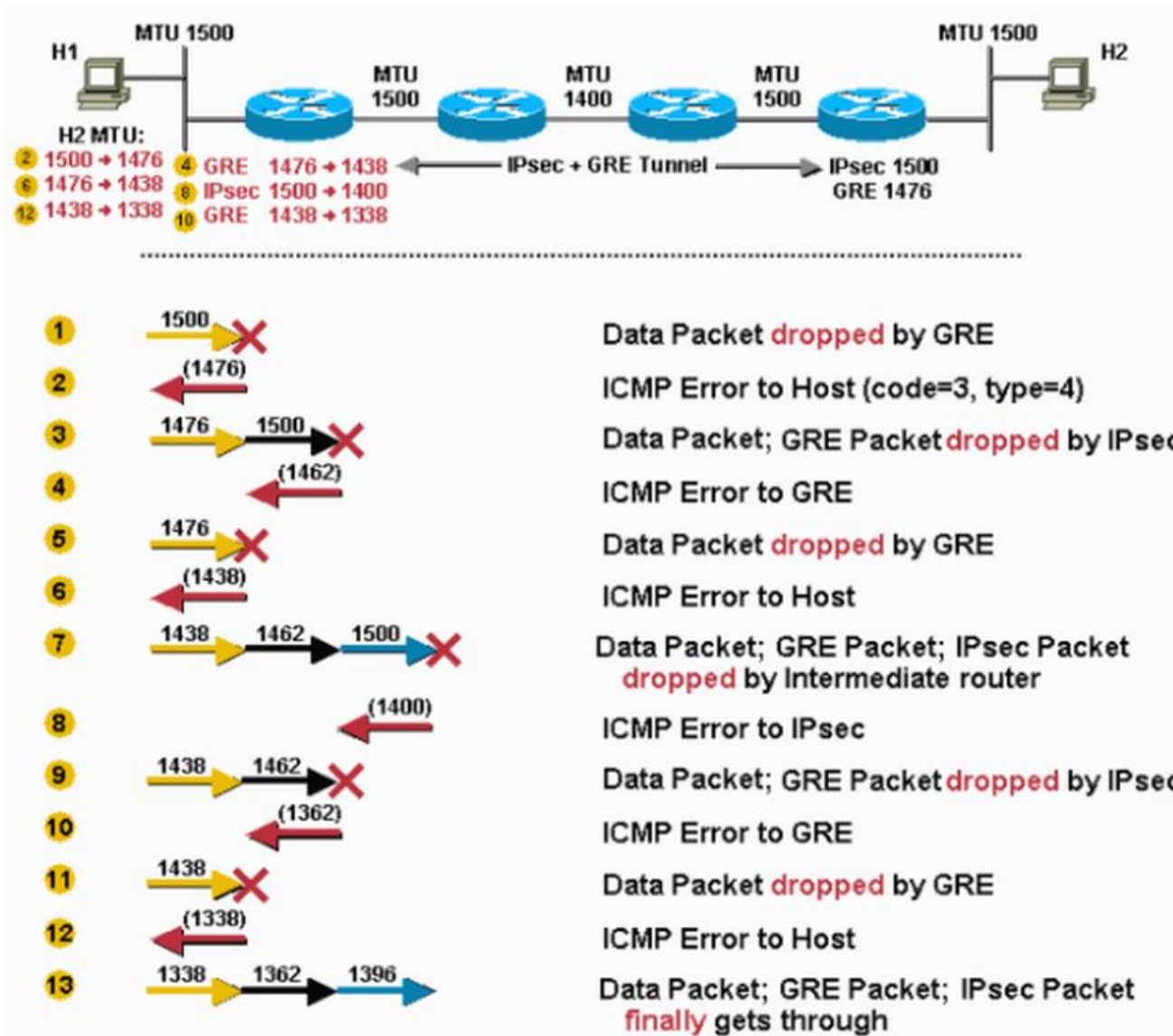
| GRE | Original Payload |



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



GRE OVER IPSEC FRAGMENTACIÓN

[illegible]



GRE OVER IPSEC CONFIGURACION

Interface <gre-MK1-MK3>

General Status Traffic

Name: gre-MK1-MK3

Type: GRE Tunnel

MTU: 1400

Actual MTU: 1400

L2 MTU: 65535

Local Address: 1.1.1.2

Remote Address: 2.2.2.2

IPsec Secret: *****

Keepalive: 00:00:10 . 10

DSCP: inherit

Dont Fragment: no

☒ Clamp TCP MSS

OK Cancel Apply Disable Comment Copy Remove Torch

enabled running slave

IPsec Policy <1.1.1.2:0->2.2.2.2:0>

General Action

Src. Address: 1.1.1.2

Src. Port:

Dst. Address: 2.2.2.2

Dst. Port:

Protocol: 47

☐ Template

OK Copy Remove

dynamic enabled Template

IPsec Policy <1.1.1.2:0->2.2.2.2:0>

General Action

Action: encrypt

Level: require

IPsec Protocols: esp

☐ Tunnel

SA Src. Address: 1.1.1.2

SA Dst. Address: 2.2.2.2

Proposal: default

Priority: 0

OK Copy Remove

dynamic enabled Template

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
```

IPsec						
Policies	Groups	Peers	Remote Peers	Mode Configs	Proposals	Installed SAs
Keys	Users					
	Flush	Find				
SPI	Src. Address	Dst. Address	Auth....	Encr....	Current B...	
0	1.1.1.2	3.3.3.2	none	none	0	
6d4615f	2.2.2.2	1.1.1.2	sha1	aes c...	8587	
e92c34c	1.1.1.2	2.2.2.2	sha1	aes c...	115636	

ALTA DISPONIBILIDAD

Redundancia

Tiempos de
Convergencia

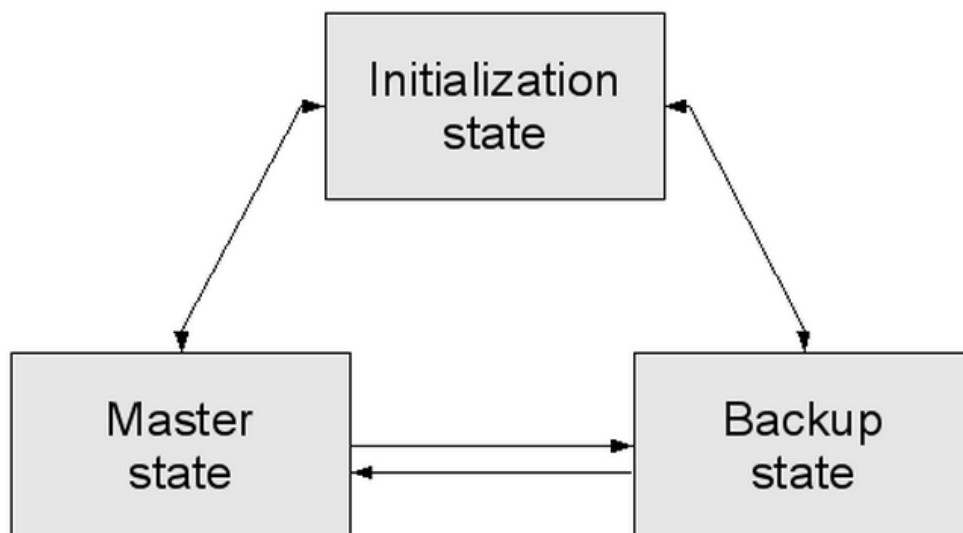
Documentación
de la Red

Protocolo
redundante

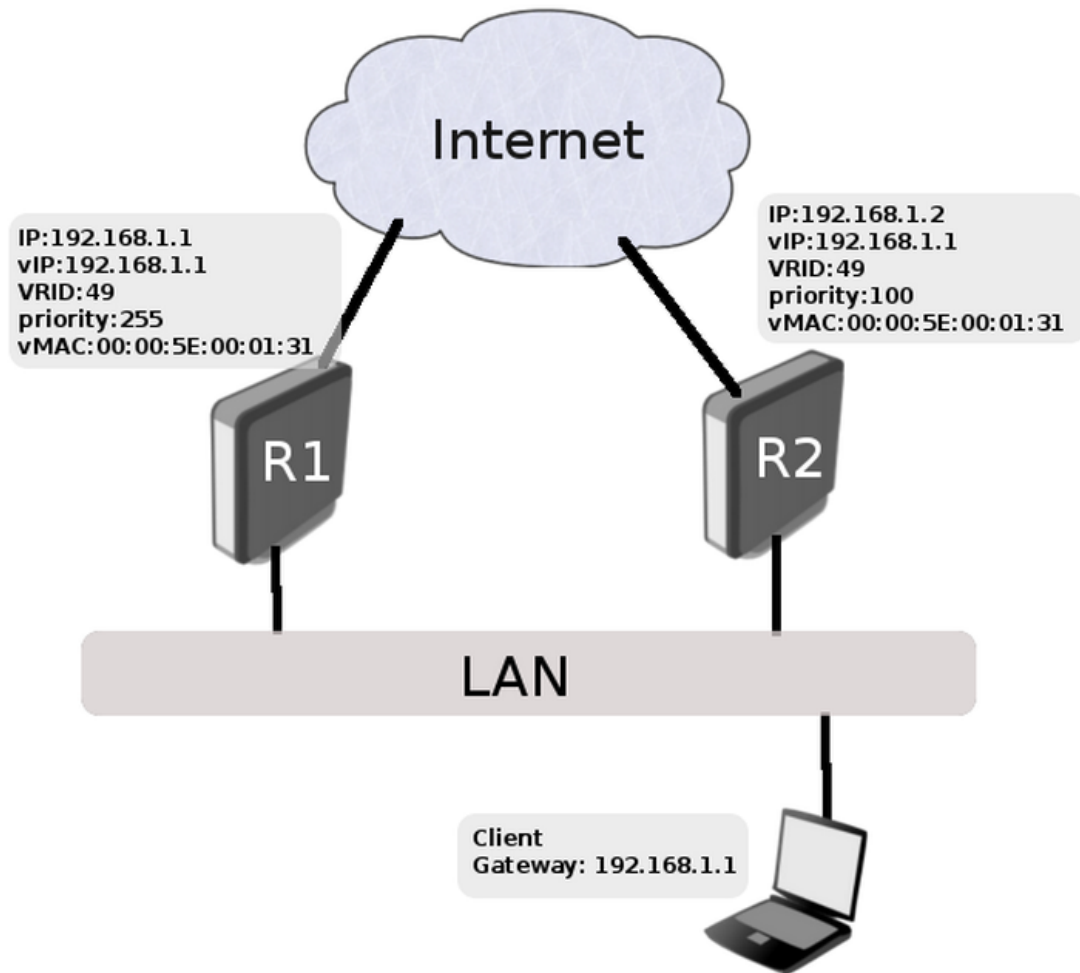


Virtual Router Redundancy Protocol (VRRP)

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.



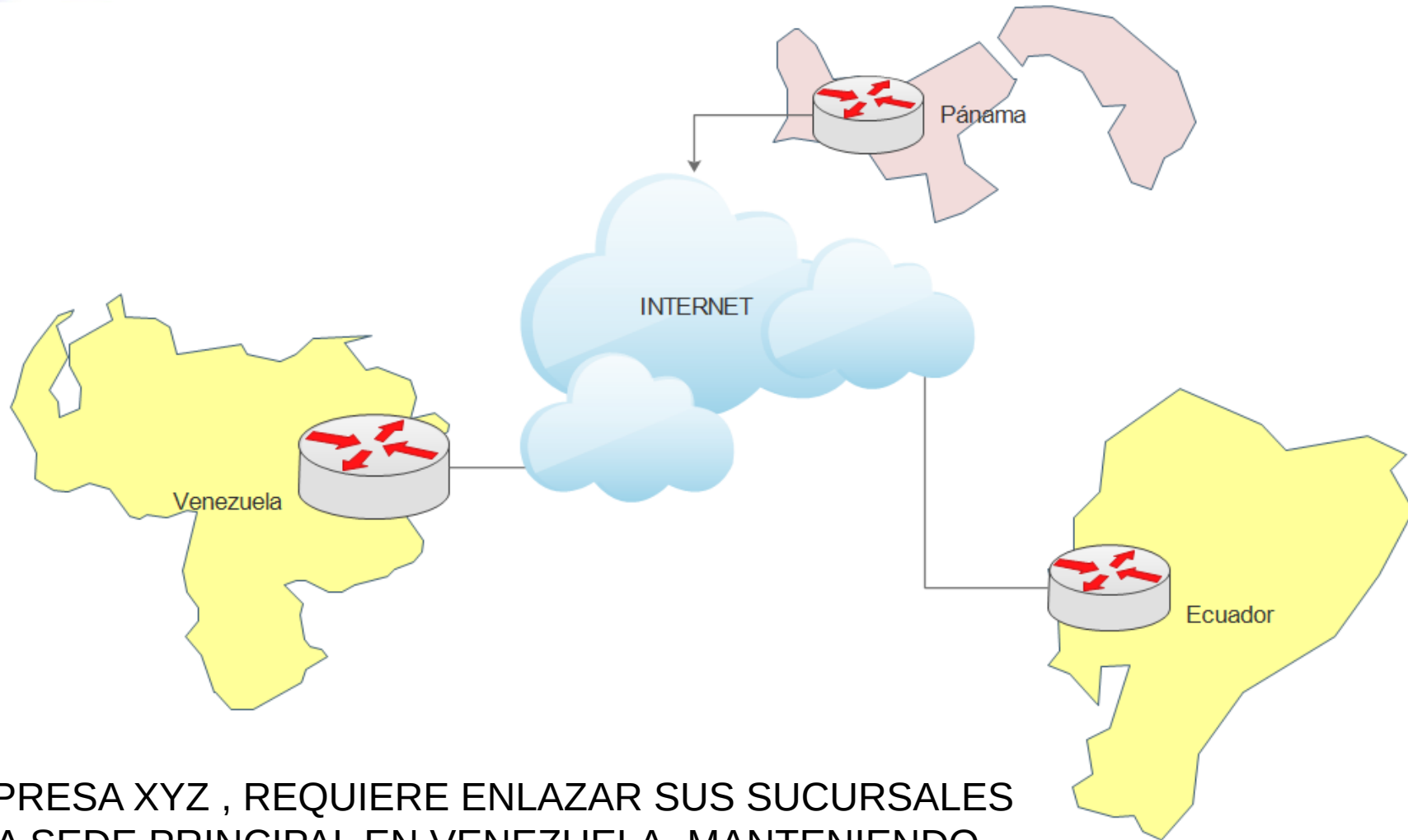
Virtual Router Redundancy Protocol (VRRP)



Soportado por distintas
Marcas de Tecnología

Tiempo detección de
Falla de 3 Segundos.

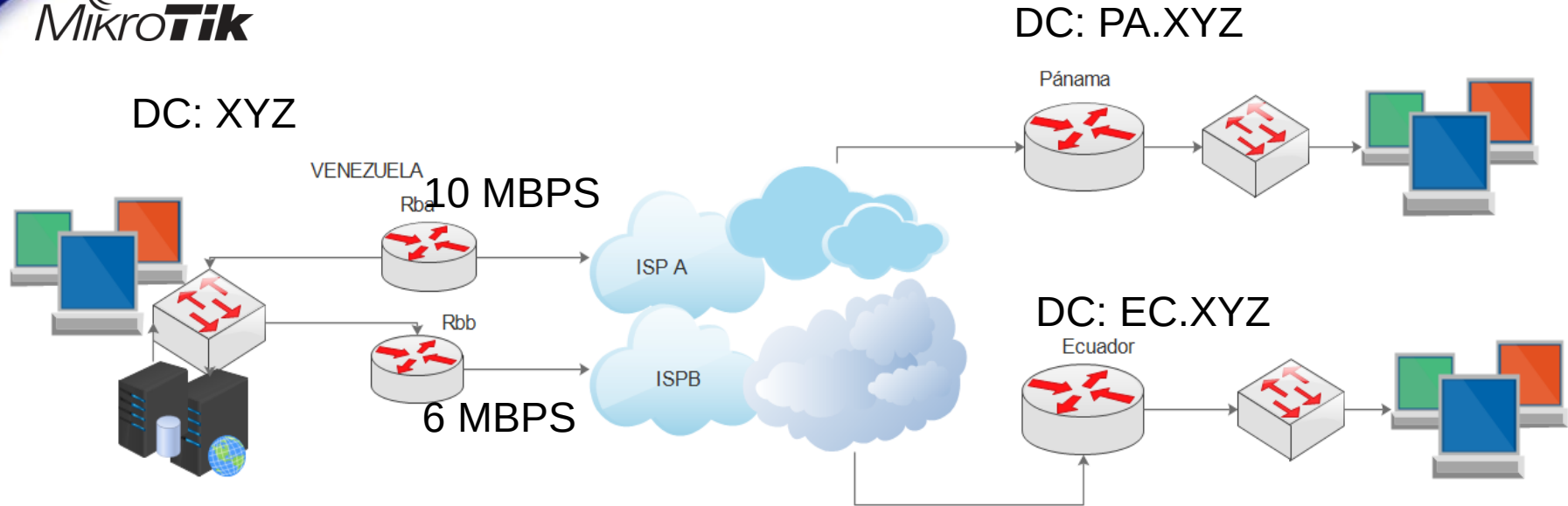
ESCENARIO



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

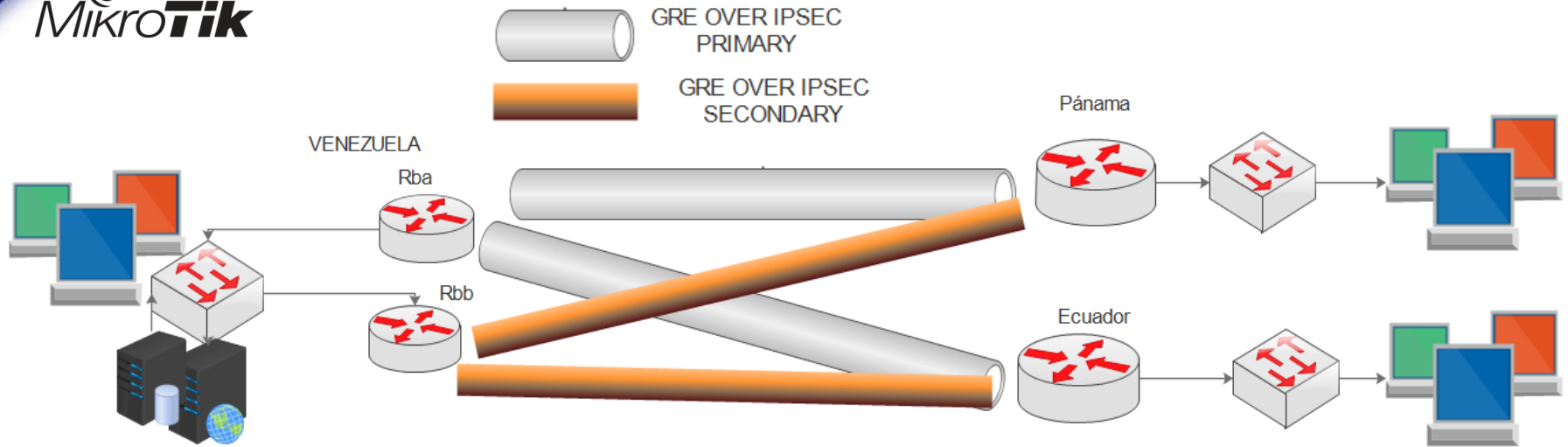
MikroTik



- 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

MikroTik



```
#
/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
```



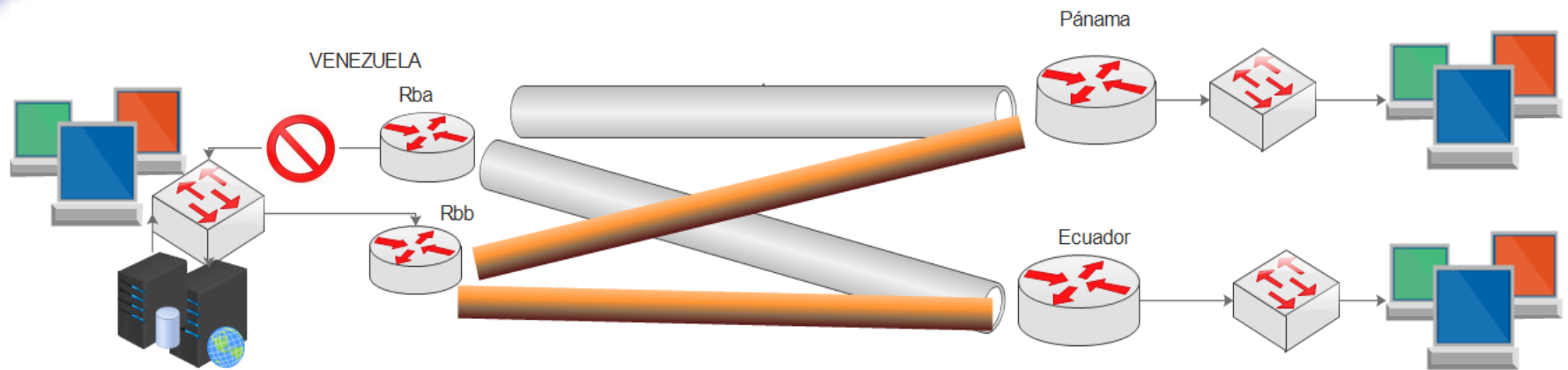
Ejemplo Rba

```
/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
```



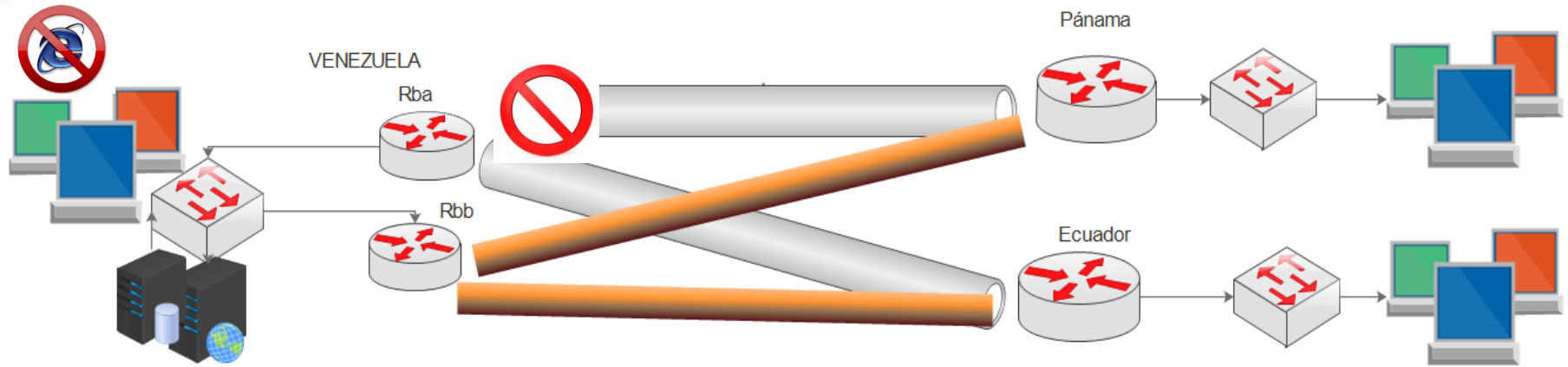
Ejemplo Rbb

PUNTOS DE FALLA



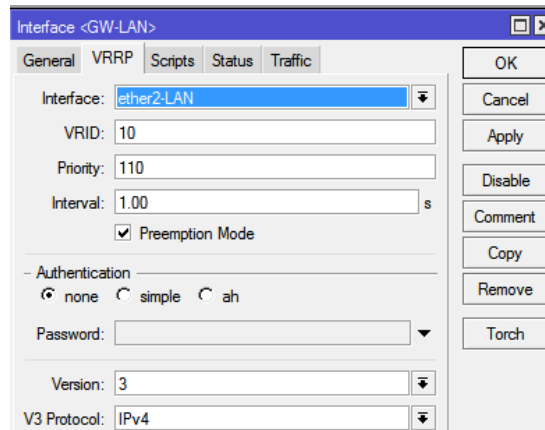
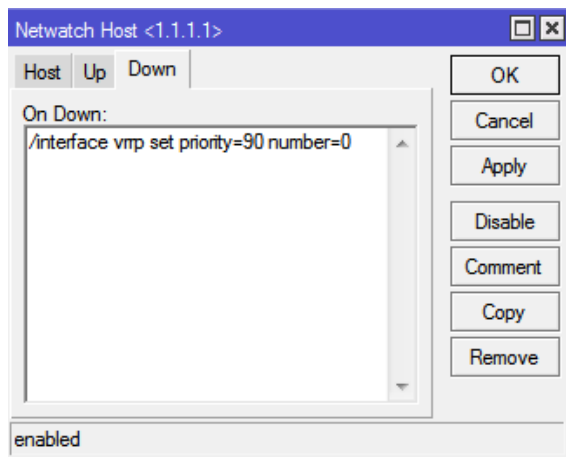
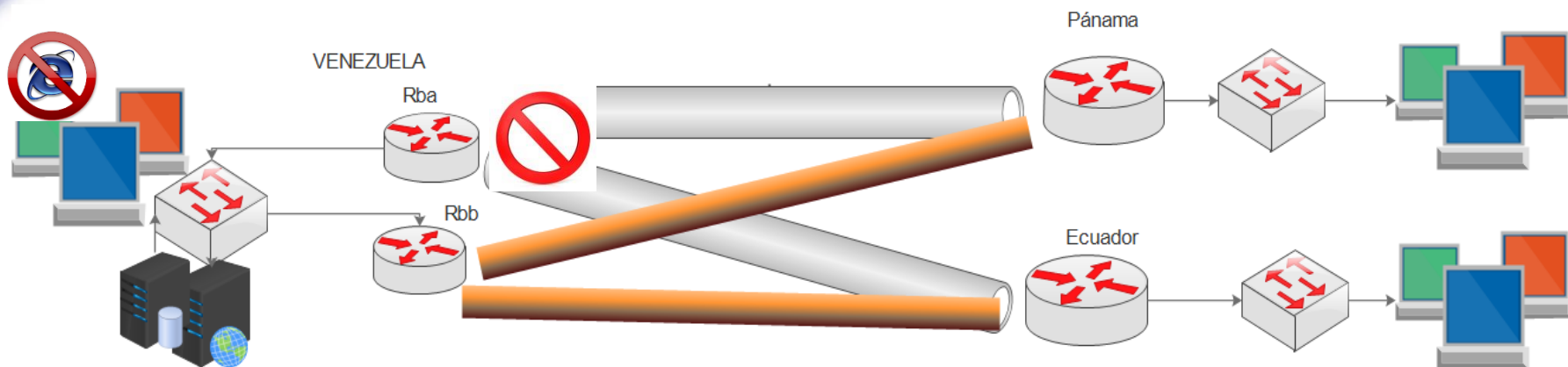
SI EL ROUTER A ES EL MASTER DE LA CONFIGURACIÓN PLANTEADA AUTOMATICAMENTE DESPUÉS DE 3s EL ROUTER B TOMA SU LUGAR COMO GATEWAY DE LA RED Y OSPF CON TIEMPOS DE **1s HELLO 4s DEAD** ACTUALIZA SU TABLA ENRUTAMIENTO

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.

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>



*Mikro***Tik**