Richart Rojas

INOVA Networks

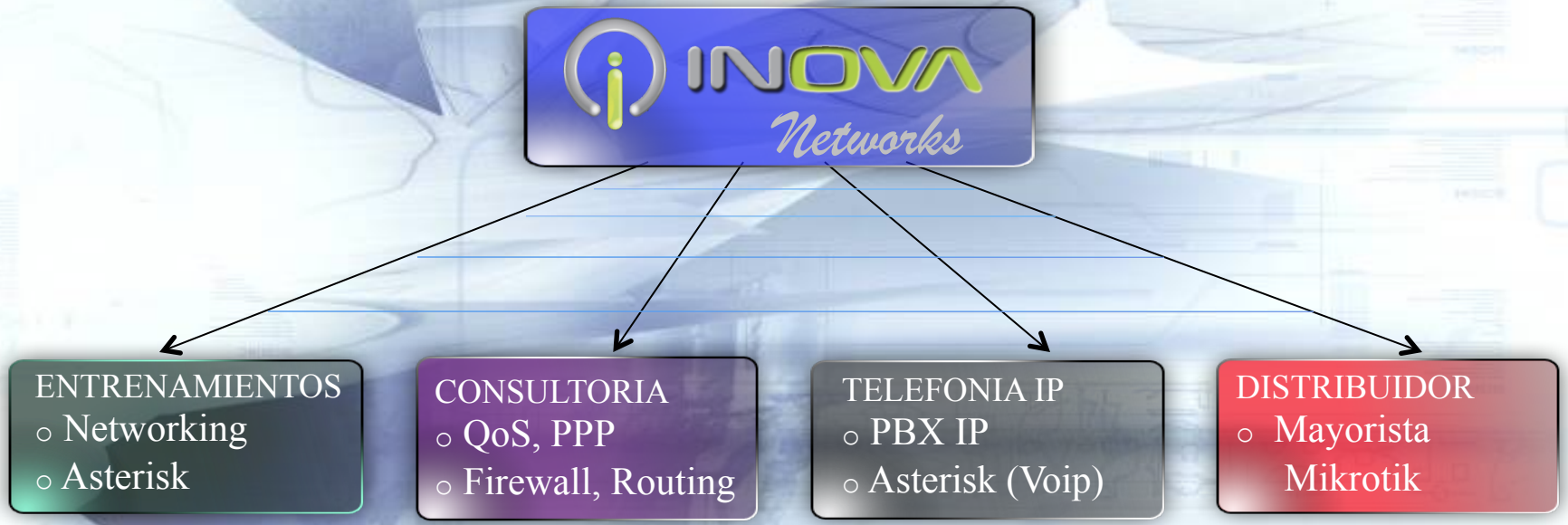
Bolivia
2014

MUM

Mikrotik Security best practices

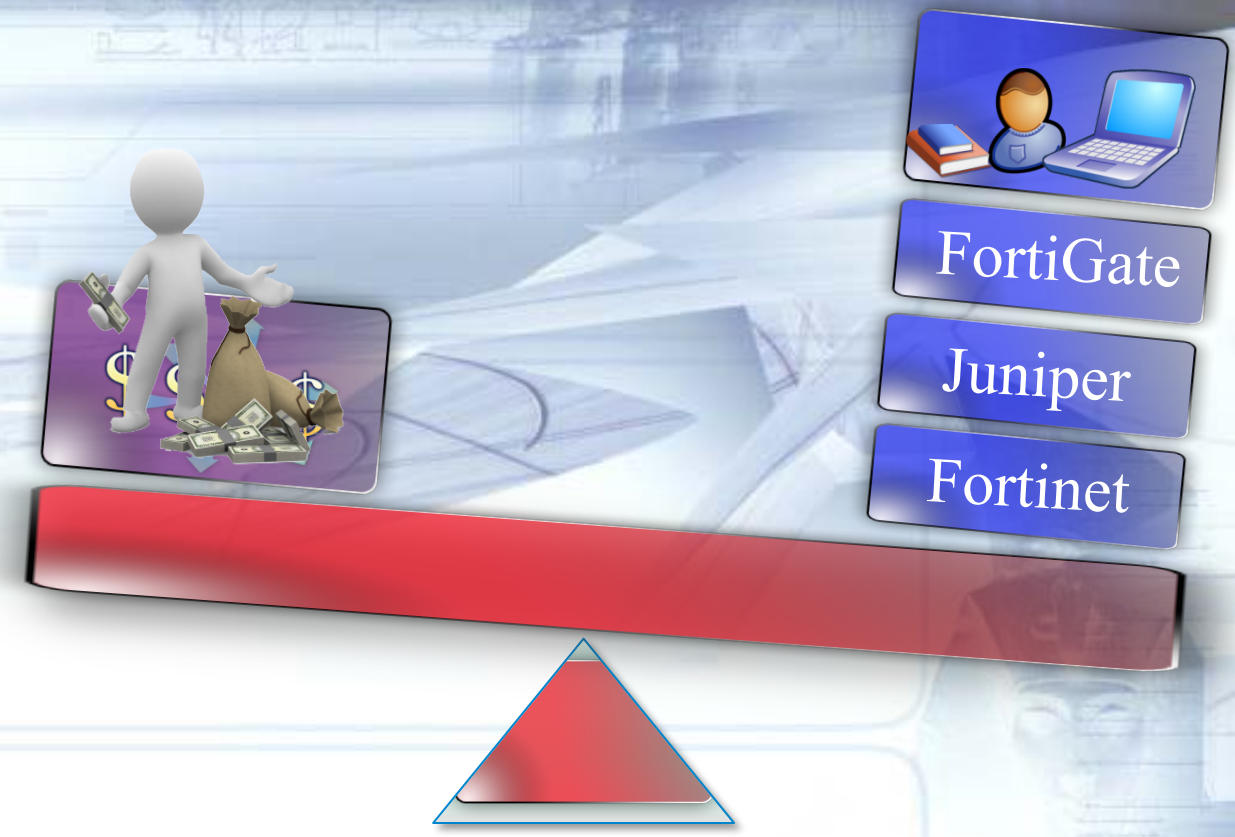
Presentacion

- **Richart W. Rojas**
- **Mikrotik Certified Consultant**
  (MTCNA, MTCWE, MTCTCE, MTCRE, MTCUME, MTCINE)



Area de trabajo

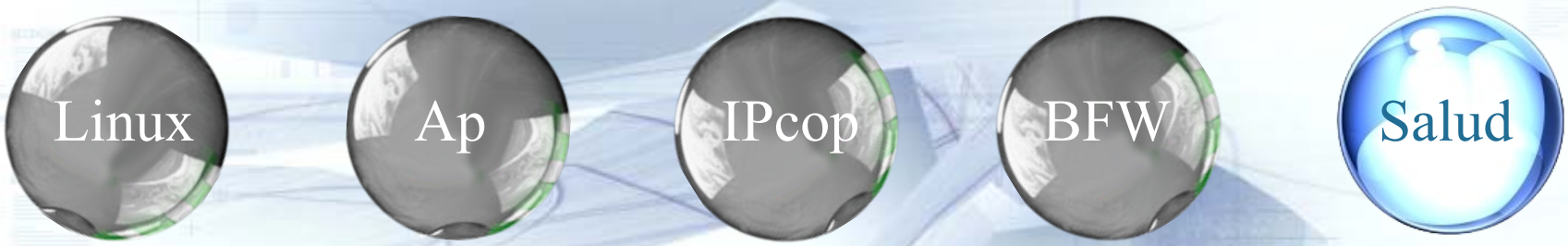
Como empesar?



Una historia común

INOVA

Como empesar?



Una historia común

INOVA

Resignarse???....como seguimos?

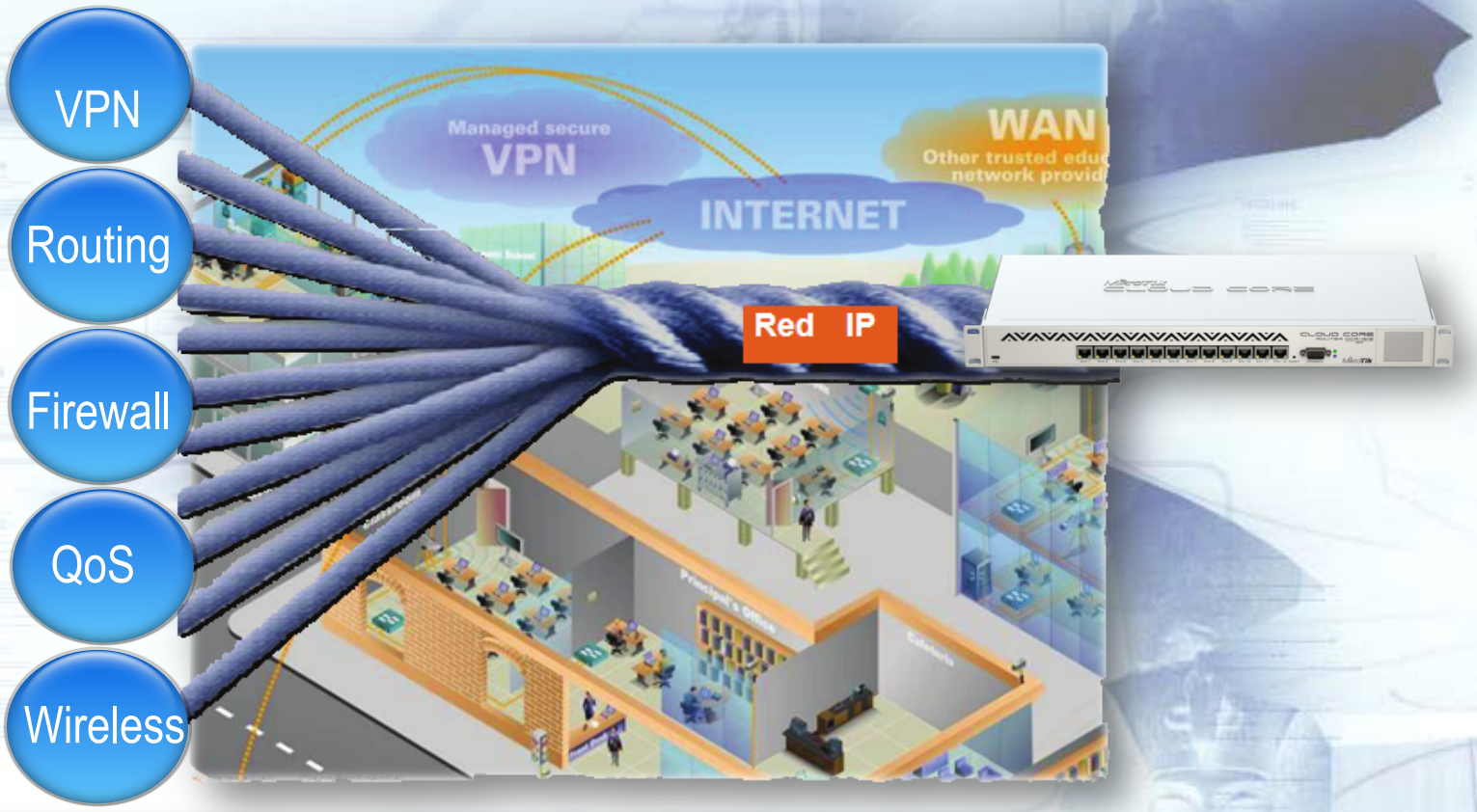
LO QUE ENCONTRAMOS EN MIKROTIK

INOVA

LO QUE ENCONTRAMOS EN MIKROTIK

* Estabilidad
* Flexibilidad
* Herramientas
* Desarrollo continuo
* Compatibilidad -RFC
* Precio/Calidad

Multiples Soluciones



Múltiples soluciones con Mikrotik (Conectividad Completa VPNs, Seguridad, balanceo de carga, Redundancia, QoS. Esa es potencialidad que tiene Mikrotik…tantos beneficios en una solución...)

Ahora donde esta MK?

Bolivia
2014

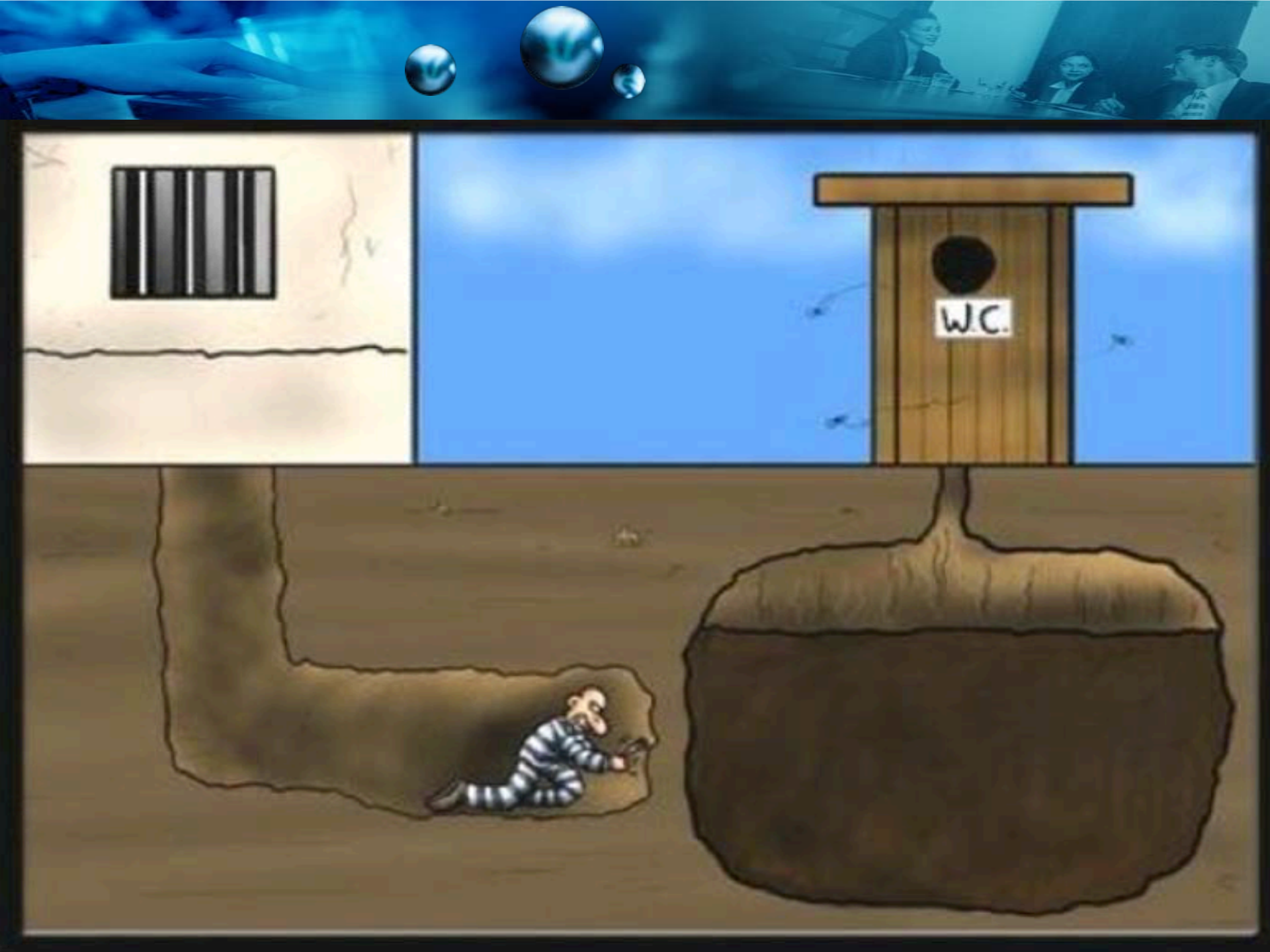
Mikrotik?

Mikrotik.. mi primera experiencia

INOVA

Security Mikrotik

Security


W.C.

Modelo OSI


7
Aplicación
6
Presentación
5
Sesión
4
Transporte
3
Red
2
Enlace de datos
1
Física

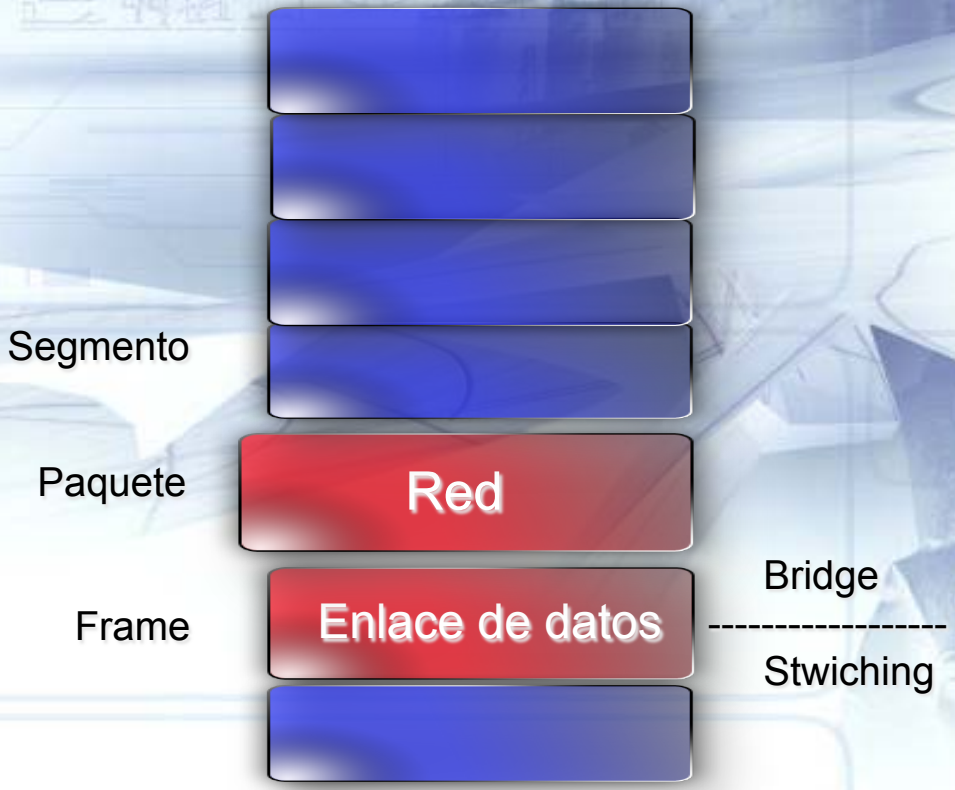
Modelo OSI

Seguridad es un proceso continuo y los administradores deben tener en cuenta desde la capa física hasta la capa de aplicaciones.

Teniendo como referencia el modelo OSI, la seguridad de las capas superiores siempre depende de las capas inferiores. Una red segura necesita garantizar, además de otras cosas, las informaciones coherentes entra la capa 2 (enlace) y la capa 3 (red)

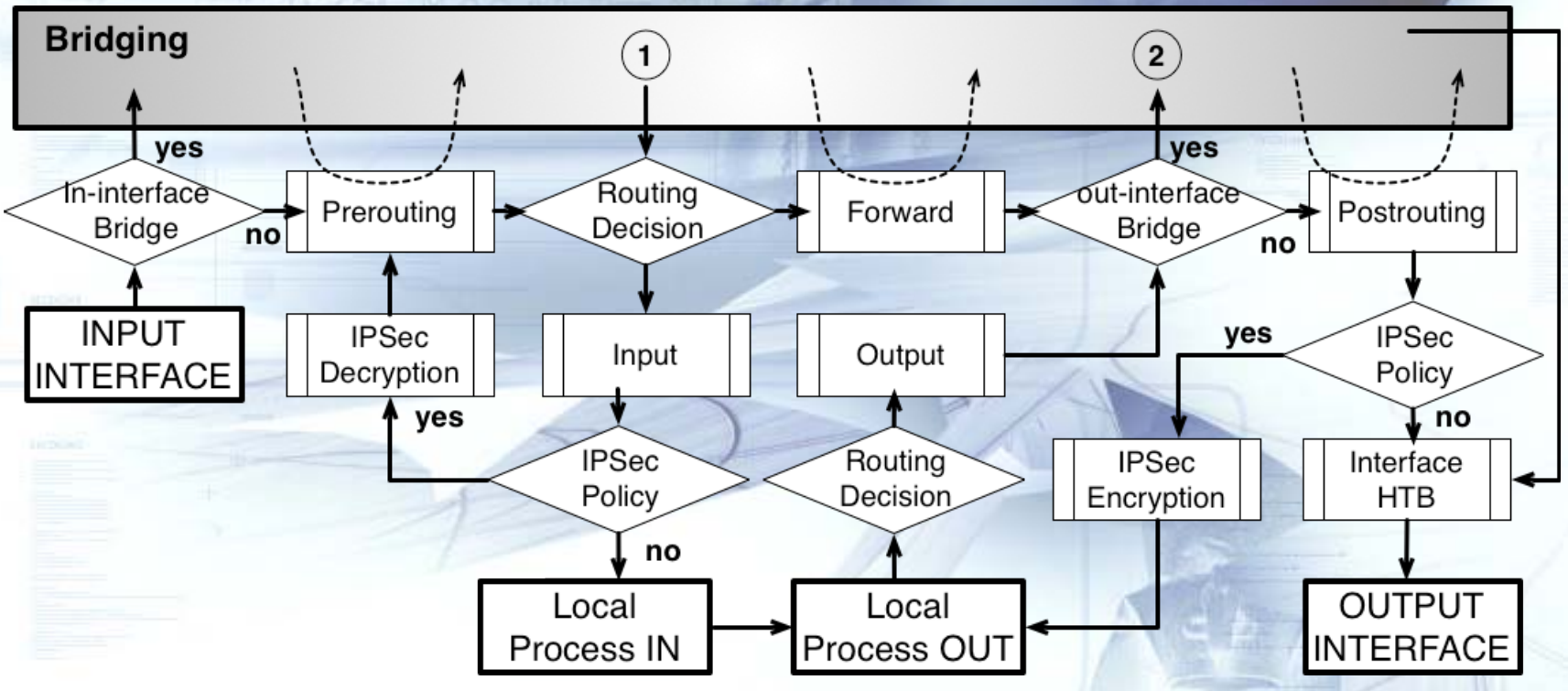
Existen inúmeros ofensores a la disponibilidad de la red por ataques de negación de servicio que explotan vulnerabilidades inherentes a la capa II

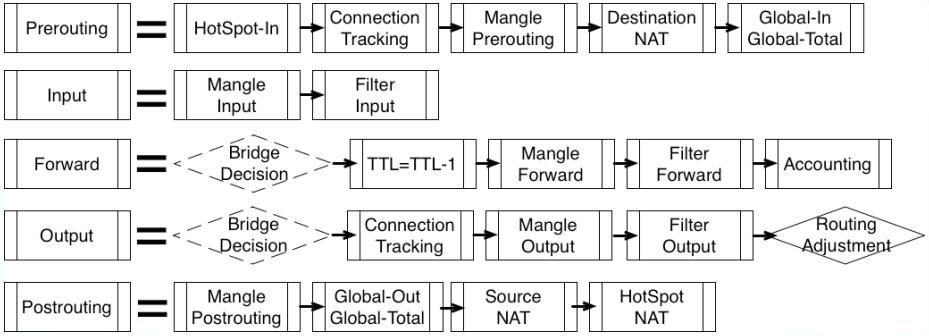
Modelo OSI

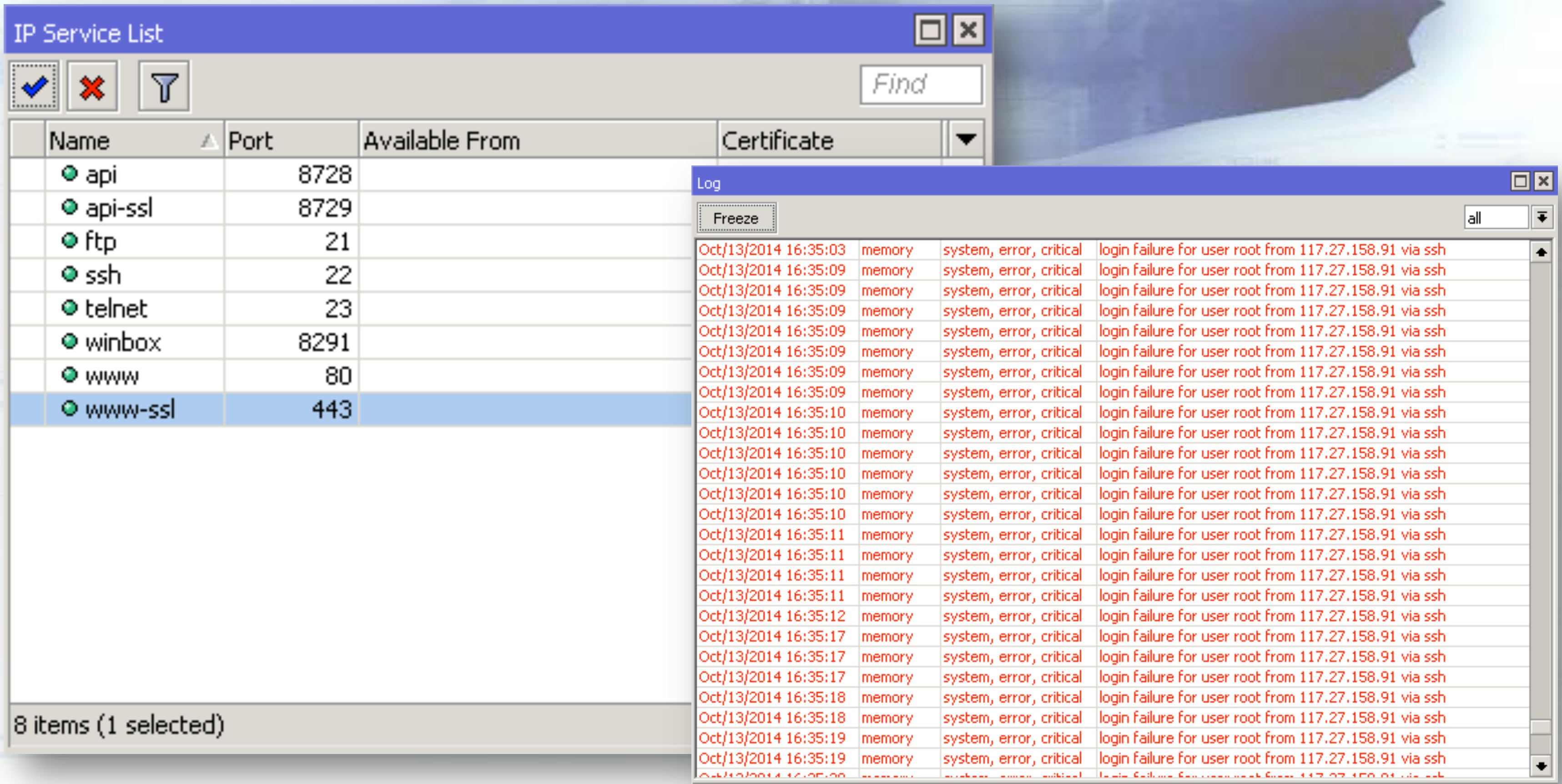

Segmento
Paquete
Red
Frame
Enlace de datos
Bridge

Stwiching

Packet flow

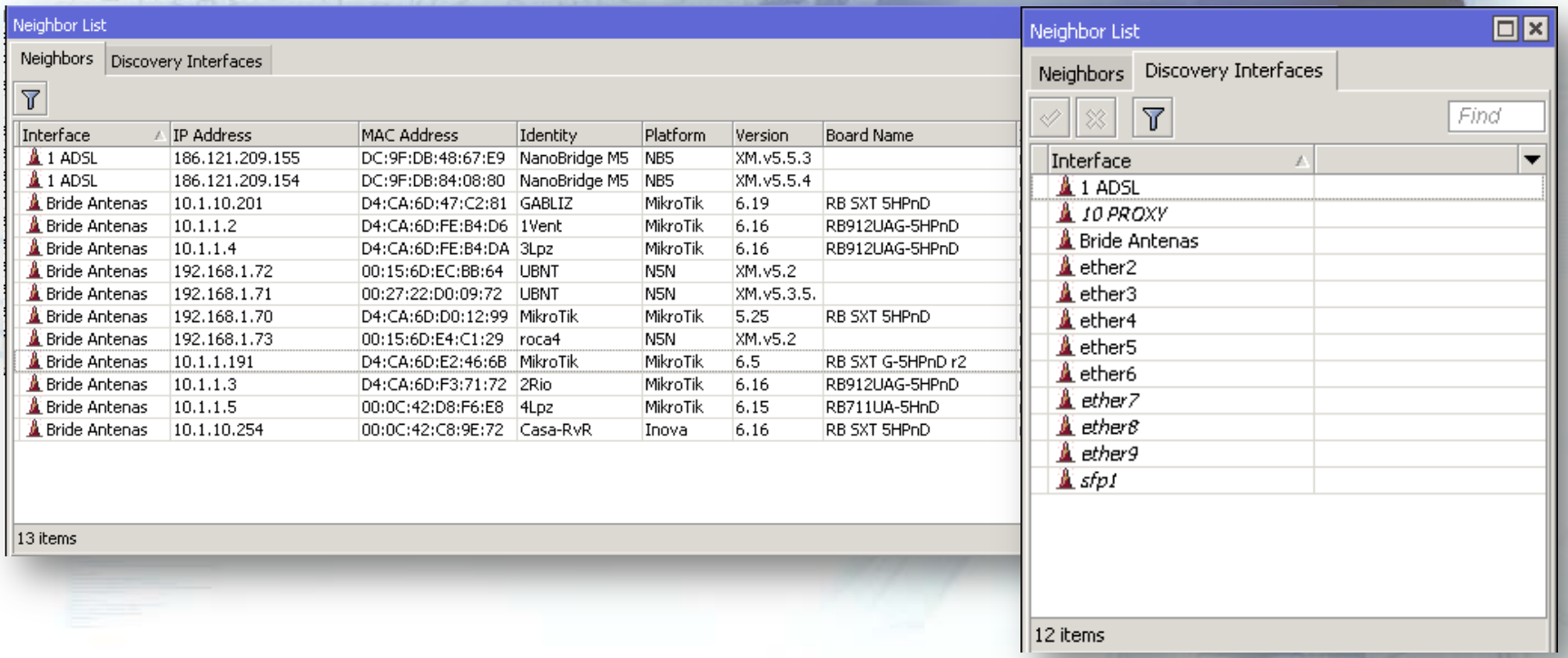

Bridging
1
2
yes
In-interface Bridge
no
Prerouting
Routing Decision
Forward
yes
out-interface Bridge
no
Postrouting
INPUT INTERFACE
IPSec Decryption
Input
Output
yes
IPSec Policy
no
yes
IPSec Policy
Routing Decision
IPSec Encryption
Interface HTB
no
Local Process IN
Local Process OUT
OUTPUT INTERFACE


Prerouting = HotSpot-In → Connection Tracking → Mangle Prerouting → Destination NAT → Global-In Global-Total
Input = Mangle Input → Filter Input
Forward = Bridge Decision → TTL=TTL-1 → Mangle Forward → Filter Forward → Accounting
Output = Bridge Decision → Connection Tracking → Mangle Output → Filter Output → Routing Adjustment
Postrouting = Mangle Postrouting → Global-Out Global-Total → Source NAT → HotSpot NAT



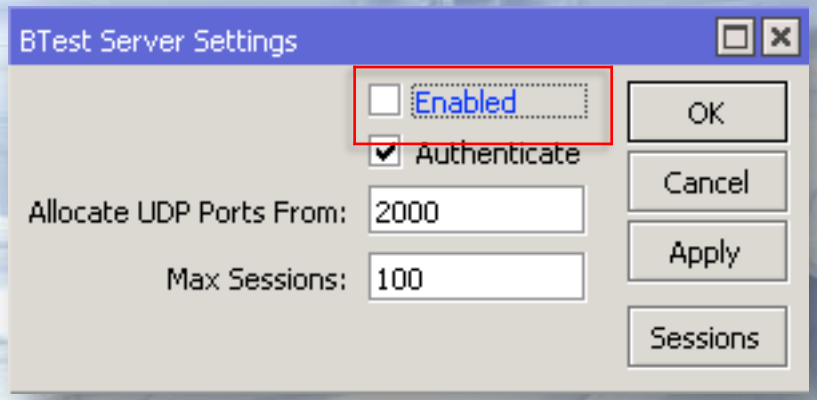
- Deshabilitar servicios no utilizados

IP/Neighbords



Desactivar Descubrimiento Interfaces donde no necesario. Todas las interfaces que no lo hacen directamente conectarse a su propia infraestructura.

Tools / Btest Server

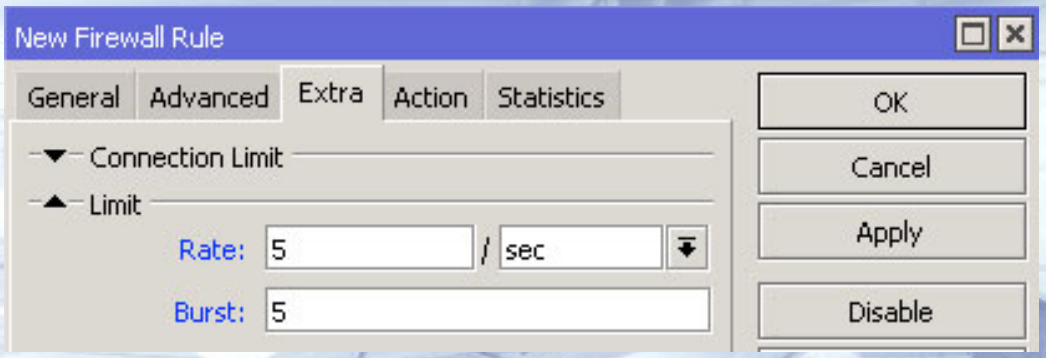


Por defecto, el bandwidth test server esta habilitado. Asegúrese sólo este activo cuando sea necesario

Que acciones podemos seguir?

Manos a la Obra

Ping Flooding



Consiste en un volumen aleatorio de de mensajes ICMP

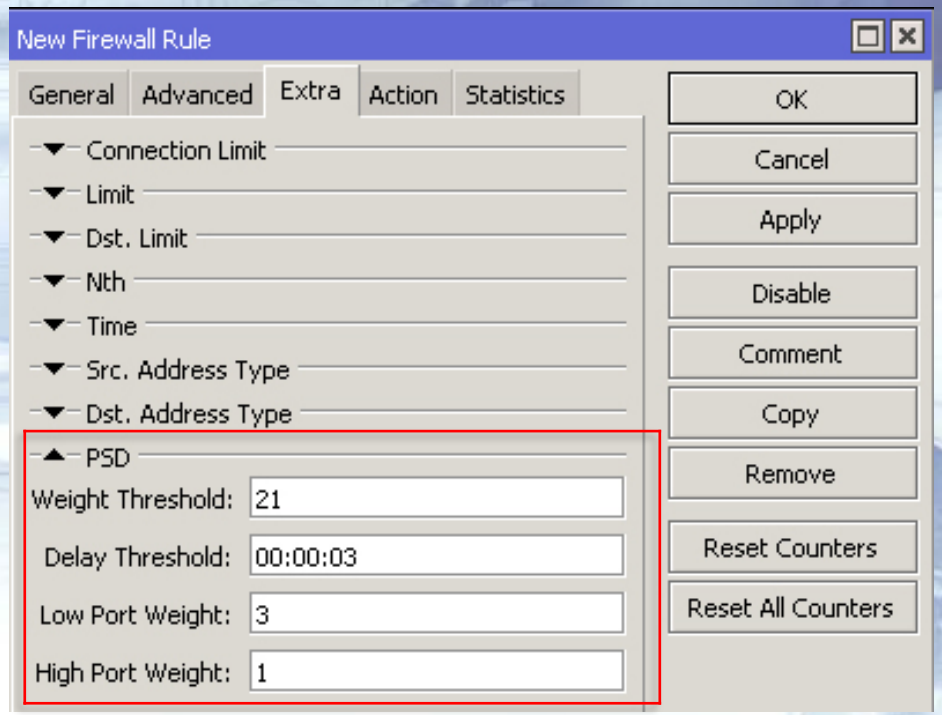
Ping 0:0 y 8:0

Traceroute 11:0 y 3:3

Pat MTU Dsicovery 3:4

INOVA

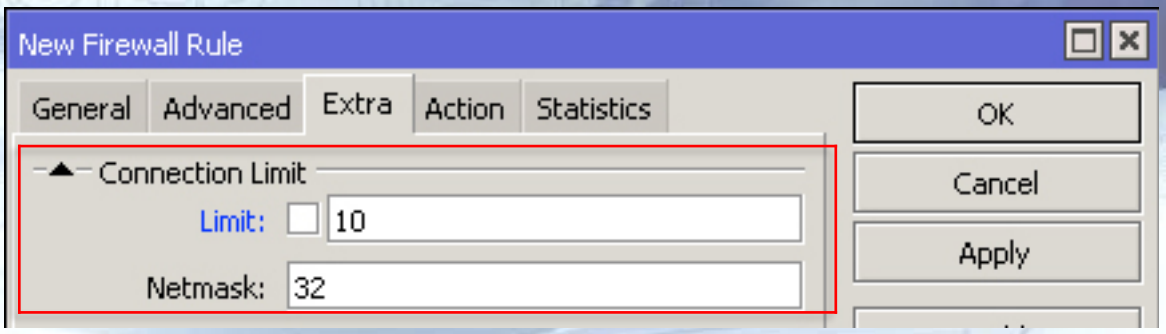
Port Scan

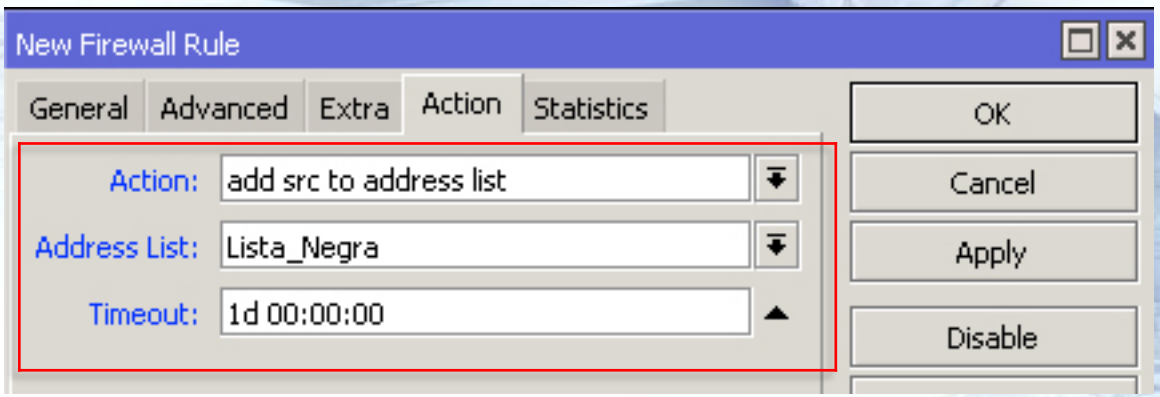


Es una Prueba secuencial buscando puertos abiertos
Puertos bajos 0 al 1023
Puertos altos 1024 al 65535

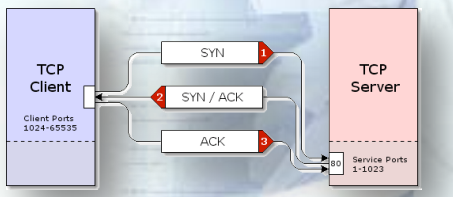
INOVA

DoS Attack

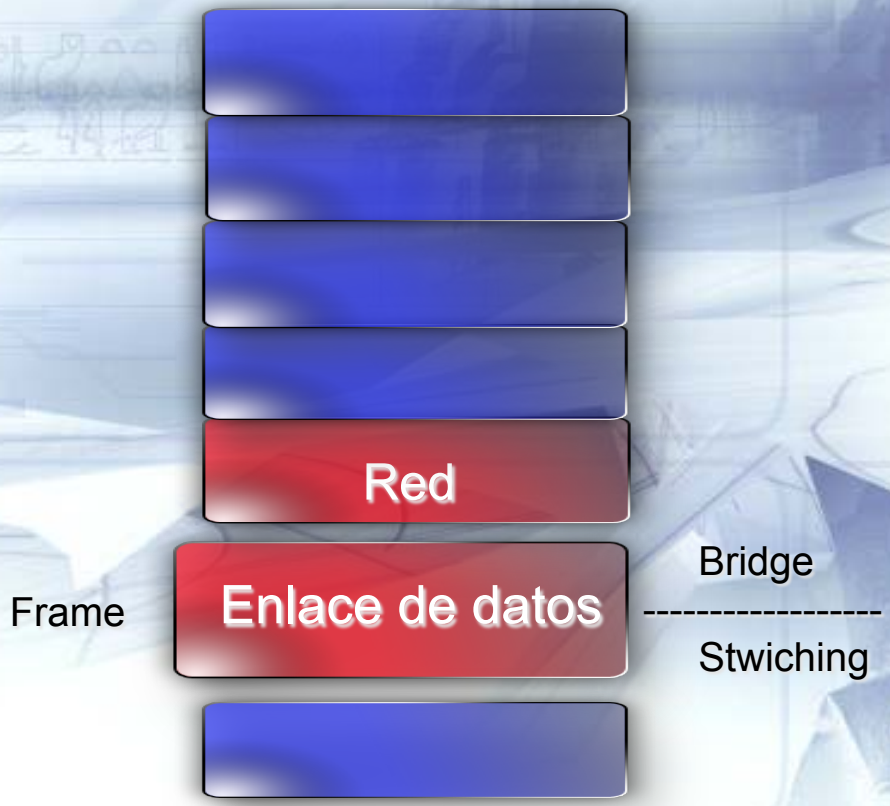




Un ataque de DoS es consumir los recursos del sistema, Usualmente es atacado con paquetes de requisición de conexiones TCP/SYN

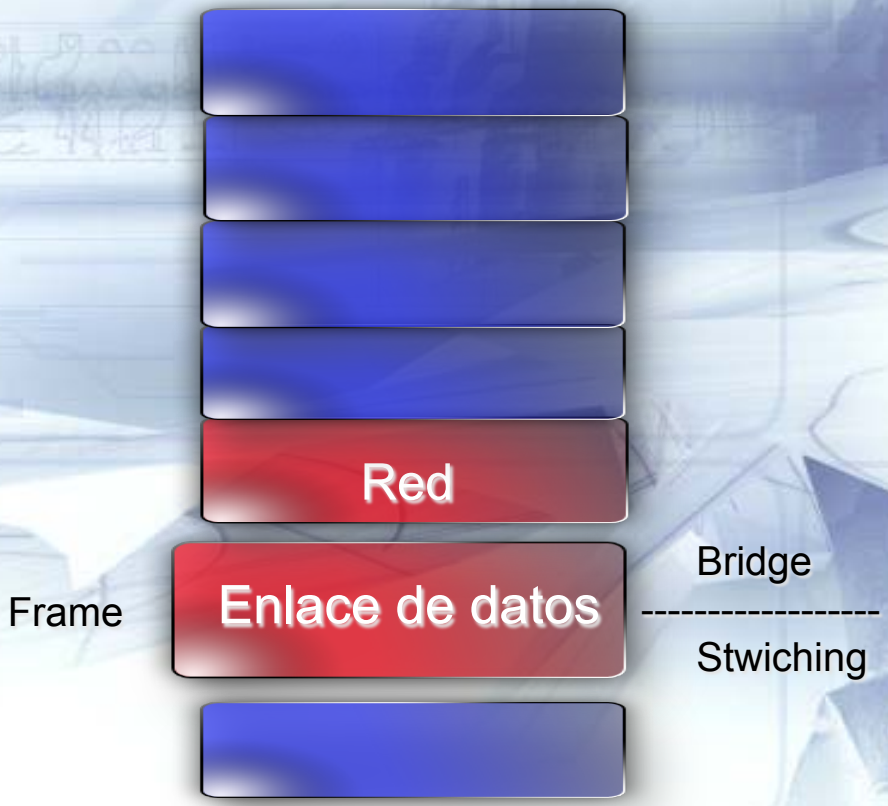


Modelo OSI



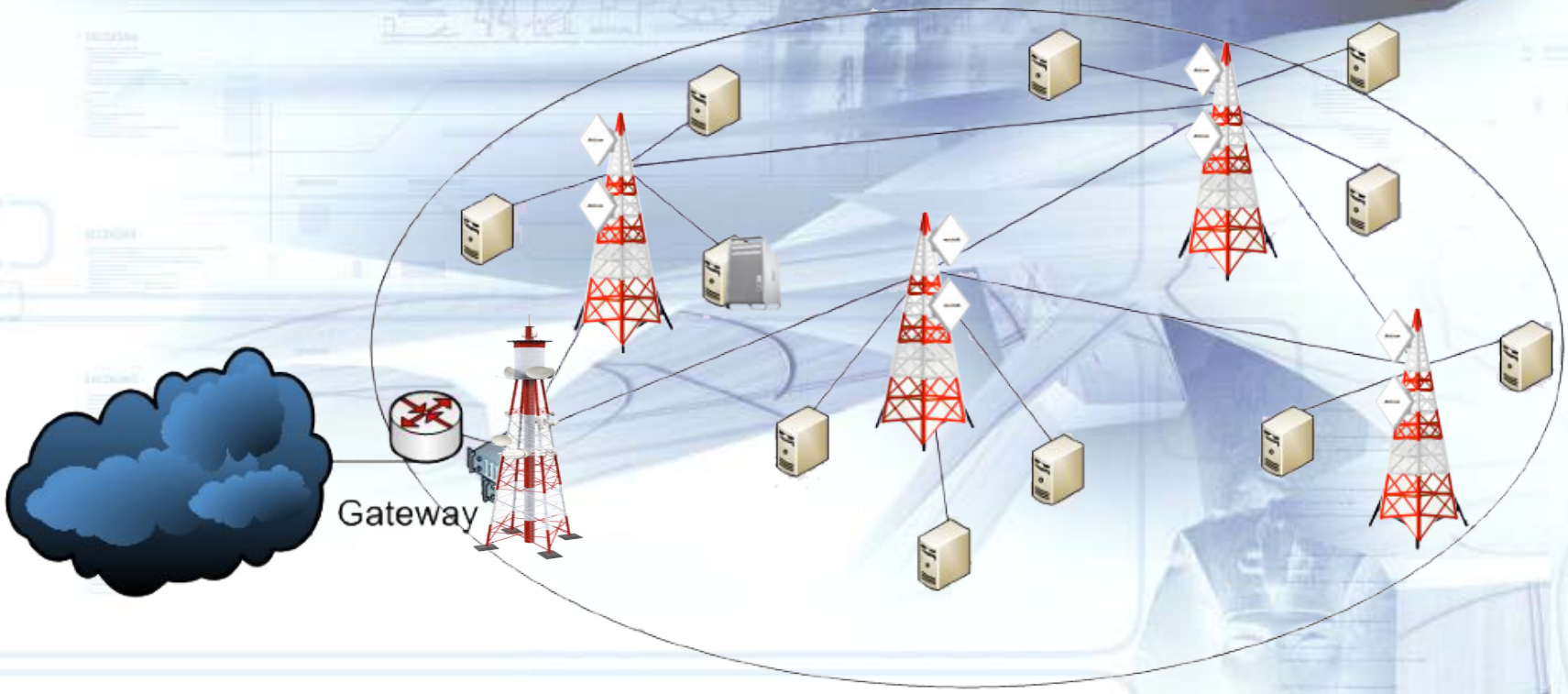
El Stwich mantiene una tabla con las MAC conectado a ella relacionándolo con la puerto donde fueron aprendida, CAM Table es limitado

Modelo OSI



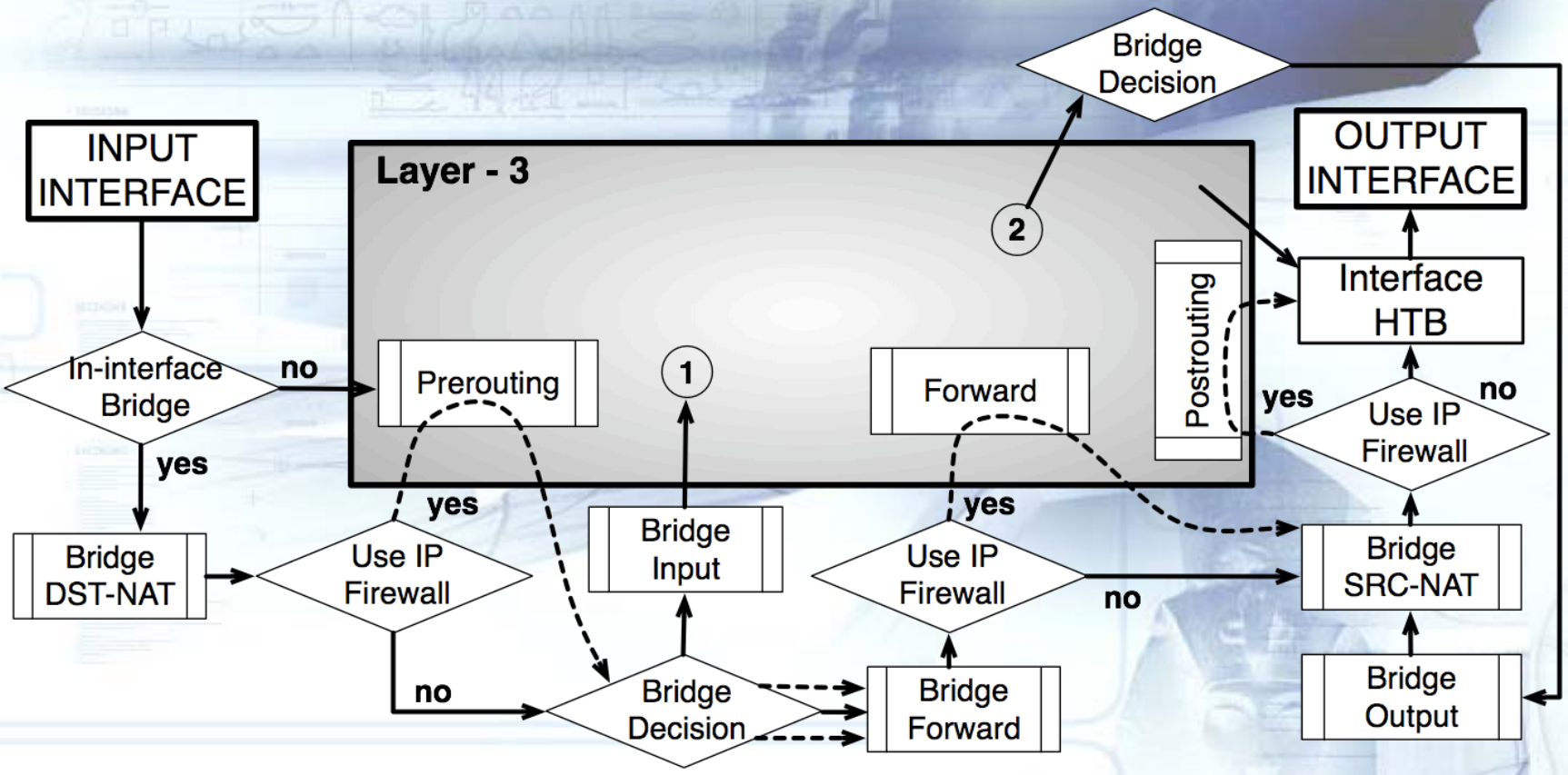
El Bridge mantiene una tabla con las MAC conectado a ella relacionándolo con la puerto donde fueron aprendidos, esos MACs son repasados en la otras bridges

Red en Capa 2



El Gateway de los clientes es el Gateway de borde.
Existe un dominio de Broadcast

Bridge


Bridge Decision
INPUT INTERFACE
Layer - 3
OUTPUT INTERFACE
2
Postrouting
Interface HTB
In-interface Bridge
no
Prerouting
1
Forward
yes
Use IP Firewall
no
yes
yes
yes
Bridge DST-NAT
Use IP Firewall
Bridge Input
Use IP Firewall
Bridge SRC-NAT
no
no
Bridge Decision
Bridge Forward
Bridge Output

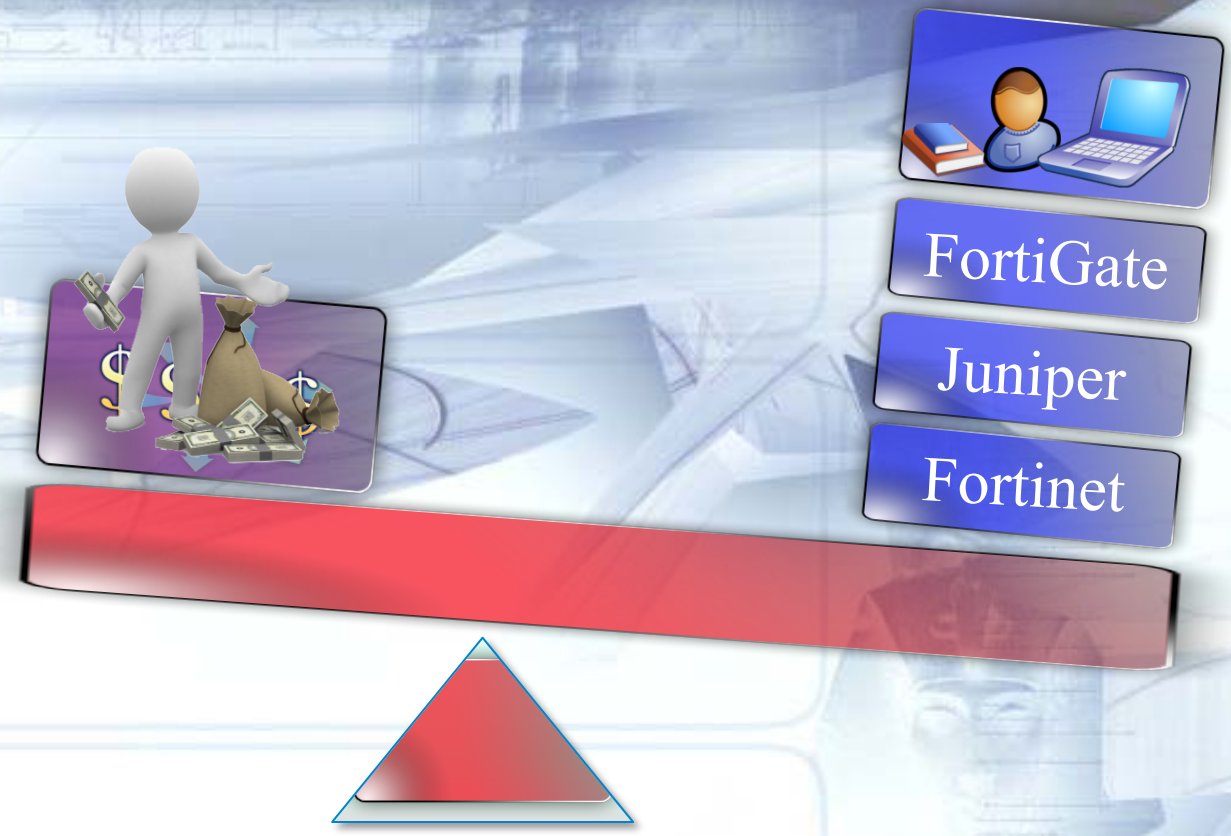
Inundacion de la tabla de Hosts

(MAC Flooding)

Inanicion de Redes DHCP
(DCHP Starvation)

* El atacante genera numerosos pedidos DHCP y cumple con todas las fases del proceso hasta obtener un IP

* El atacante genera numerosos pedido de DHCP perno no confirma



Una historia común

INOVA

Una historia común

INOVA

GRACIAS POR SU ATENCION!!!!

Contactos

Mail: wrojas@inova.com.bo
Web: www.inova.com.bo
Tel: 591-2-2906508
Cel: 591-72540809
Ciudad: La Paz / Santa Cruz - Bolivia