MPLS/VPLS para ISP

poniente Alfredo Giordano

05/09/2014 1.30PM

MUM MEXICO 2014

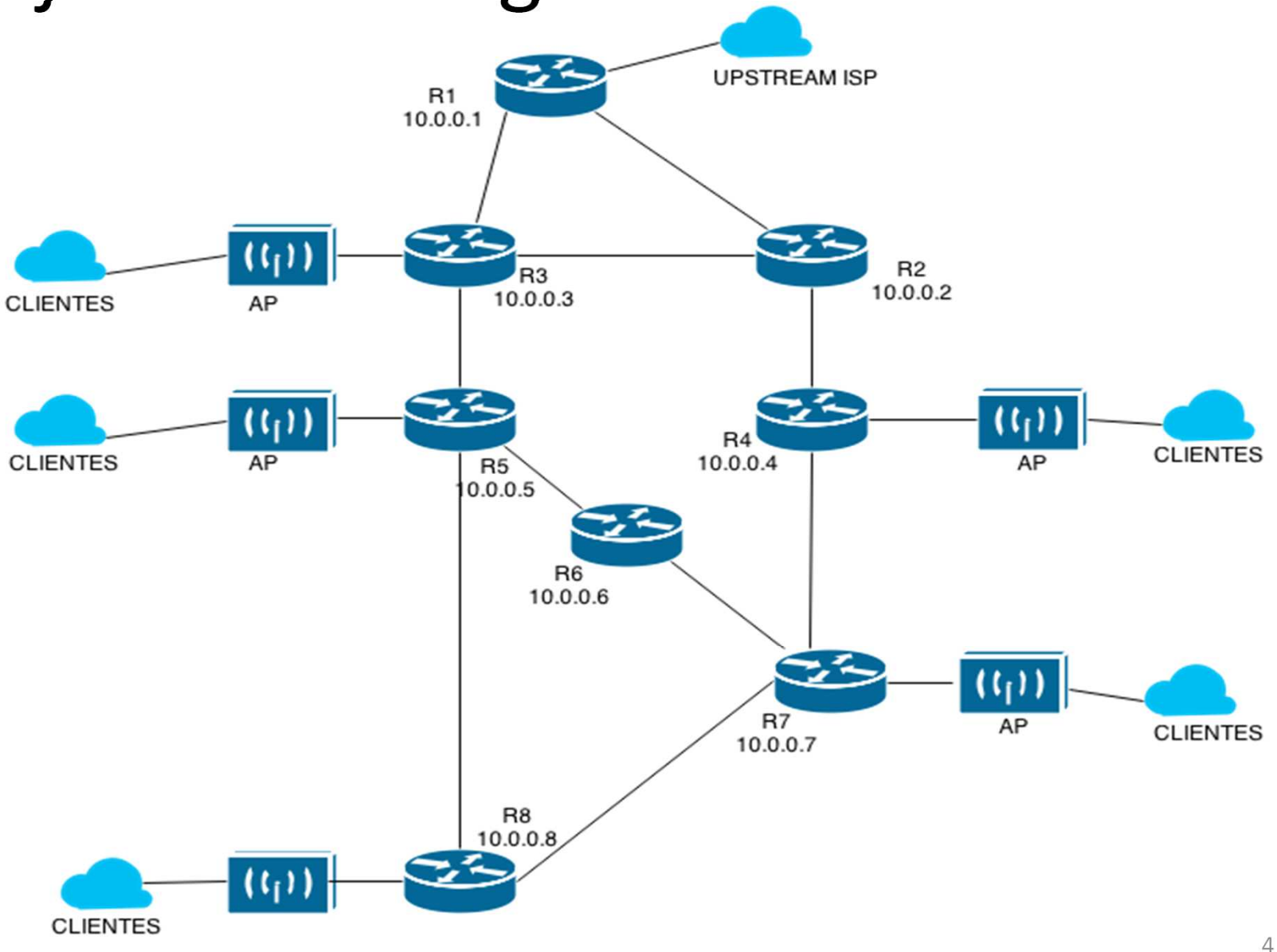
Alfredo Giordano

- Graduado en Ingeniería electrónica en Politécnico de Torino (Italia) y UIC de Chicago, Illinois (USA)
- Consultor y Trainer certificado por MikroTik
- Consultor certificado por Cisco y otros
- Trabajando en Telecomunicaciones desde el 2001
- Miembro activo de RIPE-NCC
  (Réseaux IP Européens Network Coordination Centre)
- Carrier ISP CEO y designer
- Especializado en Routing, QoS, WAN access, wireless

Objetivos

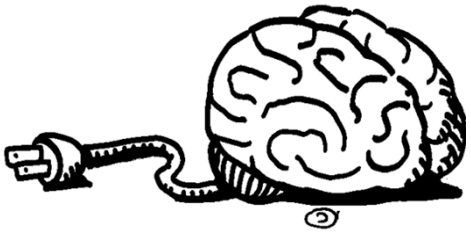
- Construcción de una red de transporte y acceso para ISP performante, modular y escalable
- Racionalizar el uso de los recursos IP
- Minimizar los posibles problemas de seguridad
- Optimizar la gestión de usuarios por medio de un único punto de autenticación y manejo de cuentas

Objetivos – Diagrama de red



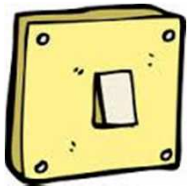
Herramientas:

- Cerebro

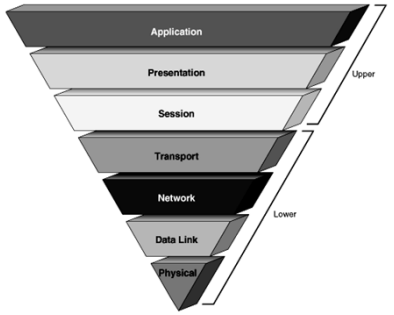


- MikroTik

- MPLS



- PPPoE



Modelo OSI

- OSPF

- VPLS

OSPF

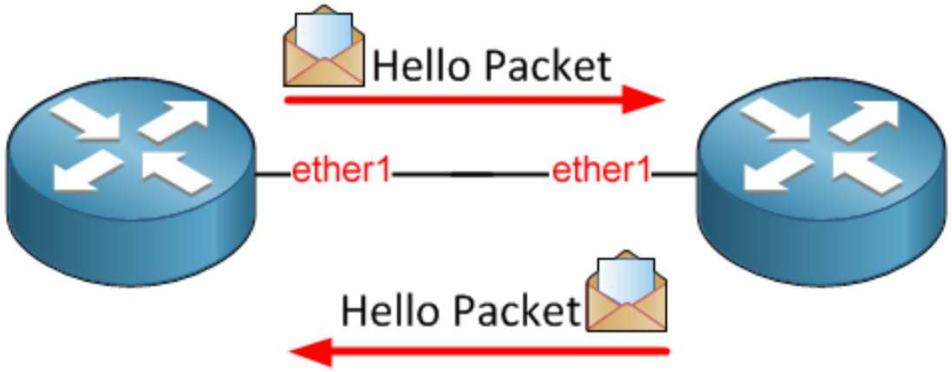
Open Shortest Path First

Panorámica OSPF

- OSPF es un protocolo de routing (IGP) dinámico basado en el estado del link (LSA)
- OSPF detecta los cambios en la topología de la red como la caída de un link o de un nudo, y converge (cuando posible) en una nueva ruta de red en unos segundos
- No usa TCP/IP para transportar la información del protocolo (usa protocolo IP 89)
- Soporta Jerarquías métrica y agregación de rutas

Panorámica OSPF

- Cuando activamos OSPF nuestro router empieza a enviar paquetes de Hello.
- Un paquete de Hello es como un mail que contiene:

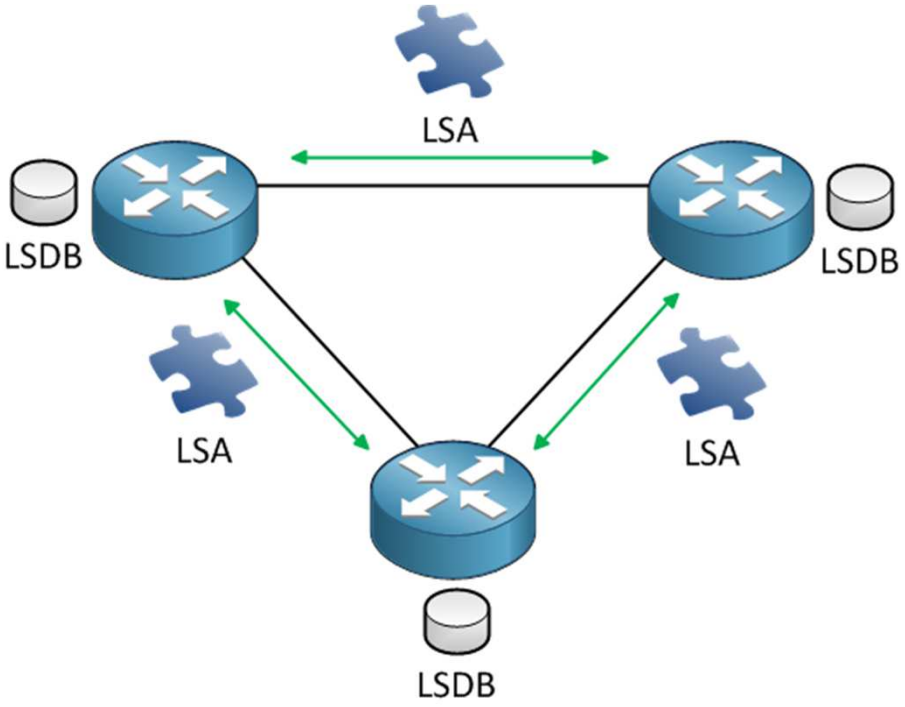


  - RouterID
  - Intervalo de Hello
  - Vecinos (Neighbors)
  - Prioridad del router
  - Información de autenticación

- Si también se recibe un paquete de Hello compatible desde otro router se vuelven vecinos y pueden intercambiar información de LSA

Panorámica OSPF

- En practica OSPF para determinar la tabla de routing se basa sobre el estado de los enlaces de cada router. Dicho estado es comunicado a los demás routers del AS
- Así como en un rompecabezas todas los LSA constituyen el LSDB
- Si no se especifica MikroTik usa como RouterID la IP de valor mas bajo en el sistema
- Es buena costumbre asignar una IP a una interfaz virtual y usar dicha dirección como RouterID



Ventajas de OSPF

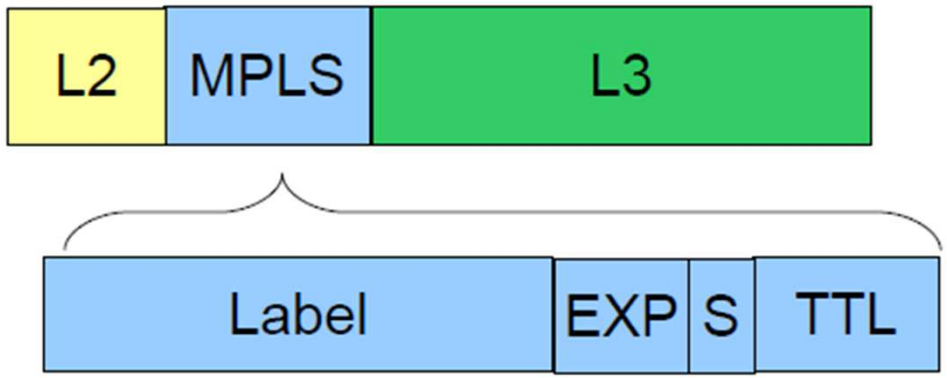
- Rápido de implementar y fácil de depurar
- Mas de 50 routers por área
- Provee redundancia
- Nos permite dar preferencia a un enlace con respecto a otro
- Puede proveer load balancing
- Puede ser usado para routing asimétrico

MPLS

Multi Protocol Label Switching

Panorámica MPLS

- MPLS no es un protocolo de routing porque la decisión para “forwardear” el paquete no se toma en base al encabezado IP. La decisión se toma en base a una etiqueta que esta aplicada al paquete.
- Desde el punto de vista del funcionamiento MPLS es mucho mas similar a VLAN que a un protocolo de routing
- A veces se define un protocolo de capa 2.5 porque las etiquetas MPLS se posicionan entre el encabezado L2 y L3

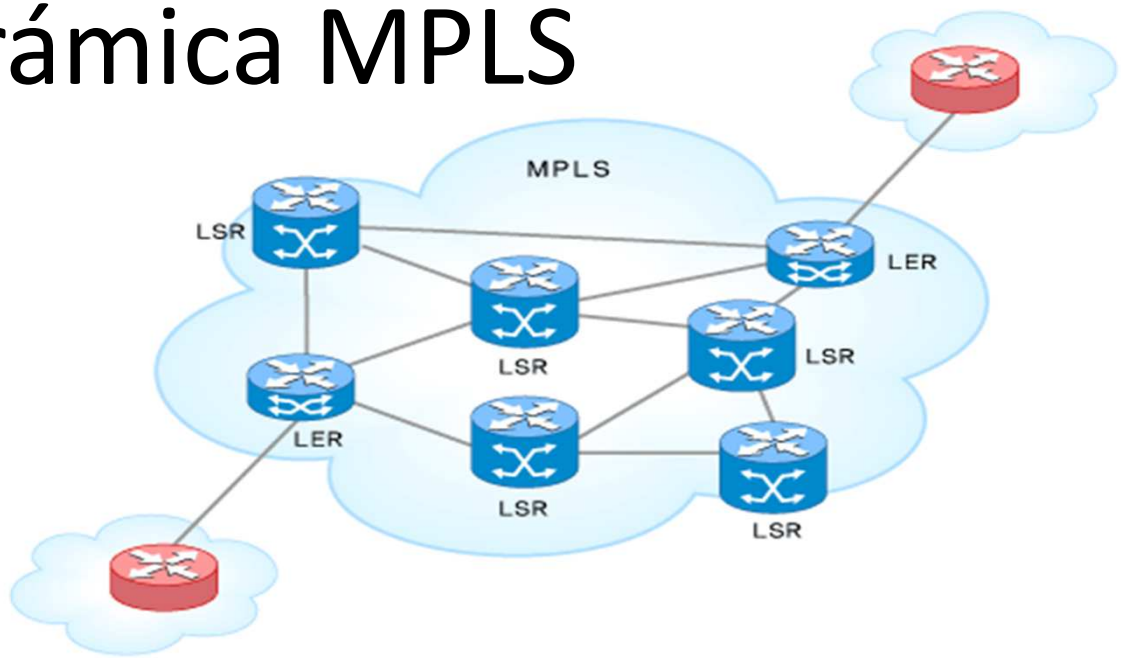


Panorámica MPLS

- En MPLS cada router asigna sus propias etiquetas por cada prefijo en la tabla de ruteo
- Por medio de LDP (Label Distribution Protocol) las etiquetas MPLS pueden ser distribuidas “auto-mágicamente”
- De esta forma cada router esta informado de las asignaciones de los demás
- ¡CUIDADO! LDP requiere de conectividad TCP/IP

➢ Es decir necesitamos que nuestra red L3 sea completamente operacional para implementar LDP

Panorámica MPLS



- En MPLS un router cuando recibe un paquete puede tomar tres acciones:
  - Insertar una etiqueta
  - Cambiar una etiqueta
  - Quitar la etiqueta
- Los LER (Label Edge Router) Pueden insertar o quitar una etiqueta
- Los LSR (Label Switch Router) solo cambian la etiqueta

➢ Nota: a segunda del camino el mismo router puede actuar como LER o LSR

Panorámica MPLS

- El trafico MPLS en los LSR es switched! Entonces:
- No pasa por el firewall y menos por mangle
- No pasa por NAT
- No pasa por QoS

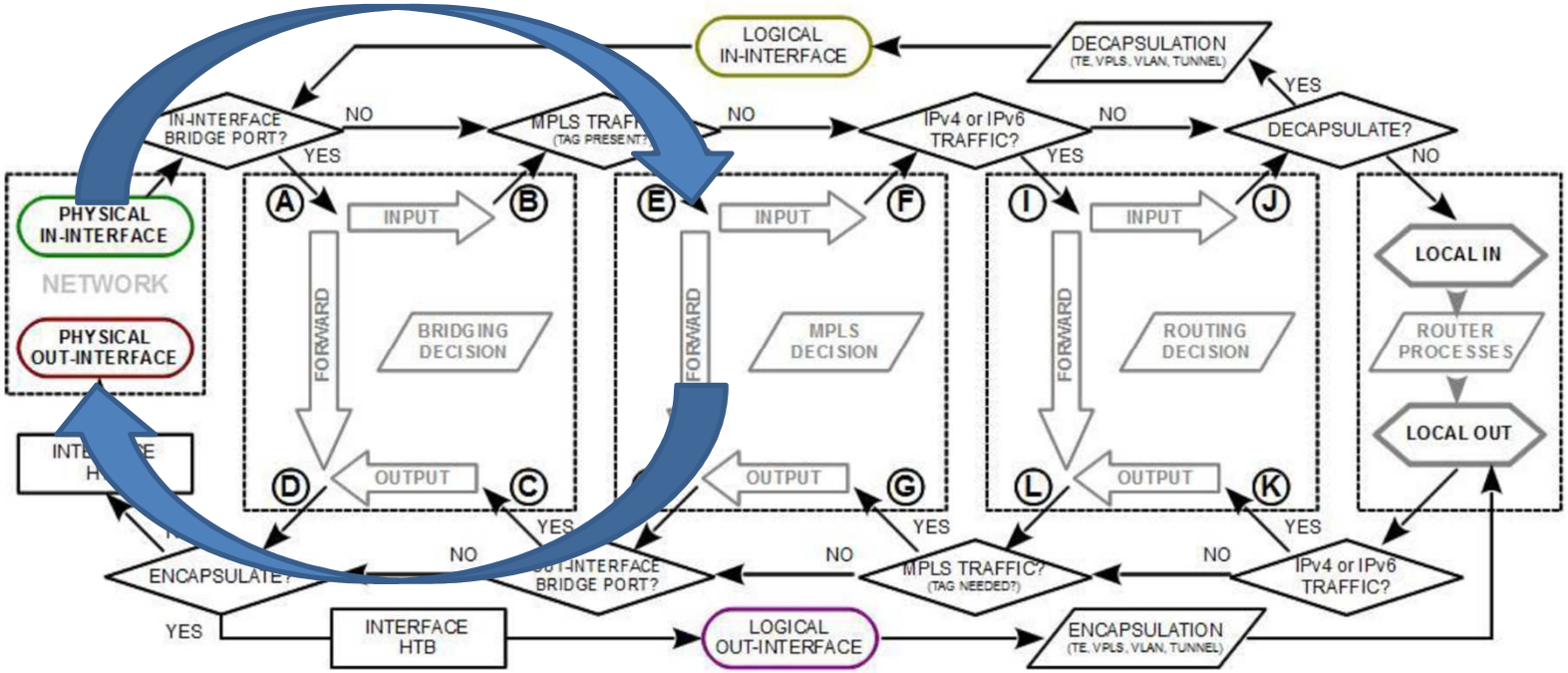
Nota: En los LER si pasa por el sistema de routing

Panorámica MPLS - PHP

- PHP (Penultimate Hop Popping) es la característica de MPLS que le permite a un LSR de remover las etiquetas cuando sabe que el siguiente switch MPLS no necesitara dicha información
- MPLS PHP
- El PHP se implementa por razones de rapidez sin PHP los LER siempre tendrían que checar 2 tablas (tabla MPLS y tabla de IP routing)

Ventajas de MPLS

- Principal beneficio: eficiencia del proceso de forwarding



- Soporta transporte de QoS
- Posibilidad de Túneles VPN fácilmente escalables
- Posibilidad de esconder la topología de red
- Y mas...

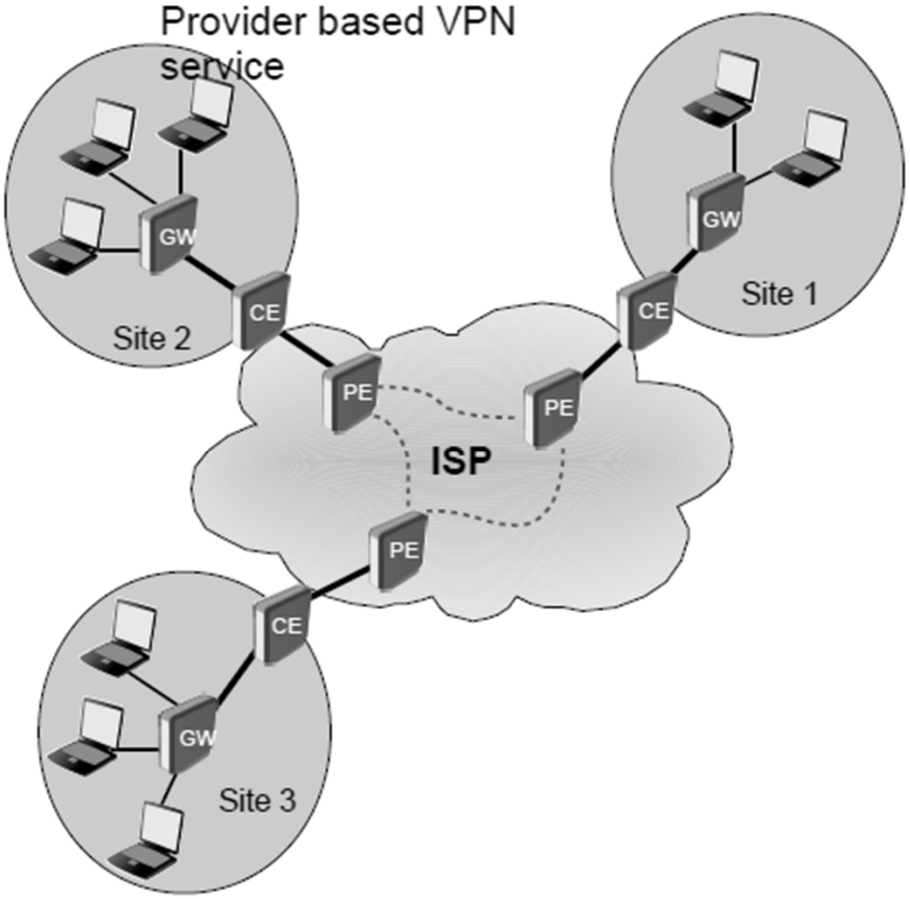
VPLS

Virtual Private Lan Service

Panorámica de VPLS

- VPLS es un método para crear túneles transparentes L2 basados en MPLS.
- Un túnel VPLS se presenta al router como una interfaz separada (exactamente como sucede para EoIP)
- Un túnel VPLS agrega una etiqueta adicional al frame MPLS

Panorámica de VPLS



- VPLS se puede considerar un tipo de VPN (Red Privada Virtual) basada en el proveedor en lugar que en el usuario final.
- Todo el trabajo de networking sucede en el interior de la red del ISP.
- Además de poder ser usado para la red de acceso también se puede usar para transportar segmentos Ethernet distantes.

Ventajas de VPLS

- VPLS es muy rápido porque no encripta ni encapsula
- si tomamos nuestras precauciones tampoco fragmenta
- Solo agrega al frame Ethernet 2 etiquetas
- Cada nuevo sitio solo necesita la configuración del router
- Almeno el 60% mas rápido que EoIP

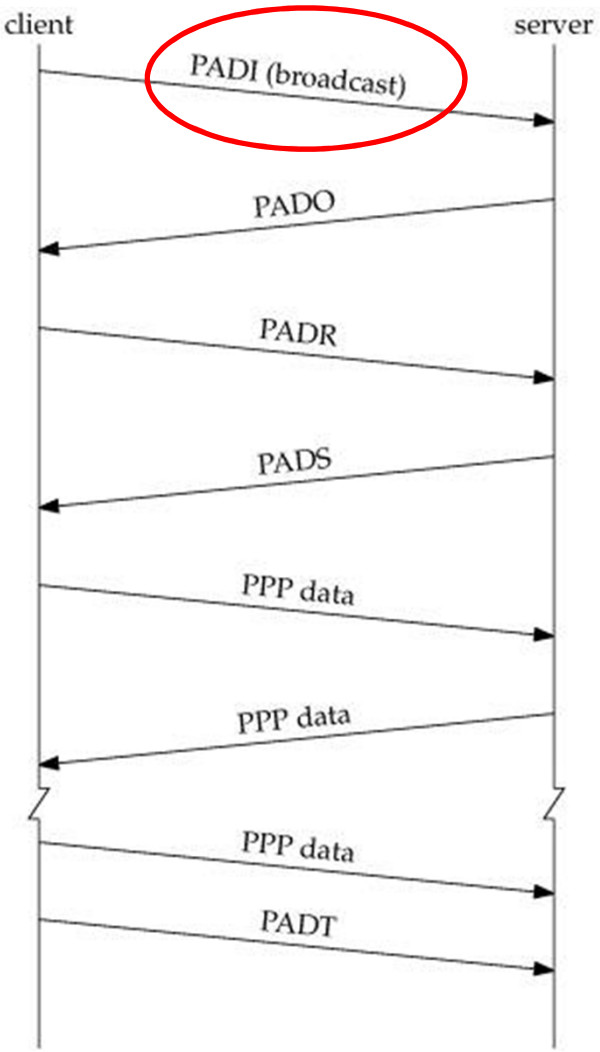
PPPoE

Point to Point Protocol over Ethernet

Panorámica de PPPoE

- El protocolo PPPoE (Point to Point Protocol over Ethernet) encapsula los frames PPP a dentro de un frame Ethernet.
- PPPoE construye un túnel punto a punto entre 2 dispositivos de red Ethernet
- PPPoE Actualmente es principalmente usado en los ISPs para controlar la conexión del cliente para xDSL, Cable, Wireless y cualquier red Ethernet que necesite trabajar con Authentication, Athorization and Accounting (AAA) a través de un server RADIUS.

Panorámica de PPPoE



- PPPoE necesita conexión directa con entre el Concentrador de Accesos y el cliente (mismo dominio de broadcast)
- En redes pequeñas esto no constituye un problema.

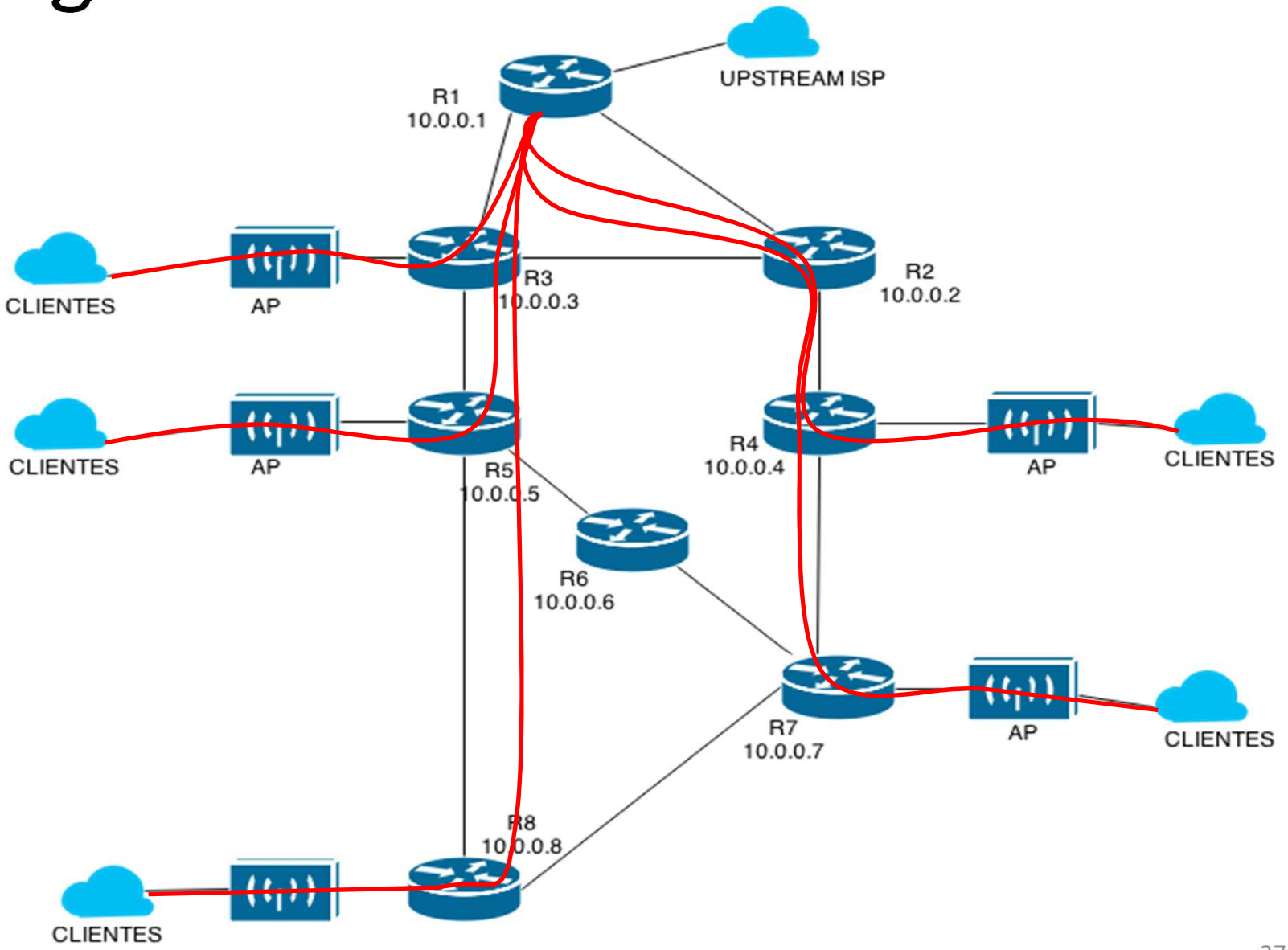
Panorámica de PPPoE

- En redes un poco mas desarrolladas un único dominio de broadcast no es una solución viable
- Rougue DHCP servers
- MAC spoofing
- Anillos (loops) L2
- Exceso de trafico broadcast

Ventajas de PPPoE

- Las mayores ventajas que los ISPs reciben desde PPPoE son ligadas al protocolo PPP y al facil manejo de AAA
- Otra notable ventaja es que PPPoE permite que cada cliente se encuentre en su propio segmento de broadcast

Diagrama de red - Tuneles



Implementación R(n)

- General

```
/system identity set name=R1
/interface bridge add name=lo
/ip address add address=10.0.0.1/32 interface=lo comment=routerID
/ip address add address=172.16.100.1/30 interface=ehter1
comment=R1_R2
/ip address add address=172.16.100.5/30 interface=ehter1
comment=R1_R3
```

- **OSPF**

```
/routing ospf instance set 0 distribute-default=always-as-type-1
redistribute-connected=as-type-1 router-id=10.0.0.1
/routing ospf interface add interface=ether1 network-type=point-
to-point
/routing ospf interface add interface=ether2 network-type=point-
to-point
/routing ospf interface add add network-type=broadcast
passive=yes
/routing ospf network add area=backbone network=172.16.100.0/24
```

Implementación R(n)

- MPLS

```
/mpls set dynamic-label-range=1000-0
/mpls interface set 0 mpls-mtu=1596
/mpls ldp set enabled=yes lsr-id=10.0.0.1 transport-
address=10.0.0.1
/mpls ldp interface add interface=ether1
/mpls ldp interface add interface=ether2
```

Implementación R(1)

- **VPLS**

```
/interface vpls add disabled=no l2mtu=1508 name=R2_CUSTOMERS
remote-peer=10.0.0.2 vpls-id=1:2
....
/interface vpls add disabled=no l2mtu=1508 name=R8_CUSTOMERS
remote-peer=10.0.0.8 vpls-id=1:8
```

- **PPPoE**

```
/interface pppoe-server server add disabled=no
interface=R2_CUSTOMERS keepalive-timeout=35 max-mru=1500 max-
mtu=1500 one-session-per-host=yes
....
/interface pppoe-server server add disabled=no
interface=R8_CUSTOMERS keepalive-timeout=35 max-mru=1500 max-
mtu=1500 one-session-per-host=yes
```

Implementación R(1)

- **PPPoE (Cont.)**

```
/ppp profile set 0 dns-server=8.8.8.8,8.8.4.4 local-
address=10.10.10.1 only-one=yes queue-type=default-small rate-
limit=512k/7M remote-address=customers-pool use-vj-compression=no
/ip pool add name=customers-pool ranges=192.168.0.1-192.168.3.254
/ppp aaa accounting=yes interim-update=60 use-radius=yes
```

- **Radius**

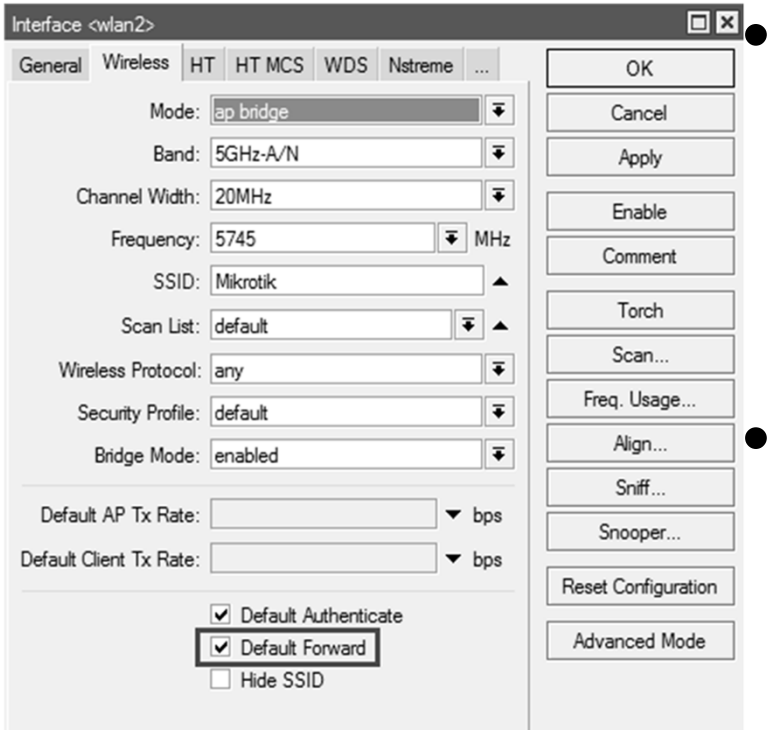
```
/radius add address=172.16.1.1 secret=xxxxxx service=ppp src-
address=10.0.0.1 timeout=5s
```

- **Upstream Provider: default route, nat, etc...**

```
/import file-name=upstream_isp.rsc
```

Consideraciones L2

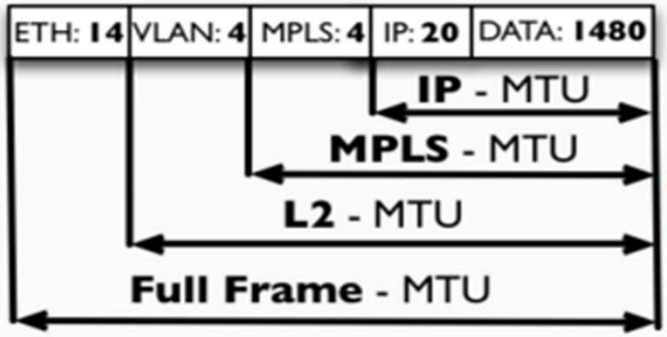
- PPPoE solo necesita conectividad L2 entre el AC y el cliente.



- Para proteger los clientes desde ellos mismos es buena idea que estén aislados y solo puedan comunicar en L2 con el AC.
- En un link wireless esto se obtiene fácilmente quitando la palomita a **“default-forward”.**

Consideraciones L2

MTU on RouterOS



Mikrotik RouterOS recognizes several types of MTU:

- IP/Layer-3/L3 MTU
- MPLS/Layer-2.5/L2.5 MTU
- MAC/Layer-2/L2 MTU
- Full frame MTU

- Basicamente lo que sucede con un tunel VPLS es que estamos captando un fame ethernet tal cual (raw) y le estamos agregando una etiqueta. Por lo tanto cuando considelamos el MTU deveremos pensar en todo el frame L2. Asi que tendremos:

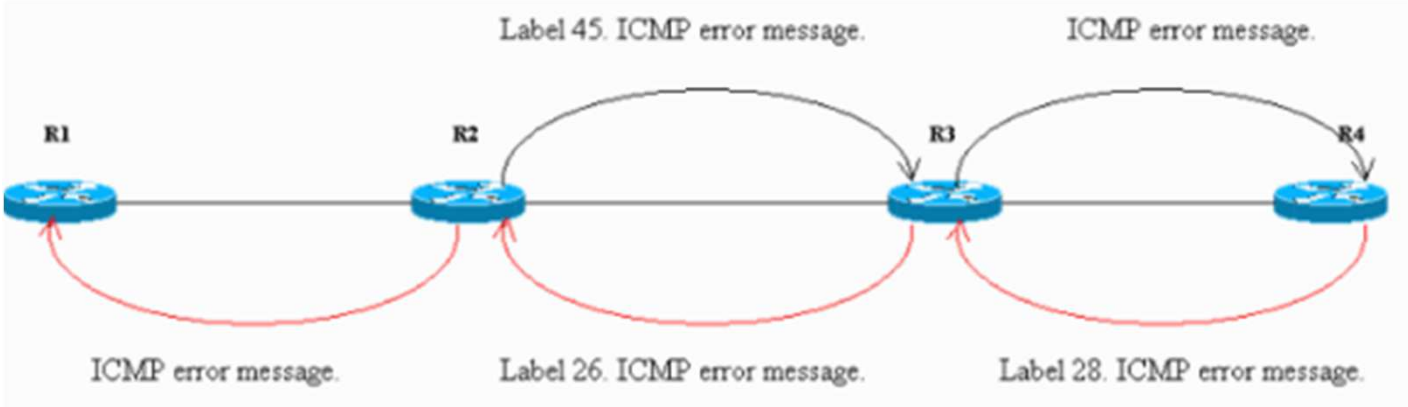
- 1500 byte datos + 8 PPPoE + 14 Ethernet+ 4 MPLS + 4 VPLS = Total 1530

Problemas – L2MTU

- Toda la cadena de transporte (AP, switch, router enlaces dorsales) tiene que soportar la L2MTU de 1530. De lo contrario hay que disminuir el MTU en PPPoE.
- La mayoría de los switches baratos solo soporta max L2MTU de 1514.
- En algunos podemos habilitar “Jumbo Frames” para tener L2MTU mayor de 1514
- Si en algún lado el L2MTU es mas chico de lo que se necesita los frames MPLS se descartaran silenciosamente haciendo difícil la depuración.

Problemas – ICMP

- Los LSR pueden ser equipos de switching que ni siquiera conocen ICMP
- Por esta razón si hay una falla en el camino LS no podemos usar traceroute para determinarla.
- Por lo mismo en traceroute solo reporta el round-trip de todo el camino LS.



Conclusiones

- MPLS y VPLS son muy poderosos y sencillos de configurar pero puede ser muy difícil de depurarlos si no se conoce la forma de como trabajan.
- Si hay algún problema al 99% es algún equipo de la competencia que no soporta un L2MTU suficiente.
- La solución propuesta es la idea de base. Fácilmente es posible mejorar aun la redundancia y las prestaciones.

Fuentes

- MikroTik wiki
- Presentación MPLS de Janis
- Imágenes cortesía de netlessons
- Teoría de MPLS

¡Gracias!

- Preguntas Comentarios y sugerencias
  - Alfredo Giordano (alfredo@tiktrain.com)