Optimix
Network Engineering

MikroTik gobernando redes urbanas FTTx (fibra óptica GPON)

Ing Jorge Filippo

Email: jfilippo@optimix.com.ar

Celu y WhatsApp: +54 9 11 6693 5494

Skype: jorgefilippo

Facebook: https://www.facebook.com/ingjorgefilippo

Objetivos Optimix Network Engineering

- Proveer estrategias de networking infalibles y eficientes.
- Capacitar a los planteles de las redes guiadas.
- Ser un aliado, para desarrollar soluciones y negocios.

Objetivos de esta exposición

- Analizar la gestión a gran escala de redes urbanas gubernamentales.
- Comprender que la gestión de tráfico y control de alta precisión en redes gubernamentales, puede realizarse dentro de la inteligencia MikroTik, independientemente del medio de transporte.
- Compartir con el auditorio la implementación de una red gubernamental en Buenos Aires, controlada por MikroTik, y transportada con GPON.

Planteo conceptual

- La gestión de una red, contempla una temática de transporte, y una temática de servicio.
- Router de Servicio, es la denominación sugerida en Optimix para señalar aquel router que administra el tráfico de los usuarios finales, controlando el contenido, anchos de banda, gestionando las IPs disponibles, y sirviendo las tecnologías de control de acceso (access lists, hotspot, etc…).
- Router de Borde (o Firewall, según su rigurosidad de control), es la denominación sugerida en Optimix para señalar aquel router que posee la/s conexiónes de los proveedores de Internet.
- Pero cuando la temática de transporte, es tercerizada, surge el rol de Router de Transporte, o Core Router (ruter estructural).
- El CoreRouter, es el router que provee la inteligencia de gestión en capa 2, que nos independiza del medio físico que nos transporte, aislando los entornos de broadcast desplegados, segurizando nuestra red.
- Entiéndase que la segurización de la red, implica **desconfiar** de nuestra red de transporte. Porque será gestionada por otra tecnología/proveedor.

Escenario físico original

- Red multiproveedores, con vínculos inalámbricos de baja calidad, conexiones ADSL, y algunos pocos vínculos dedicados.

- Estructura unificada en túneles EoIP, para:

  - Unificar físicamente en un servidor, túneles PPTP viajando por múltiples tecnologías (los túneles EoIP viajan por los PPTPs).

  - Salvaguardar dentro del Municipio (en el servidor PPTP que concentra los EoIP), la gestión de la lógica y el tráfico.

Planteo conceptual

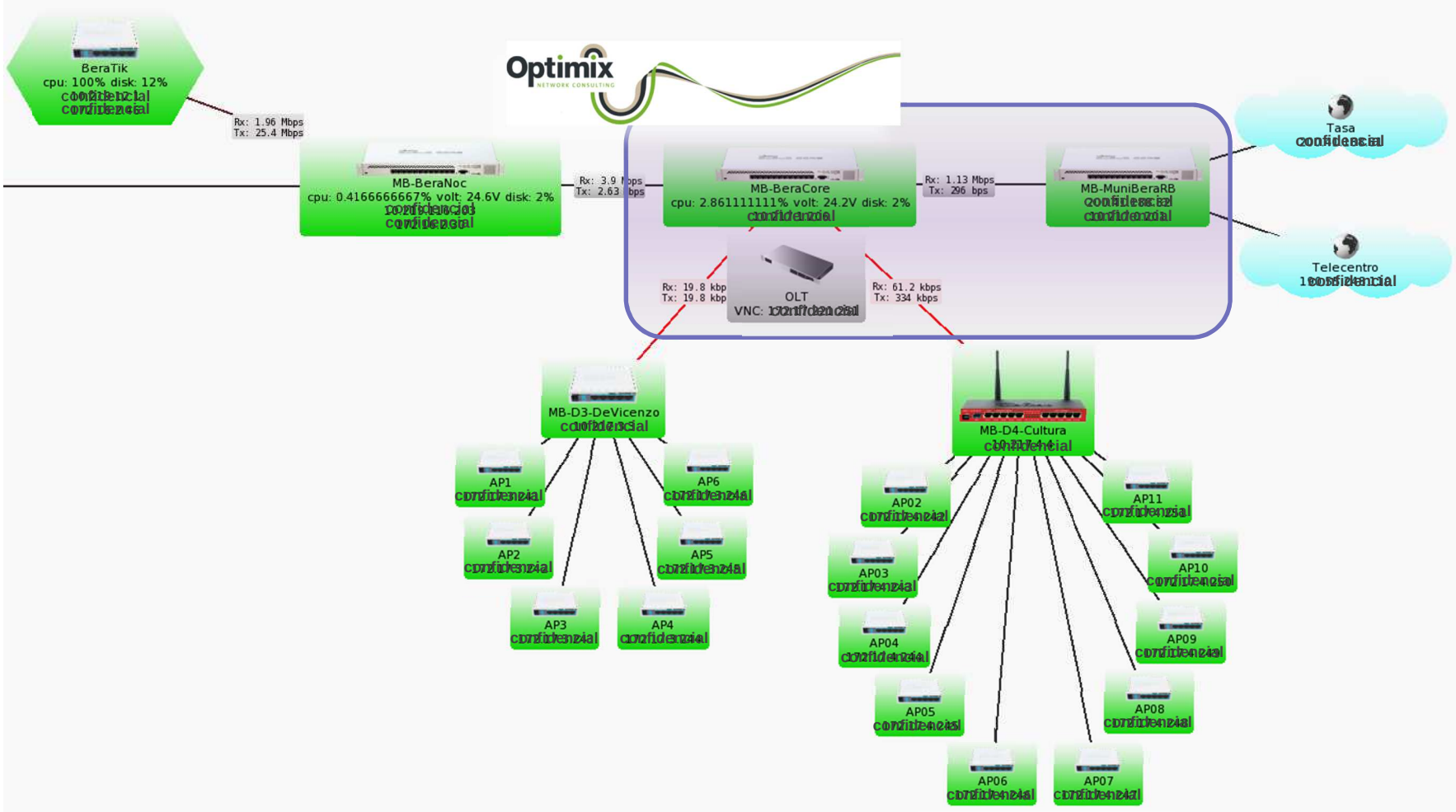
- La administración de vínculos mediante VLANs, permite desenebrar las troncales, para generar un vínculo dedicado a cada MikroTik a partir del router troncal.
- Este router troncal, gestiona las redes de la infraestructura antigua (ethernet), y de la infraestructura nueva (GPON).
- Así, se logró:
  - Una transición suave, gracias al ruteo entre los dos redes (la antigua – ethernet, y la nueva – gpon).
  - Unificar físicamente en un router concentrador, el tráfico de escala urbana.
  - Mantener la administración sobre MikroTik, evitando sufrir de las interfaces engorrosas de las antiguas tecnologías de ruteo.

Planteo conceptual

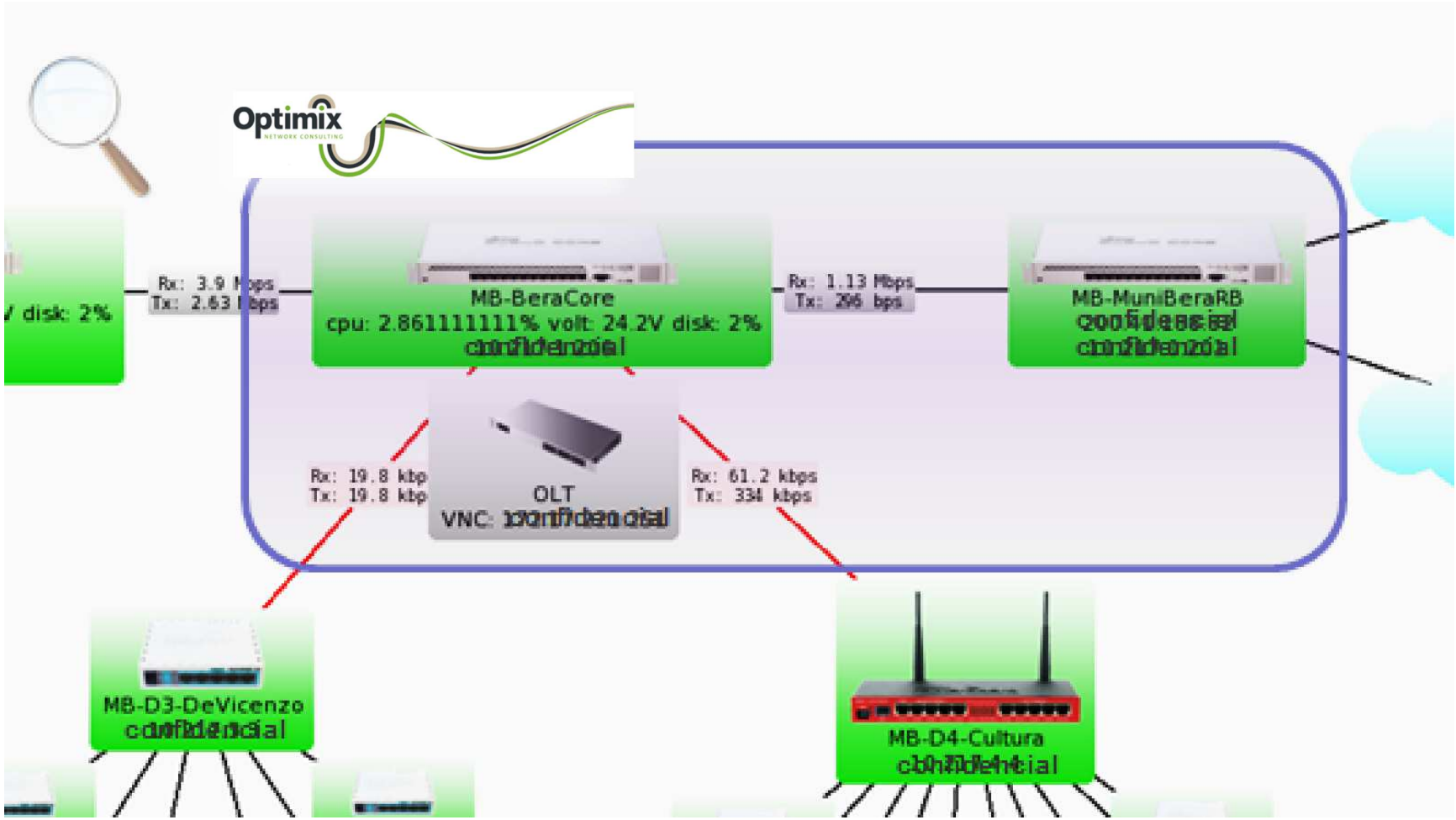
- Se conectan todas las delegaciones mediante un despliegue de fibra GPON (un filamento, con posibilidad de spliteo).
- Todos los vínculos se despliegan mediante spliteo, y se concentran las troncales mayores en la OLT.
- Esta estructura unificada en vínculos de fibra, se administran y relacionan con VLANs.
- Estas VLANs se desanudan en el dispositivo cliente llamado ONU, que posee puertos ethernet mediante los que se trasduce al mundo.


FURUKAWA
BeraCoreRT
GPON OLT FK-OLT-G
38
37
36
35
34
33
32
31
30
27
26

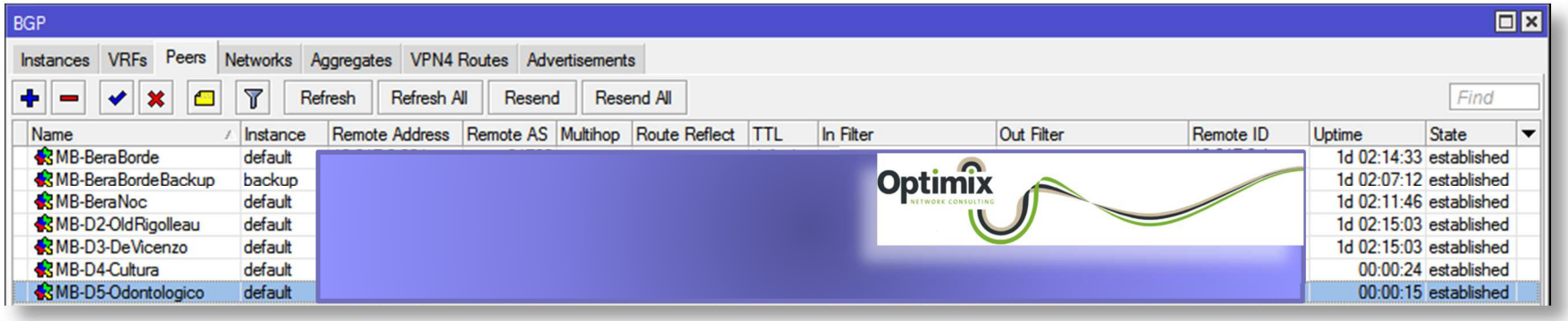
Estructura

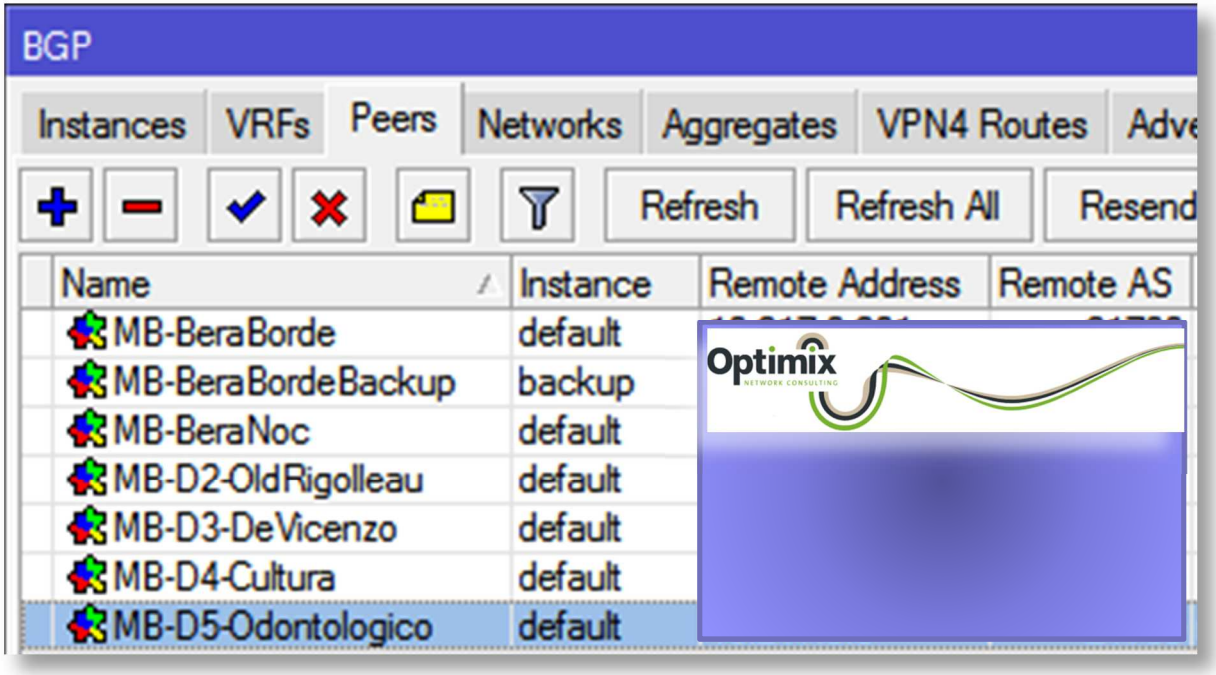

BeraTik
cpu: 100% disk: 12%
Rx: 1.96 Mbps
Tx: 25.4 Mbps
MB-BeraNoc
cpu: 0.4166666667% volt: 24.6V disk: 2%
Rx: 3.9 Mbps
Tx: 2.63 Mbps
MB-BeraCore
cpu: 2.861111111% volt: 24.2V disk: 2%
Rx: 1.13 Mbps
Tx: 296 bps
MB-MuniBeraRB
Tasa
Telecentro
OLT
Rx: 19.8 kbps
Tx: 19.8 kbps
Rx: 61.2 kbps
Tx: 334 kbps
MB-D3-DeVicenzo
MB-D4-Cultura
AP1
AP2
AP3
AP4
AP5
AP6
AP02
AP03
AP04
AP05
AP06
AP07
AP08
AP09
AP10
AP11

Estructura

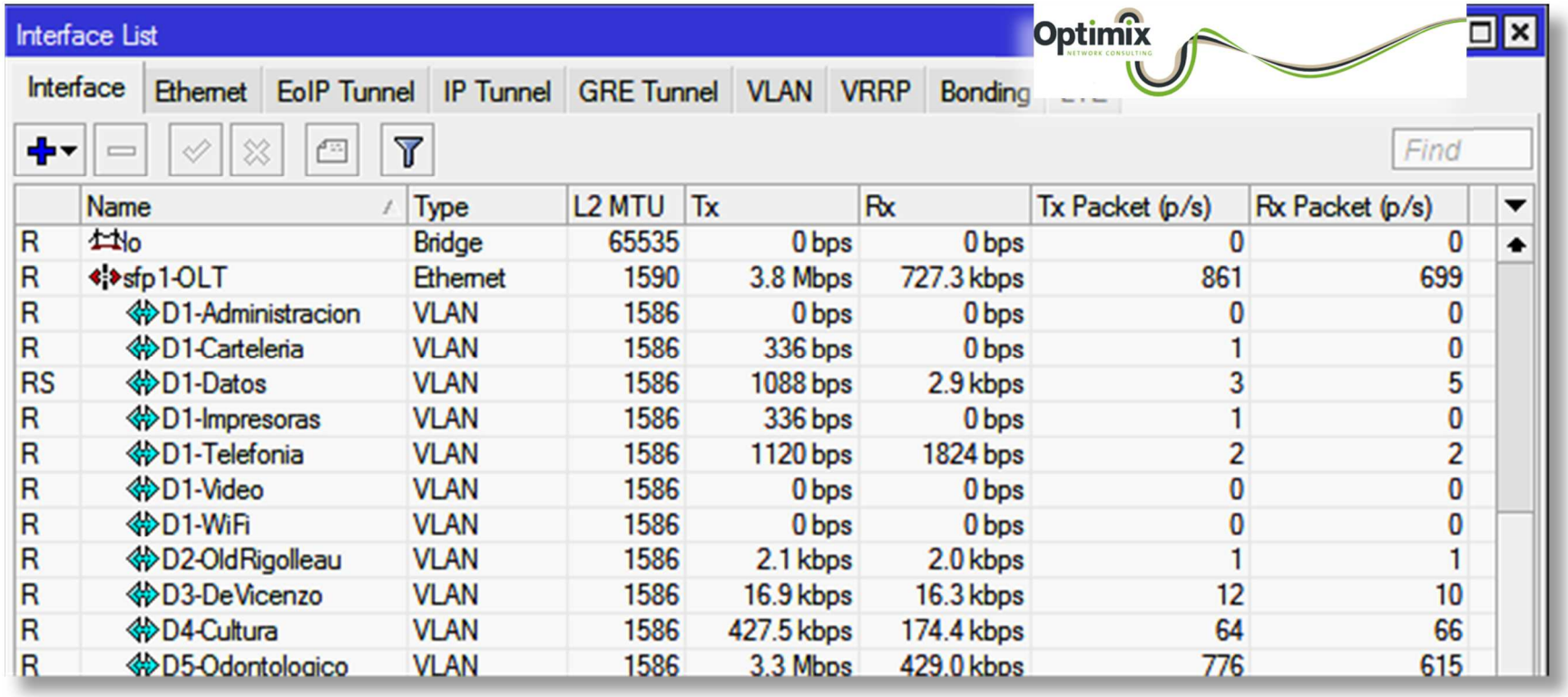

Optimix
Rx: 3.9 Mbps
Tx: 2.63 Mbps
MB-BeraCore
cpu: 2.861111111% volt: 24.2V disk: 2%
Rx: 1.13 Mbps
Tx: 296 bps
MB-MuniBeraRB
Rx: 19.8 kbps
Tx: 19.8 kbps
OLT
Rx: 61.2 kbps
Tx: 334 kbps
MB-D3-DeVicenzo
MB-D4-Cultura

Router Core


BGP
Instances
VRFs
Peers
Networks
Aggregates
VPN4 Routes
Advertisements
Refresh
Refresh All
Resend
Resend All
Find
Name
Instance
Remote Address
Remote AS
Multihop
Route Reflect
TTL
In Filter
Out Filter
Remote ID
Uptime
State
MB-BeraBorde default 1d 02:14:33 established
MB-BeraBordeBackup backup 1d 02:07:12 established
MB-BeraNoc default 1d 02:11:46 established
MB-D2-OldRigolleau default 1d 02:15:03 established
MB-D3-DeVicenzo default 1d 02:15:03 established
MB-D4-Cultura default 00:00:24 established
MB-D5-Odontologico default 00:00:15 established
Optimix

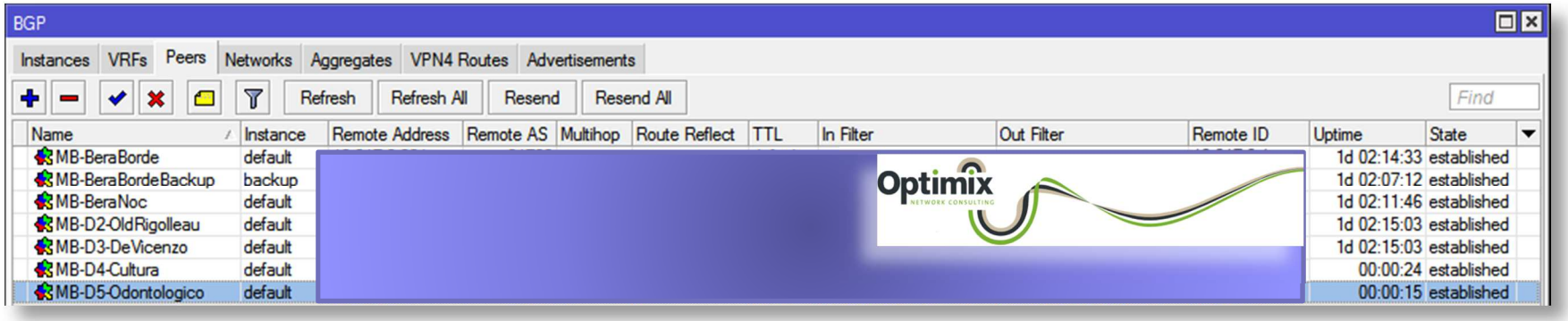

BGP
Instances
VRFs
Peers
Networks
Aggregates
VPN4 Routes
Refresh
Refresh All
Resend
Name
Instance
Remote Address
Remote AS
MB-BeraBorde default
MB-BeraBordeBackup backup
MB-BeraNoc default
MB-D2-OldRigolleau default
MB-D3-DeVicenzo default
MB-D4-Cultura default
MB-D5-Odontologico default
Optimix

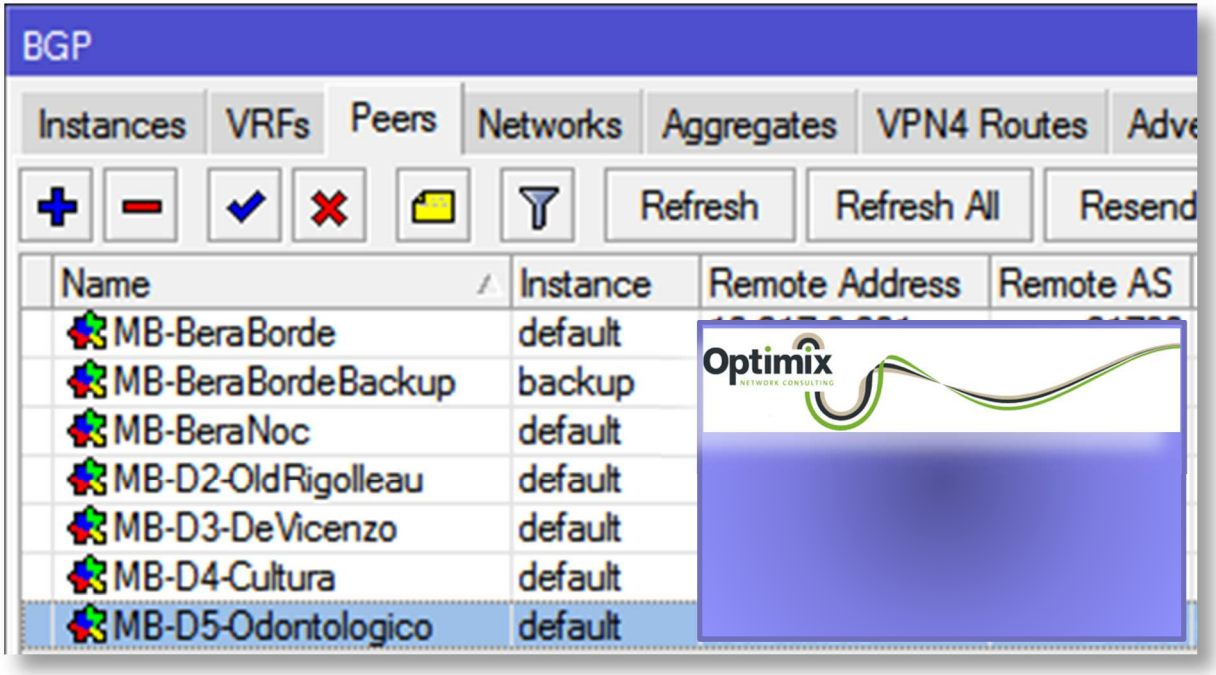
Router Core – VLANs



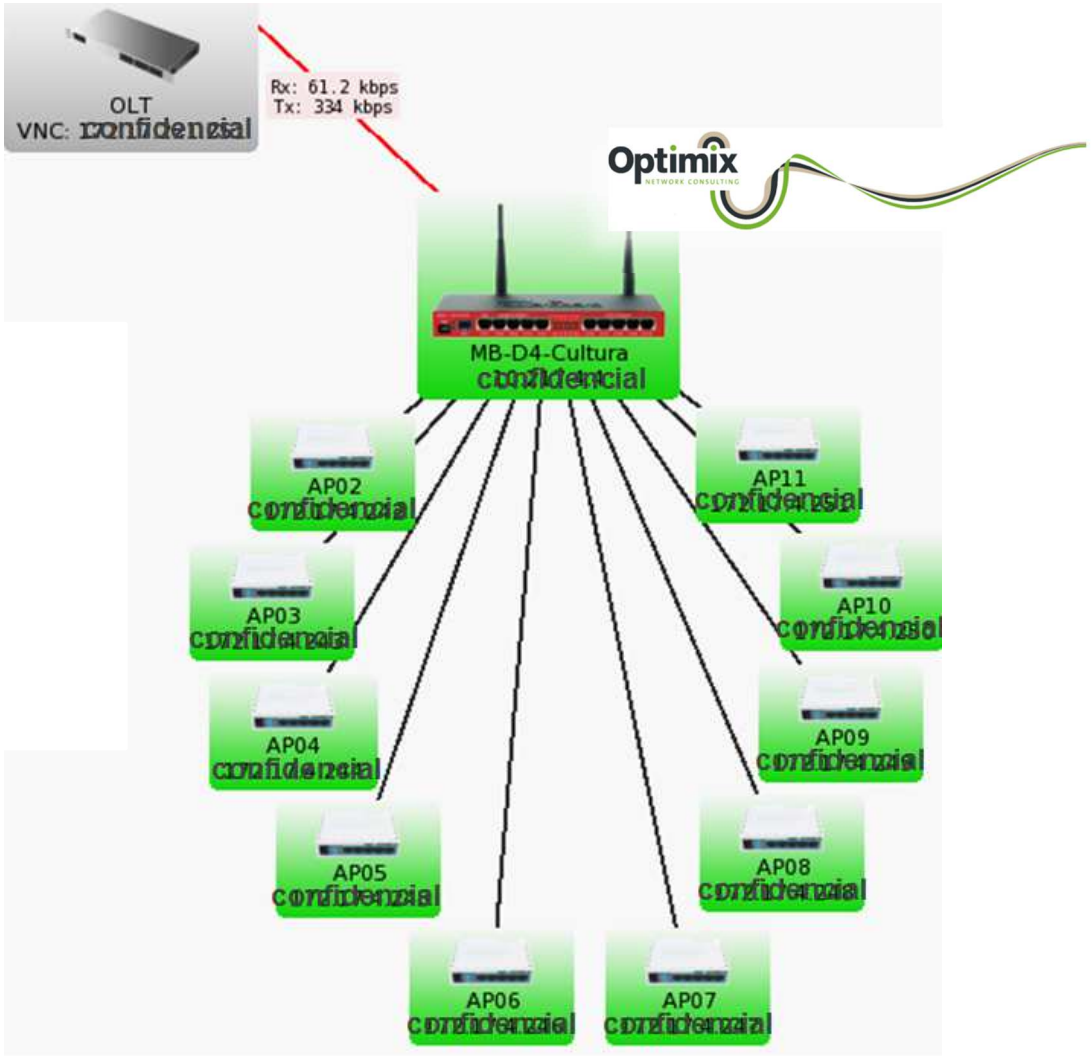
	Name	Type	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)
R	lo	Bridge	65535	0 bps	0 bps	0	0
R	sfp1-OLT	Ethernet	1590	3.8 Mbps	727.3 kbps	861	699
R	D1-Administracion	VLAN	1586	0 bps	0 bps	0	0
R	D1-Carteleria	VLAN	1586	336 bps	0 bps	1	0
RS	D1-Datos	VLAN	1586	1088 bps	2.9 kbps	3	5
R	D1-Impresoras	VLAN	1586	336 bps	0 bps	1	0
R	D1-Telefonia	VLAN	1586	1120 bps	1824 bps	2	2
R	D1-Video	VLAN	1586	0 bps	0 bps	0	0
R	D1-WiFi	VLAN	1586	0 bps	0 bps	0	0
R	D2-OldRigolleau	VLAN	1586	2.1 kbps	2.0 kbps	1	1
R	D3-DeVicenzo	VLAN	1586	16.9 kbps	16.3 kbps	12	10
R	D4-Cultura	VLAN	1586	427.5 kbps	174.4 kbps	64	66
R	D5-Odontologico	VLAN	1586	3.3 Mbps	429.0 kbps	776	615

Router Core – BGP

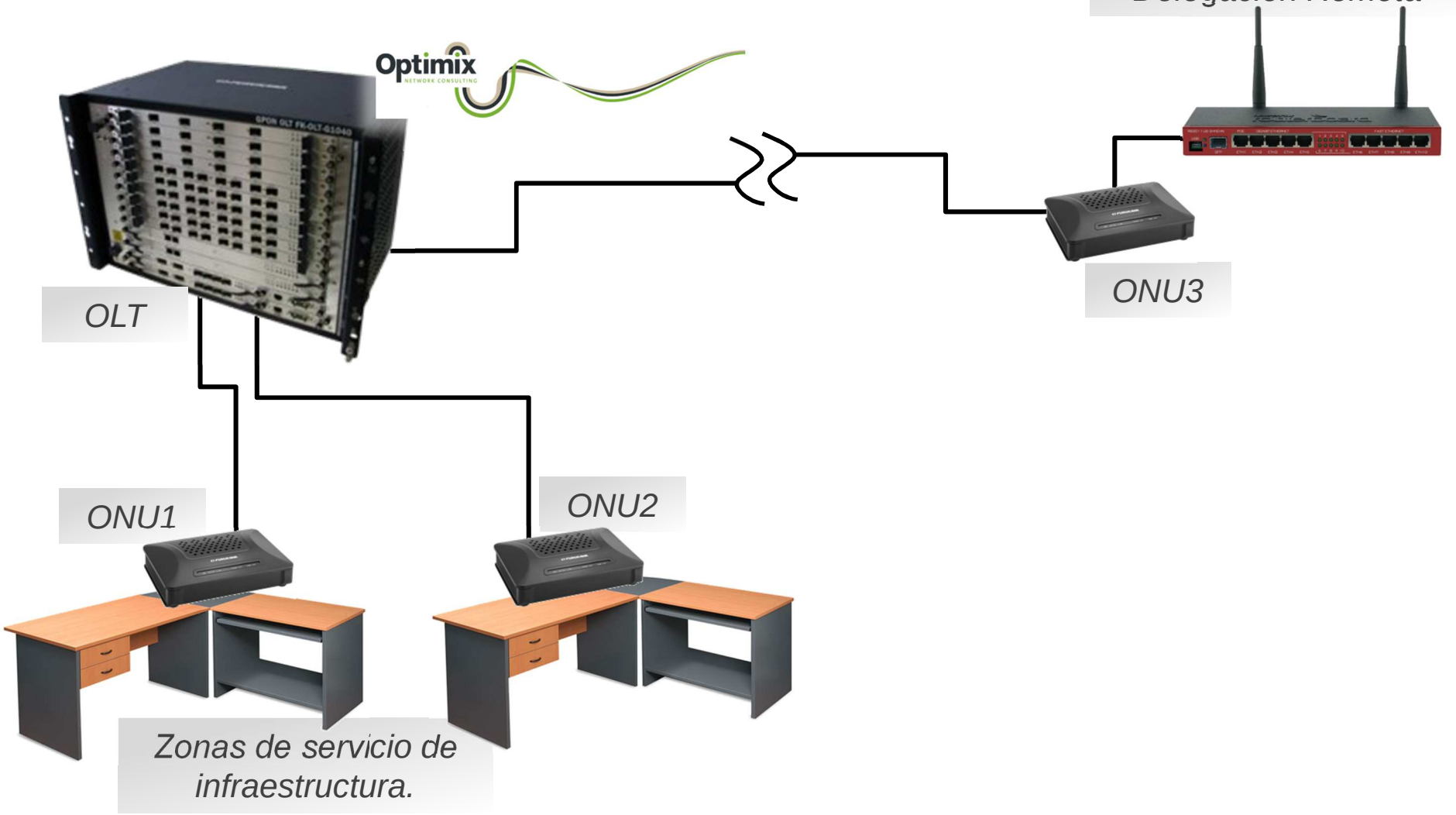




Dependencias remotas



GPON


Router de Servicio de Delegación Remota
OLT
ONU3
ONU1
ONU2
Zonas de servicio de infraestructura.

Leonardo da Vinci

- Artista, científico e inventor Florentino (actual Italia), 1452-1519.

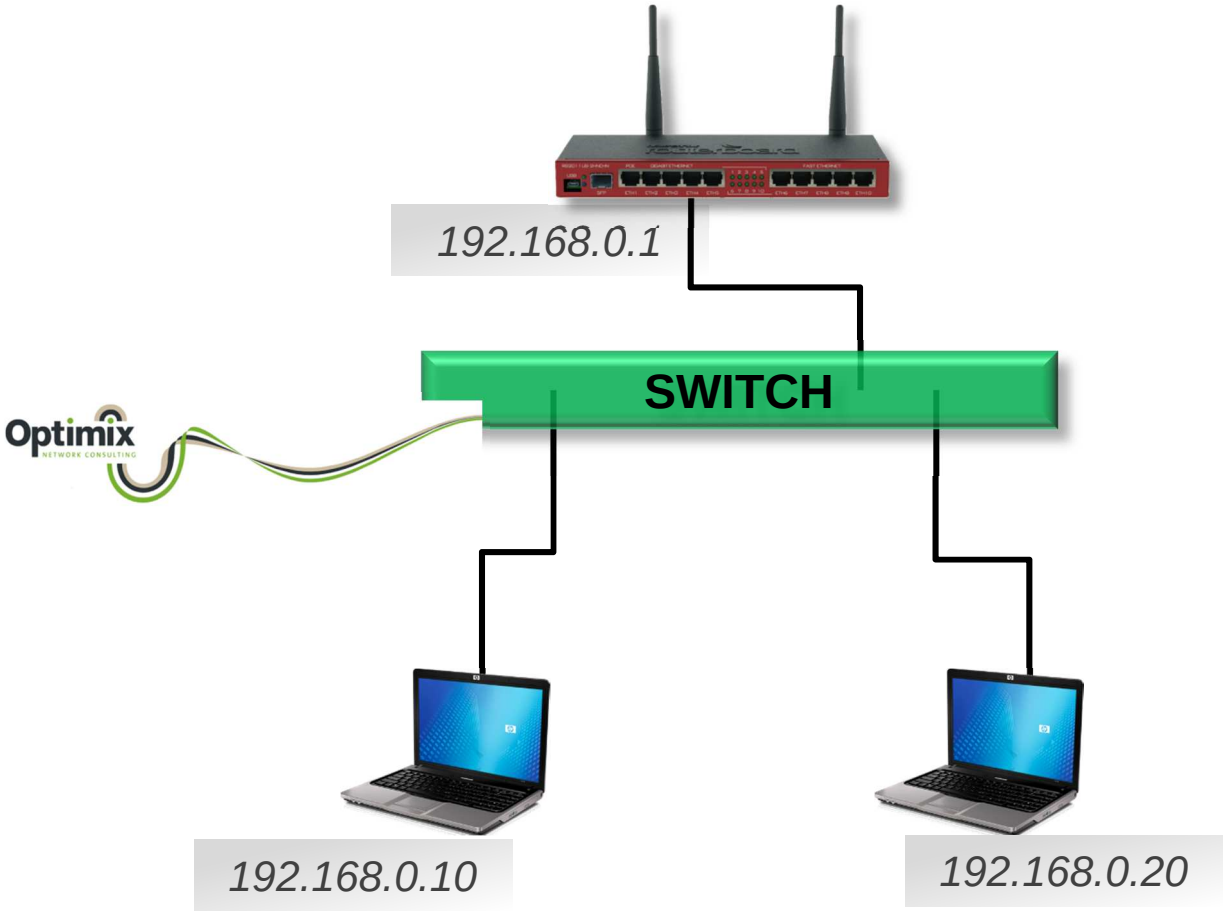
  - Los que se enamoran de la práctica, sin la teoría, somo como los pilotos sin timón ni brújula, que nunca podrán saber a dónde van.

Optimix
Network Engineering

Conceptos fundamentales de una arquitectura segura

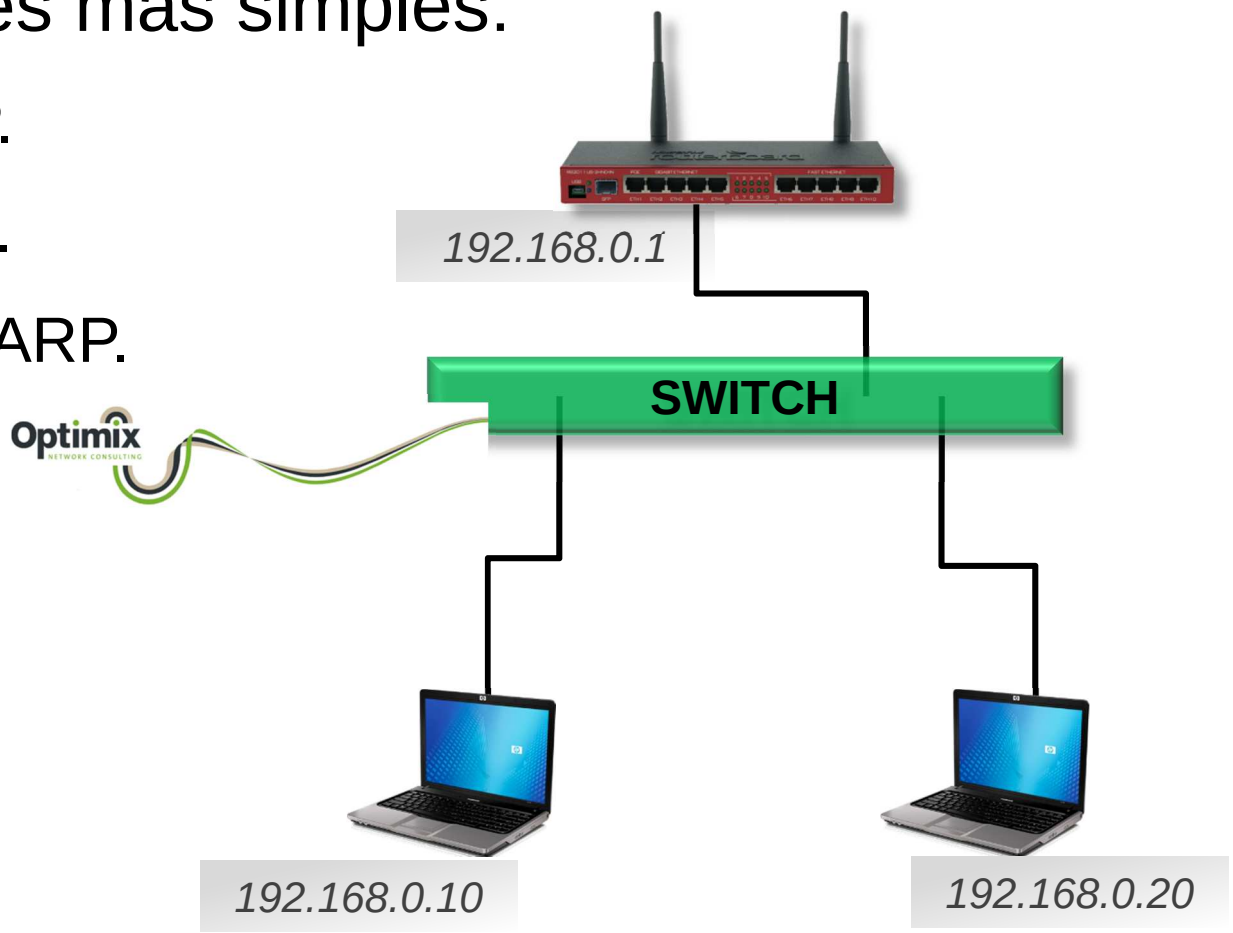
Causas y consecuencias de las distintas arquitecturas que nos guían hacia la red de Berazategui.

Red en L2

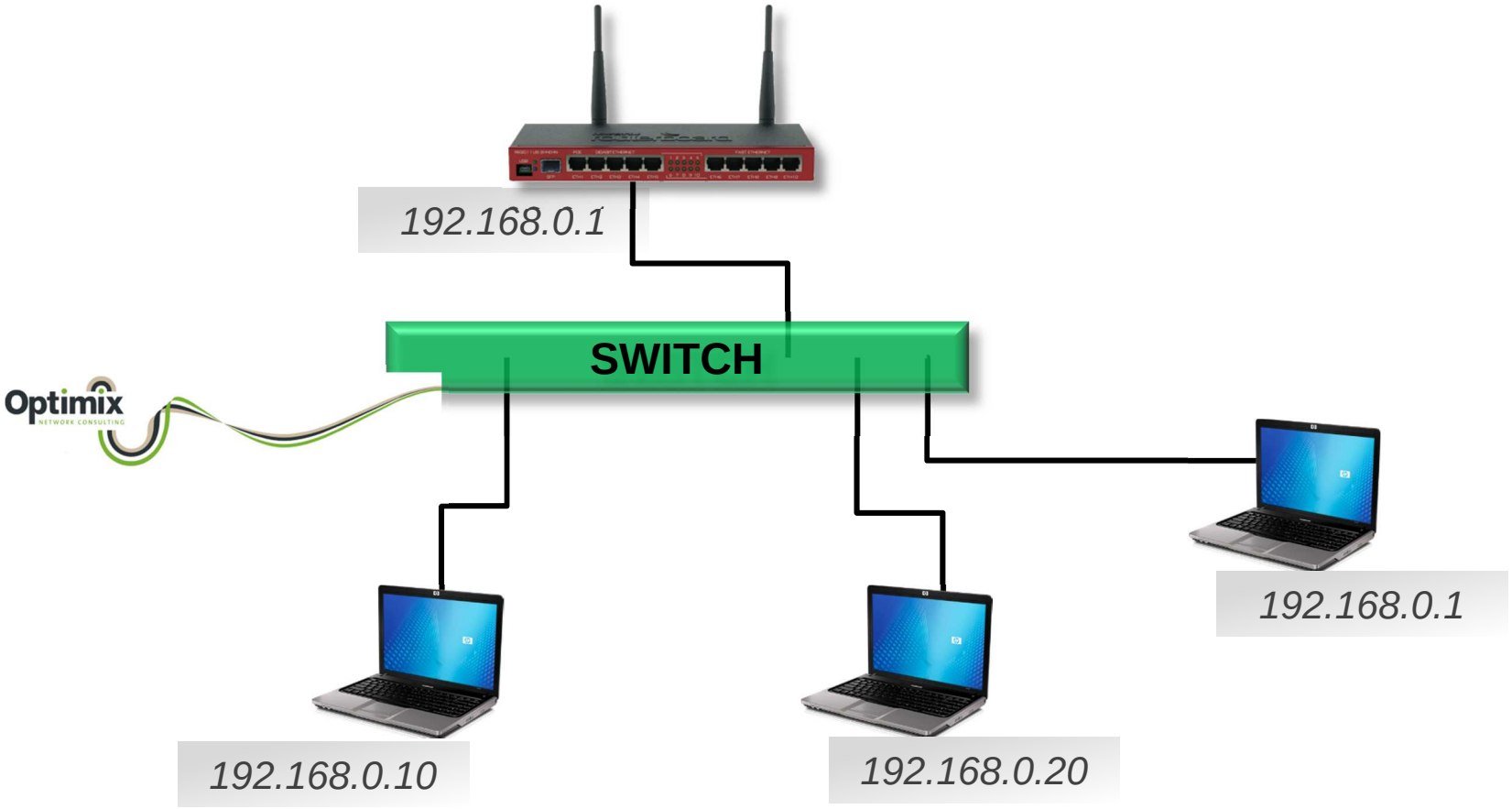


Red en L2

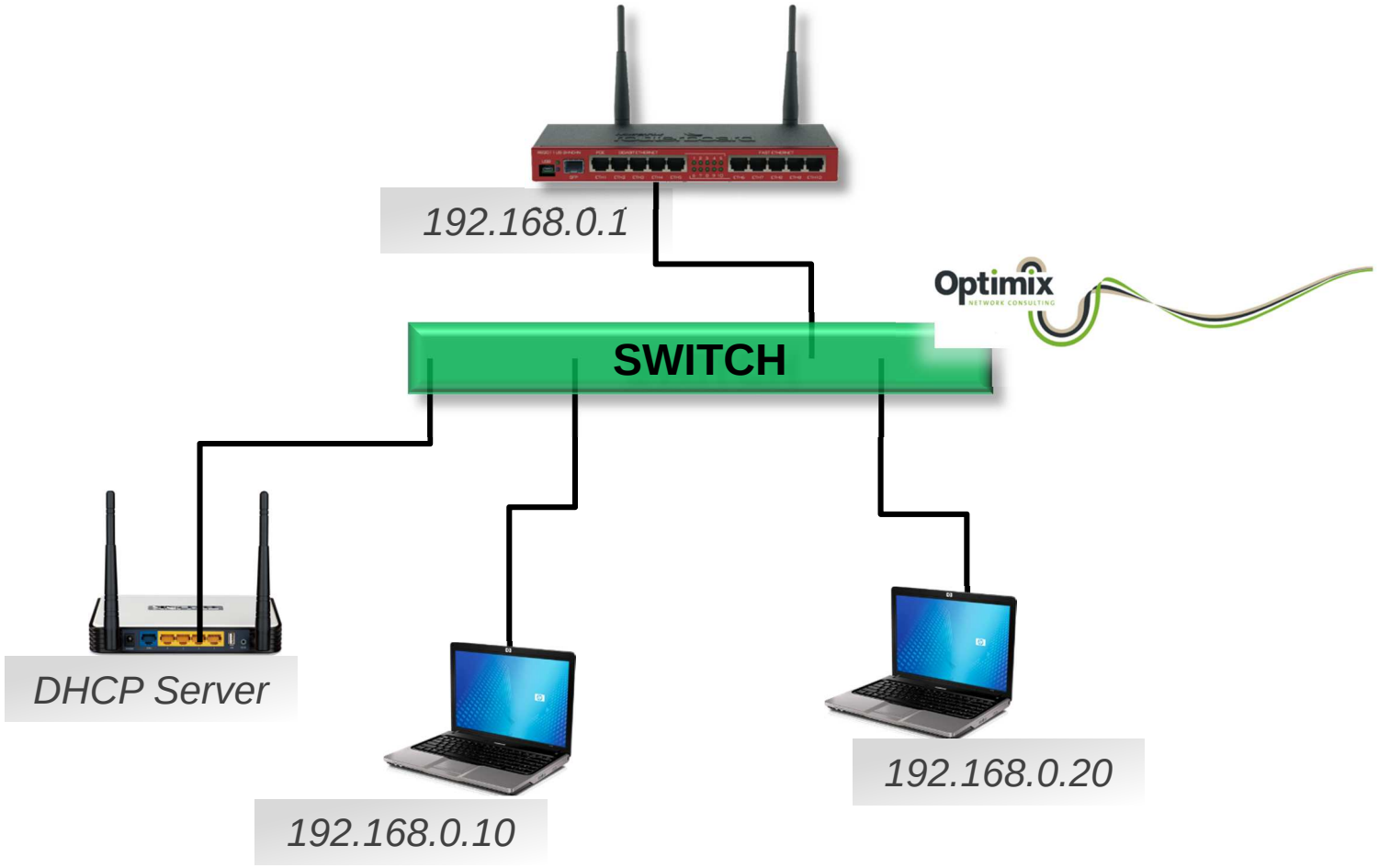
- Vulnerabilidades más simples:
  - Conflicto de IP.
  - DHCP espurio.
  - Tormentas de ARP.



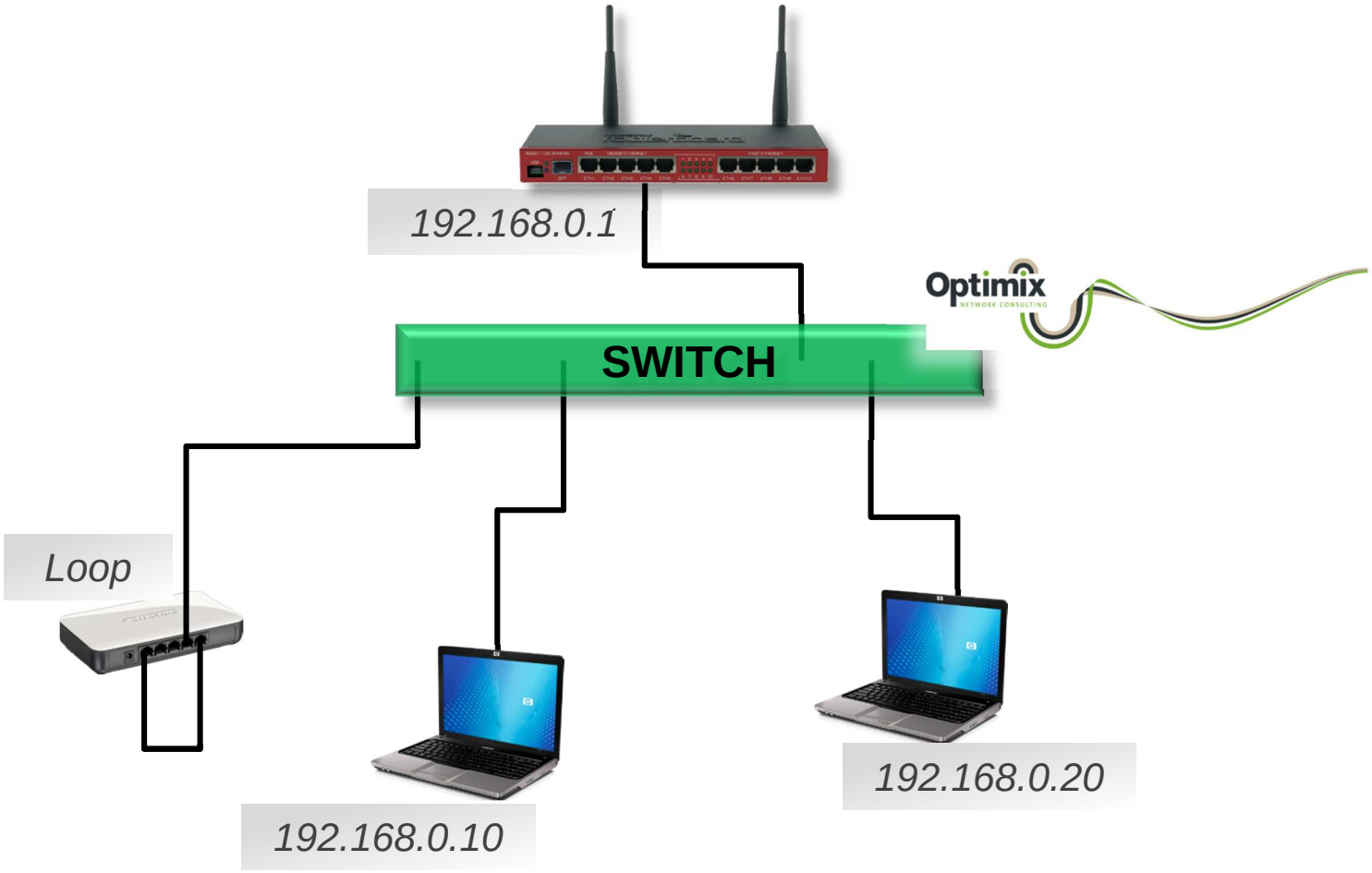
Red en L2 – Conflicto de IP



Red en L2 – DHCP espurio

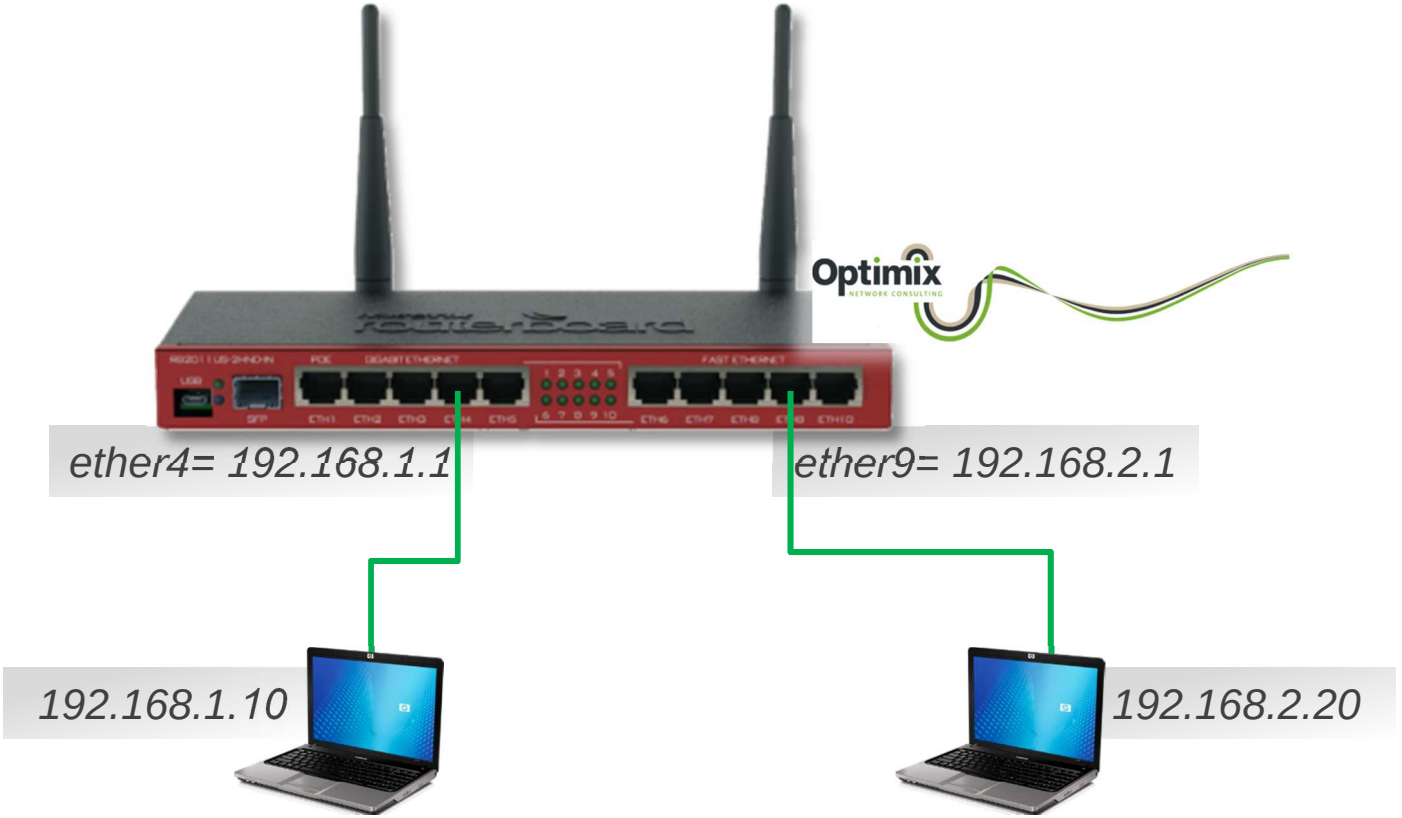


Red en L2 – Tormentas de ARP



Solución 1 – Una red por puerto

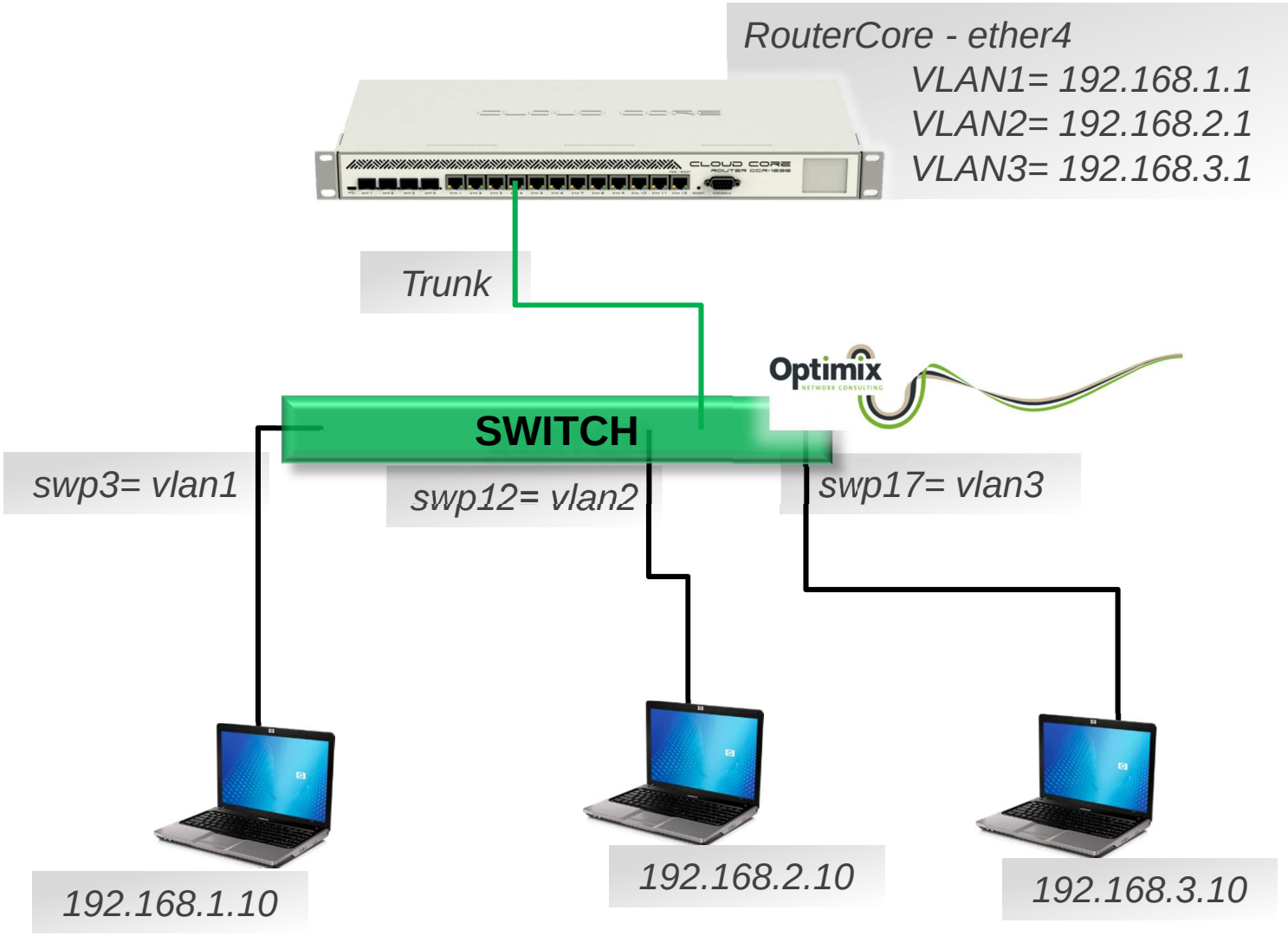
- Aprovechando que cada puerto de un router puede proclamar una red distinta, segmentamos en subredes, aislando los entornos de broadcast.



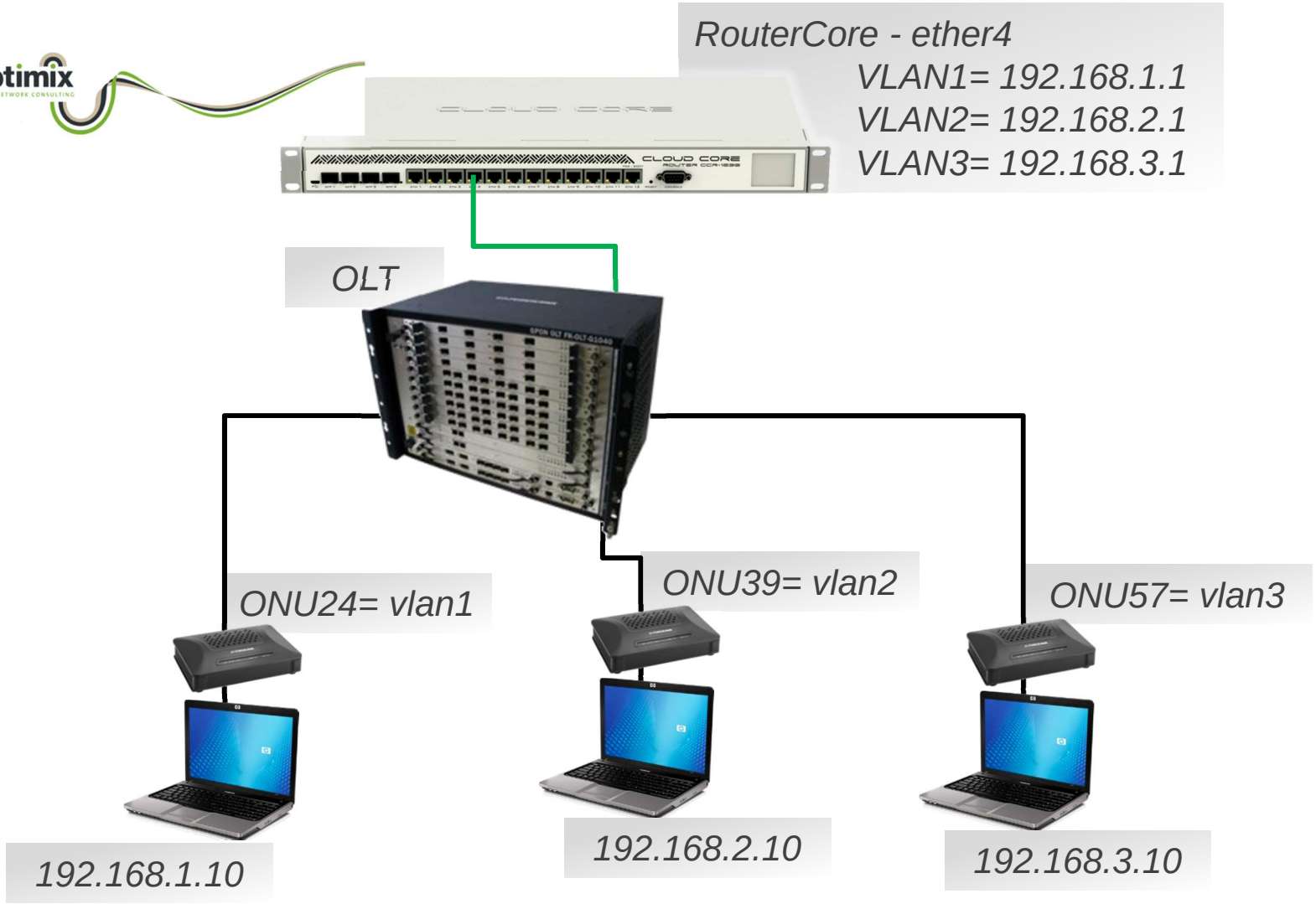
Solución 1 – Una red por puerto

- Ventajas
  - Cada cable proclama una subred distinta, induciendo la individualización lógica de las areas.
  - Las agresiones en L2, afectan al entorno de broadcast, permitiéndonos reducir el area de análisis de incidentes.
  - A pesar del aislamiento en L2, las distintas subredes pueden verse en L3 a través del router gateway.
- Desventaja
  - Estamos limitados por la cantidad de puertos físicos que posee el router.

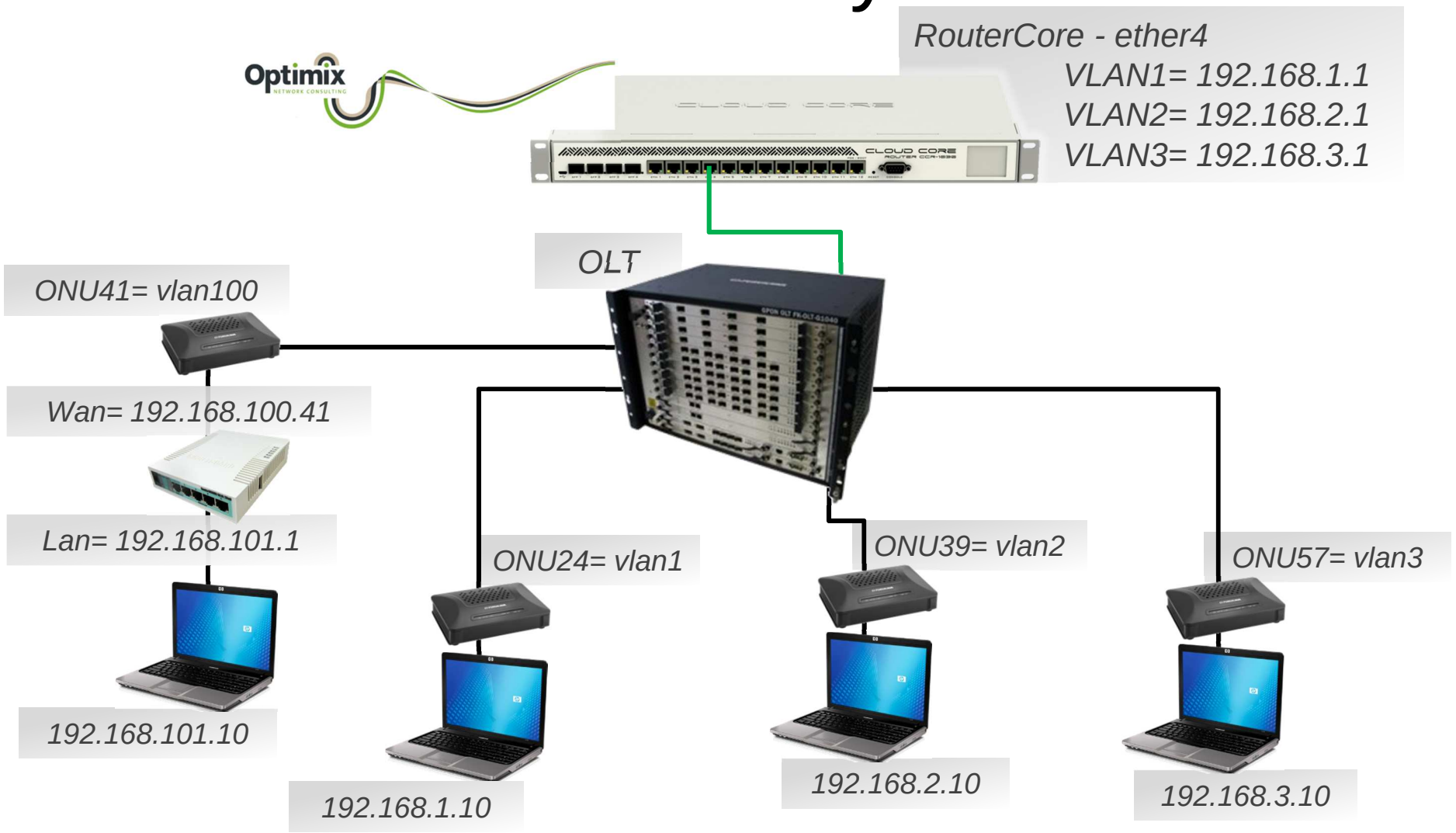
Solución 2 – VLANs



Solución 2 – VLANs



Solución 2 – VLANs y RSs



Conclusiones

- La gestión de VLANs, nos permite segmentar las delegaciones que viajan por la infraestructura de transporte.
- El resto, sigue siendo MikroTik, con lo que ya nos sentimos cómodos.
- Podemos plantear en cada destino, el concepto de Router de Servicio, para mayor control local.
- Así, la red se extiende en la ciudad, sin perder control, bidireccionalidad ni monitoreo.

Glosario

- FTTx – Fiber to X. Expresión genérica que engloba FTTH (fiber to the home) y FTTO (fiber to the office). Transmite a nivel general el concepto de transporte óptico de tráfico de red a estos tipos de usuarios.
- GPON – Gigabit passive optical network. Arquitectura para provisión de servicios de red FTTx con redes pasivas spliteables. En contraposición a despliegues de fibras punto a punto convencionales.
- OLT – Optical line termination. Concentrador principal en que se reune una zona de infraestructura GPON. Suele definir un POP.
- ONU – Optical network unit. Equipo terminal cliente que brinda conectividad final (endpoint) a un usuario o grupo de usuarios.
- POP – Point of presence. Domicilio físico en que se ubica la OLT, desde la que sale a nivel físico un despliegue GPON.
- RB – Router de borde. Router conectado (expuesto) a Internet. Definición Optimix.
- RC – Router Core. Router que gobierna concentradores de gran escala (switches, OLTs, etc…). Definición Optimix.
- RS – Router de Servicio. Router conectado a los usuarios, que suele controlarlos con visibilidad broadcast. Definición Optimix.
- VLAN – Virtual LAN. Tipo de paquetización en frames ethernet que permite aislar lógicamente distintos entornos de broadcast en un mismo medio físico.

Optimix
Network Engineering

Gracias!

Ing Jorge Filippo

jfilippo@optimix.com.ar

Skype: jorgefilippo

Celu y WhatsApp: +54 9 11 6693 5494

Facebook: Ing Jorge Filippo