Optimix
Network Engineering

Construyendo Ciudades Digitales

Ing. Jorge Filippo

Email: info@optimix.com.ar

Celu y WhatsApp AR: +54 9 11 6693 5494

Skype: jorgefilippo

Facebook: Ing Jorge Filippo

INDEX SOLUCIONES IP

MikroTik MEXICO
Enrutamiento y Soluciones Inalámbricas

Objetivos Optimix Network Engineering

- Proveer estrategias de networking **infalibles** y **económicamente** eficaces.
- Capacitar al **personal técnico** de las redes guiadas, para que puedan resolver las necesidades **cotidianas** de la red.
- Ser un aliado, para desarrollar proyectos de **escalabilidad** y **funcionalidades** ilimitadas.

Objetivos de esta exposición

- Abordar, desde una óptica técnica, un plan de Ciudad Digital (Red Urbana Municipal).
- Ordenar los roles de los técnico involucrados, haciendo eficiente y coherente el desarrollo de proyectos.
- Compartir la implementación de la red de fibra óptica municipal en Berazategui, provincia de Buenos Aires.

Introducción

- Esta exposición abordará los conceptos desde lo simple a lo complejo, para que hasta el consultor más principiante pueda aprovechar esta experiencia Optimix.
- Se asentarán los conceptos más básicos, para construir al final de la exposición los conceptos más complejos.
- Se dejarán en claro los conceptos funcionales, para comprender las mejores prácticas en redes escalables y seguras.

Optimix
Network Engineering

Historia de la red Municipal

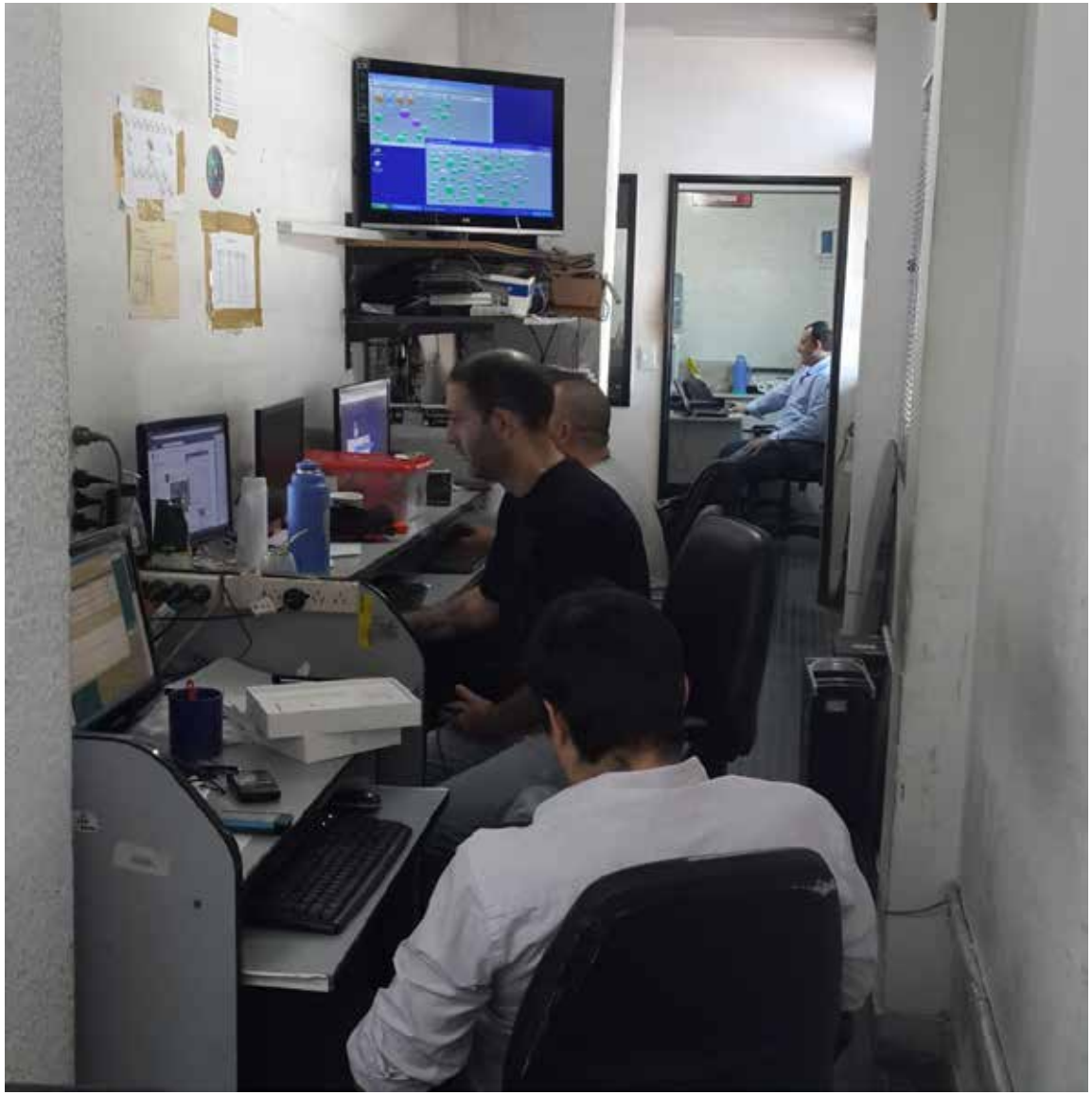
Municipalidad antigua

Municipalidad nueva

Municipalidad antigua

Municipalidad nueva

Municipalidad antigua



Municipalidad nueva

Municipalidad antigua

Municipalidad nueva

Optimix
Network Engineering

Planteo conceptual: Red Municipal, áreas independientes.

Planteo cultural

- La gestión de una red municipal exige proteger y aislar correctamente todas las áreas.

- El celo entre areas, muchas veces pone al area de sistemas en la ***encrucijada*** de ***generar privilegios***, y ***evitar privilegios***.

Planteo técnico de los usuarios

- La gestión de una red municipal de cobertura urbana, plantea una población de usuarios (dispositivos) que deben gestionarse bidireccionalmente desde una posición central.
- La gestión bidireccional, implica ***para*** cada **dispositivo** cliente, poder:
  - Controlar el ancho de banda.
  - Controlar a qué recursos internos accederá.
  - Regular libertades hacia Internet.
  - Monitorearlo y accederlo remotamente.

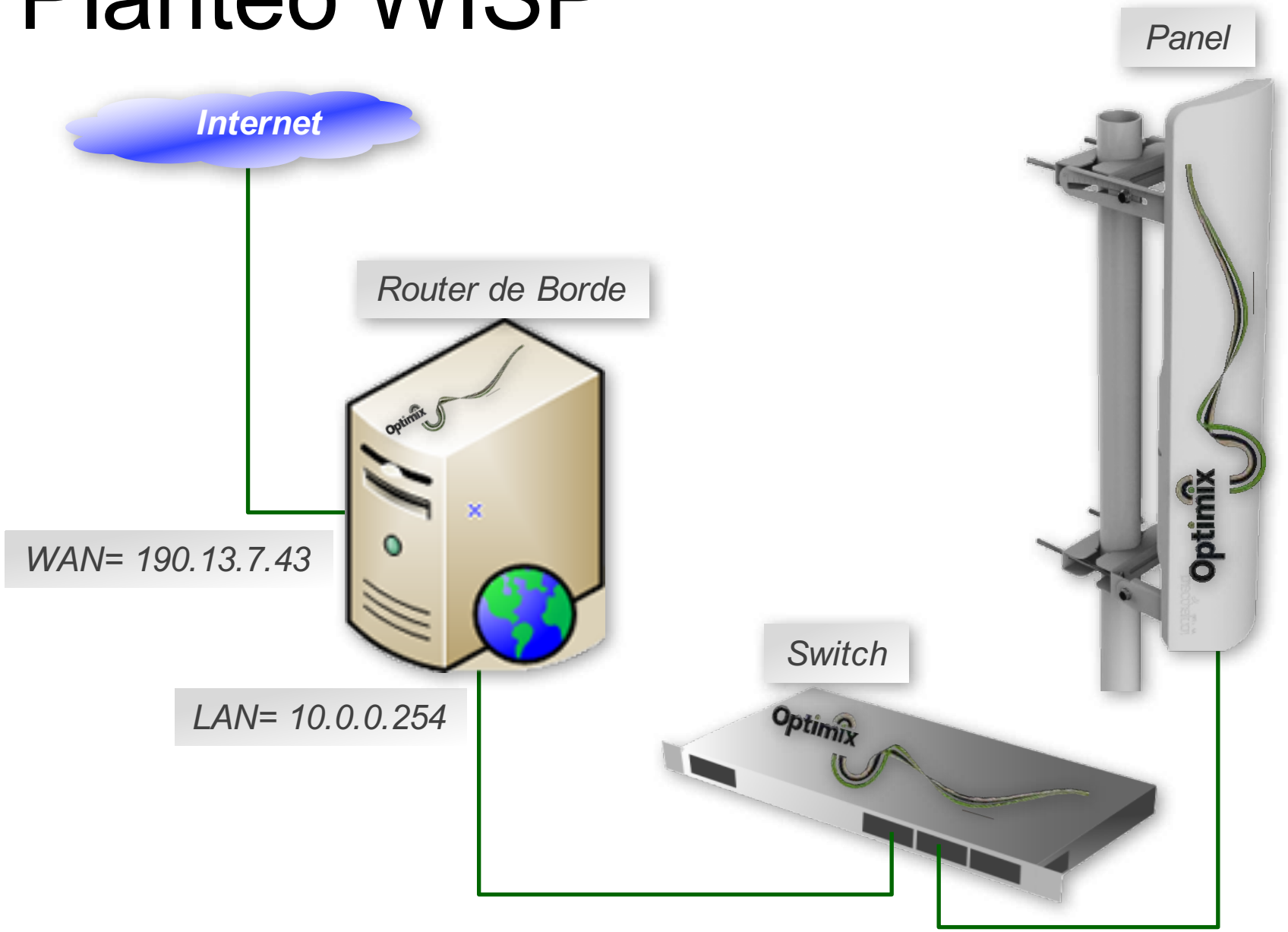
Las redes que conocemos

- La arquitectura WISP tradicional, plantea que los usuarios que están detrás de un router, están enmascarados.
- Cada cliente, es un station que toma una IP, y es el dispositivo controlado (no así su LAN).
- Así, desconocemos qué dispositivos hay en la LAN del domicilio, algo que no se admite en una red municipal.

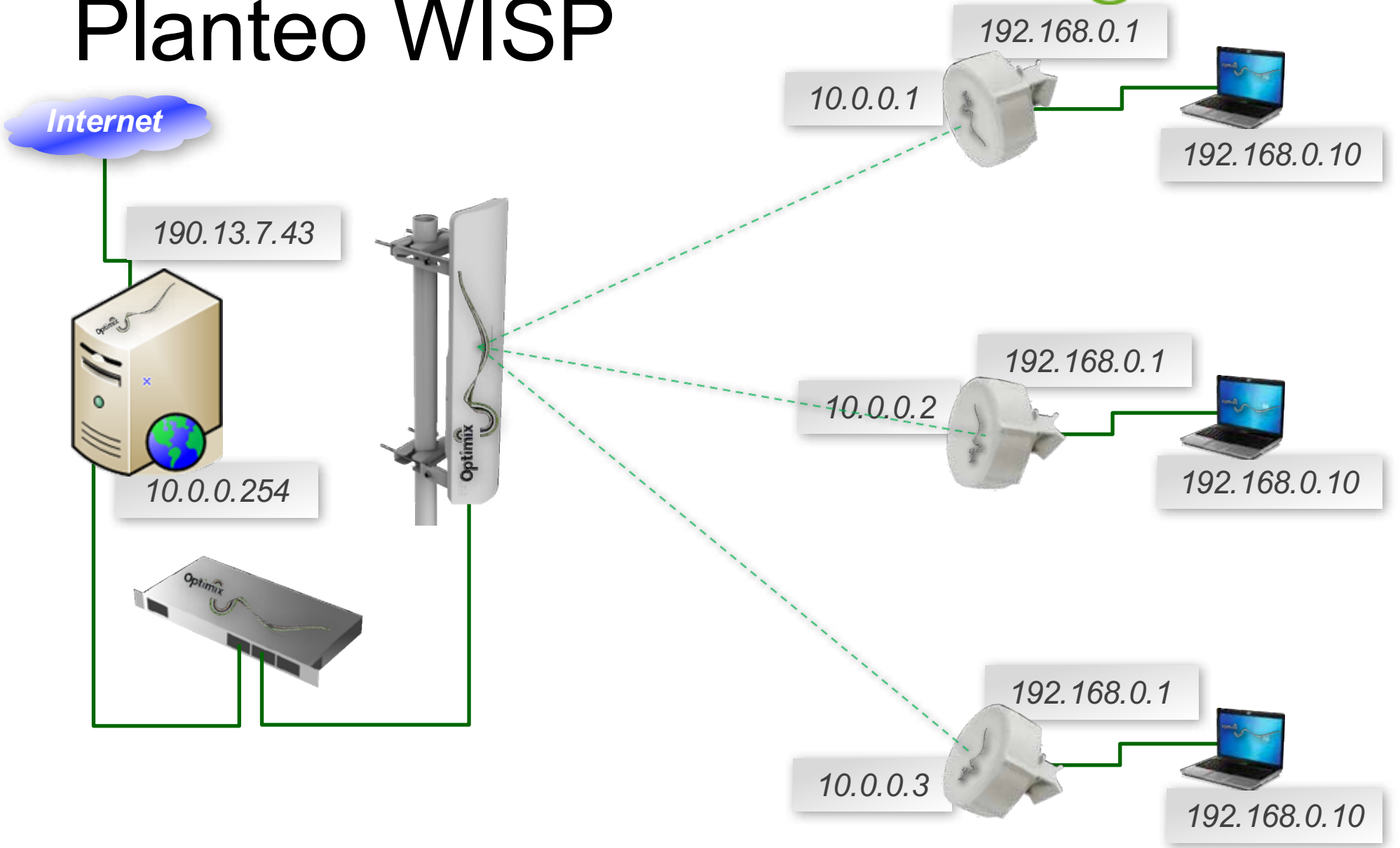
Las redes WISP tradicionales

- Podemos simplificar el análisis y decir que en una red WISP, hay mínimamente dos niveles de control:
  - El Router de Borde – El equipo que recibe los servicios de Internet, y enmascara a los usuarios para compartir ese Internet y darle vida al negocio ISP.
  - El Equipo Cliente – El equipo que se conecta lógicamente al Router de Borde (a través de switches, enlaces y paneles), y enmascara su LAN para darle servicio al domicilio.

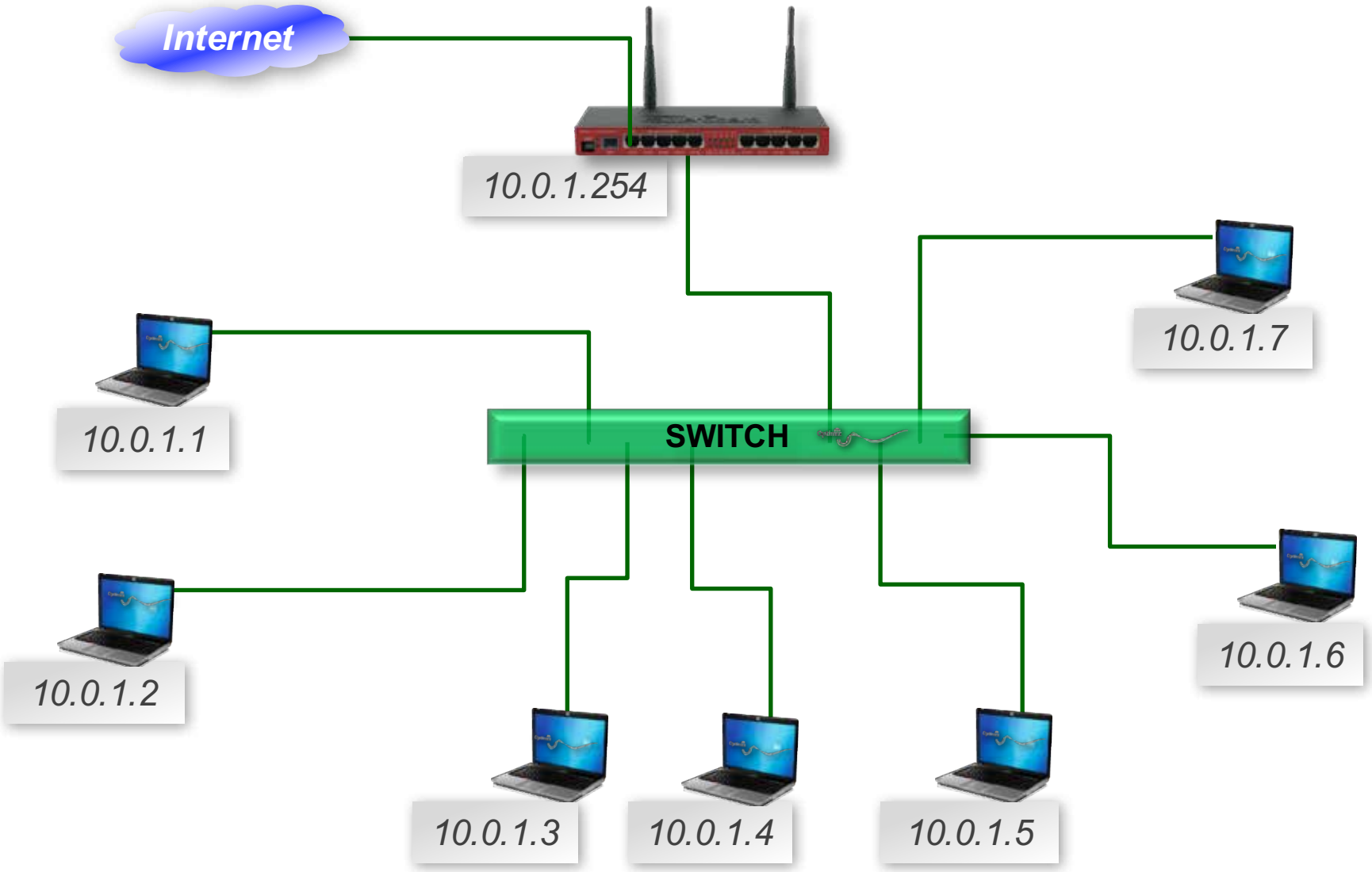
Planteo WISP



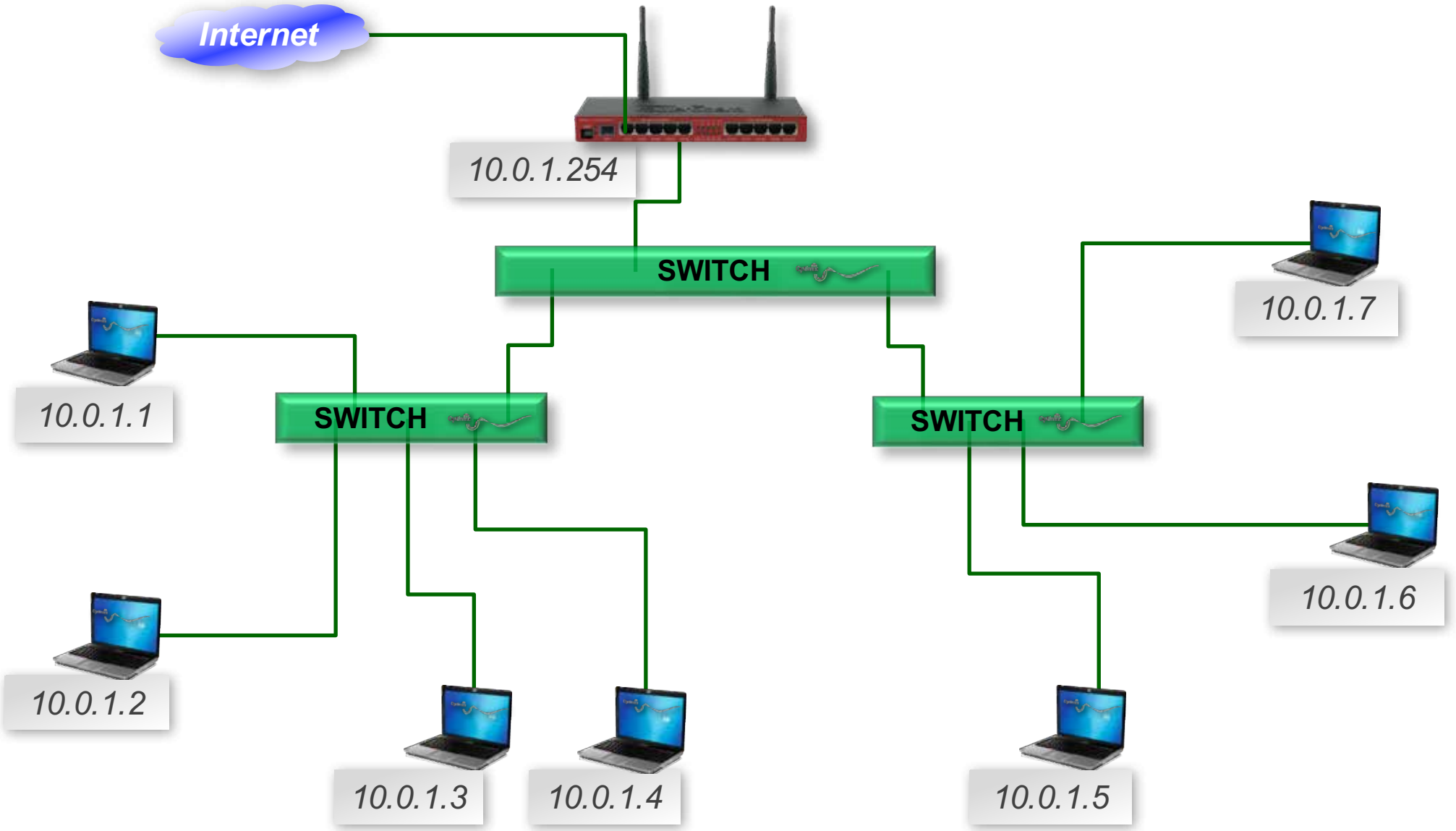
Planteo WISP



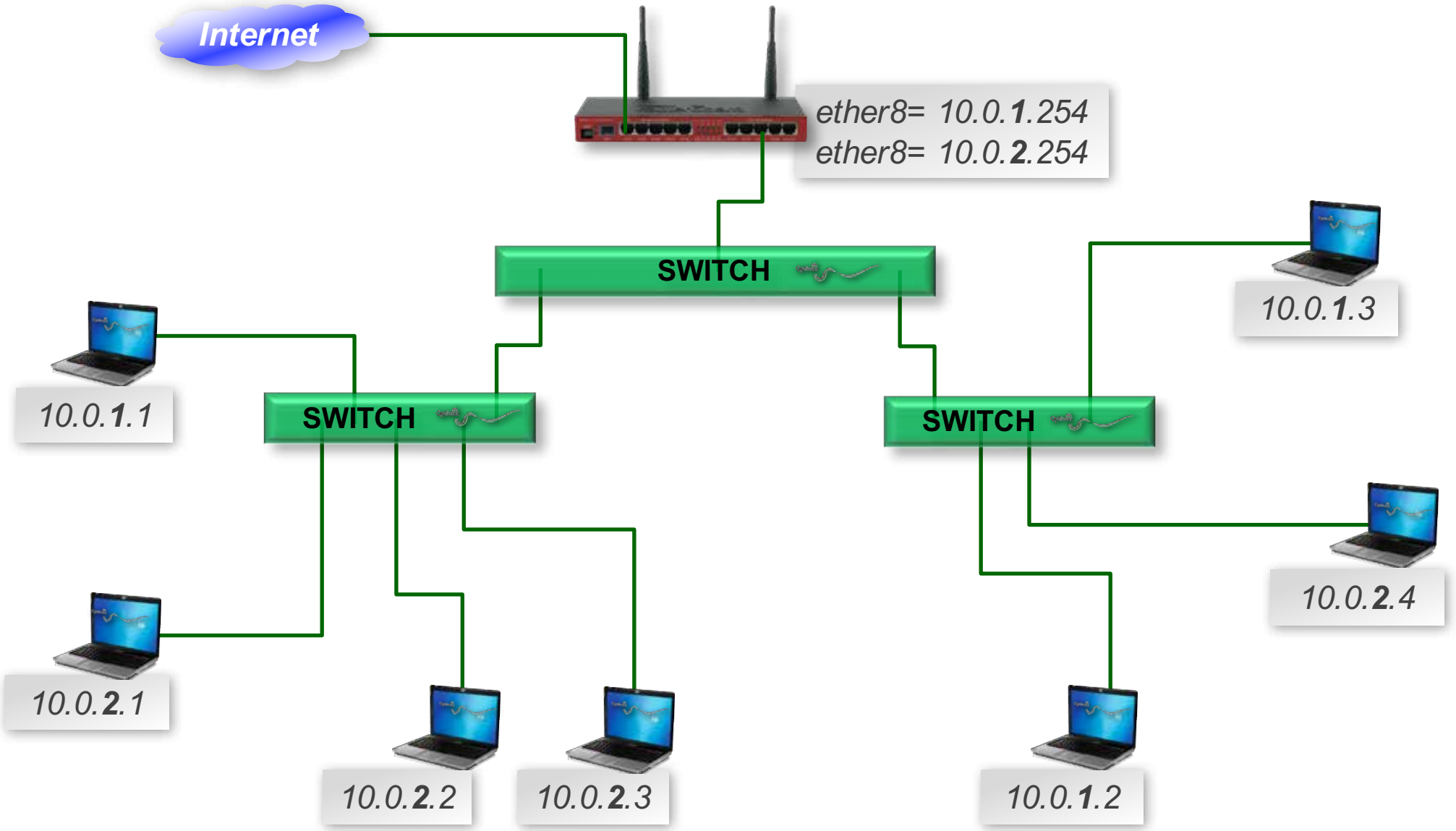
Un solo nivel de inteligencia



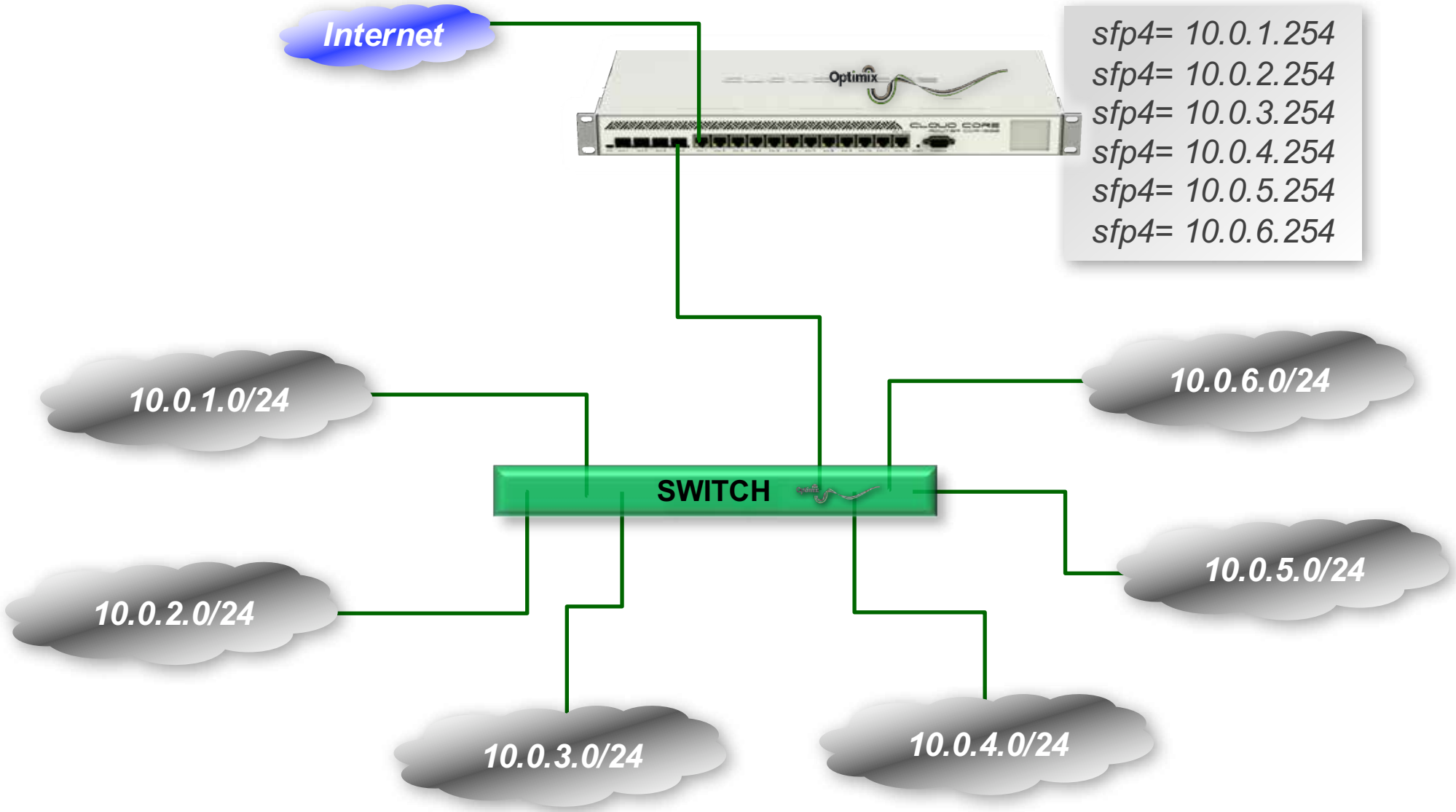
Un solo nivel de inteligencia



Un solo nivel de inteligencia

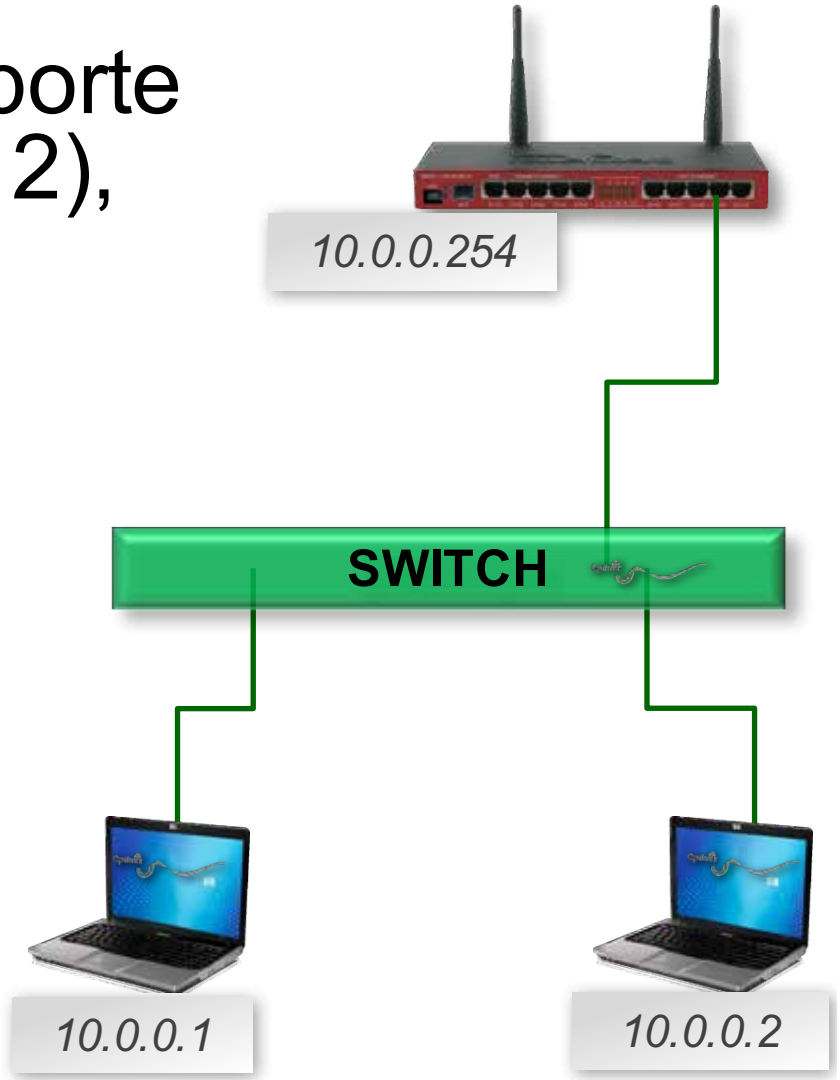


Un solo nivel de inteligencia

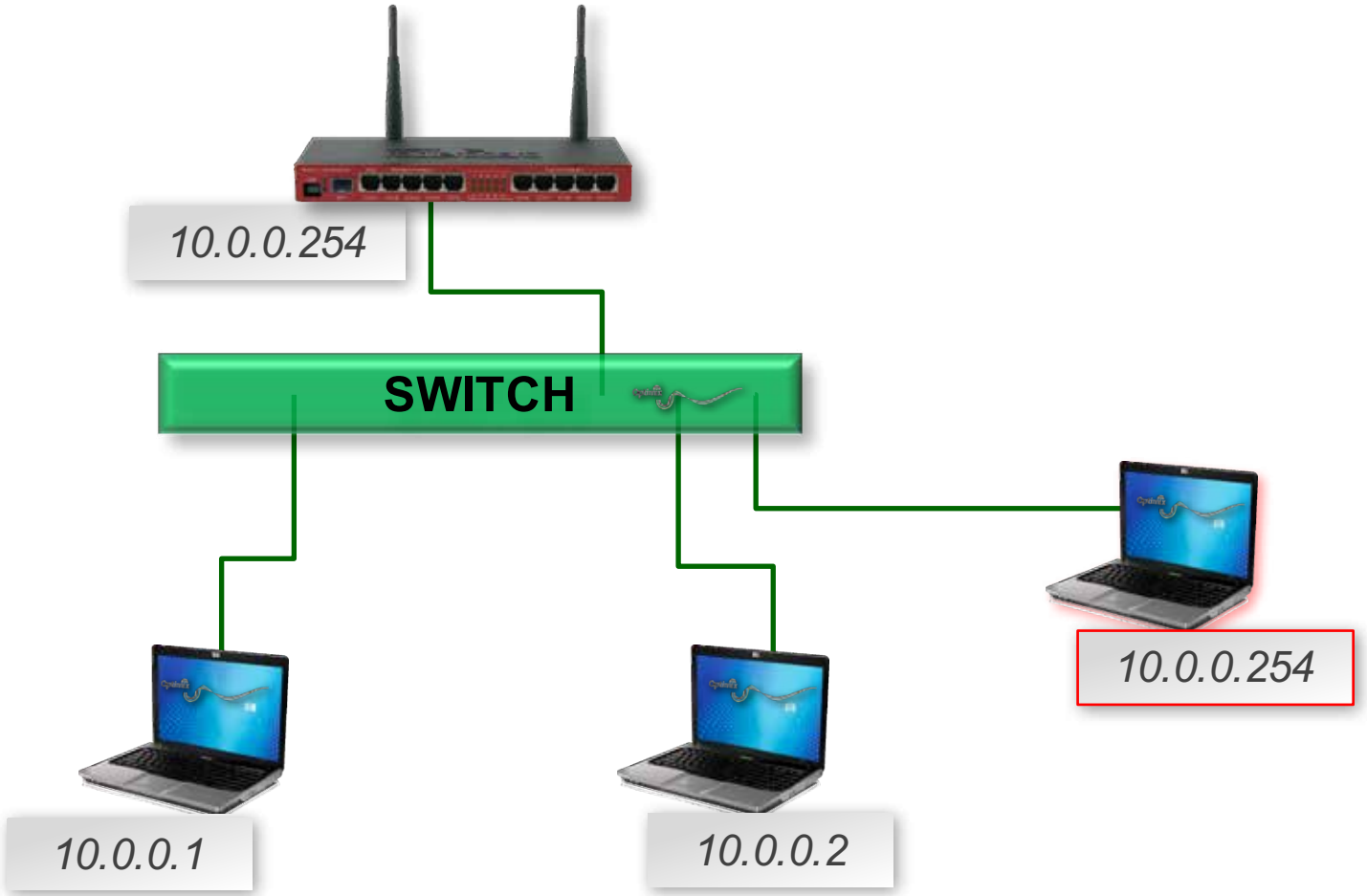


Vulnerabilidades

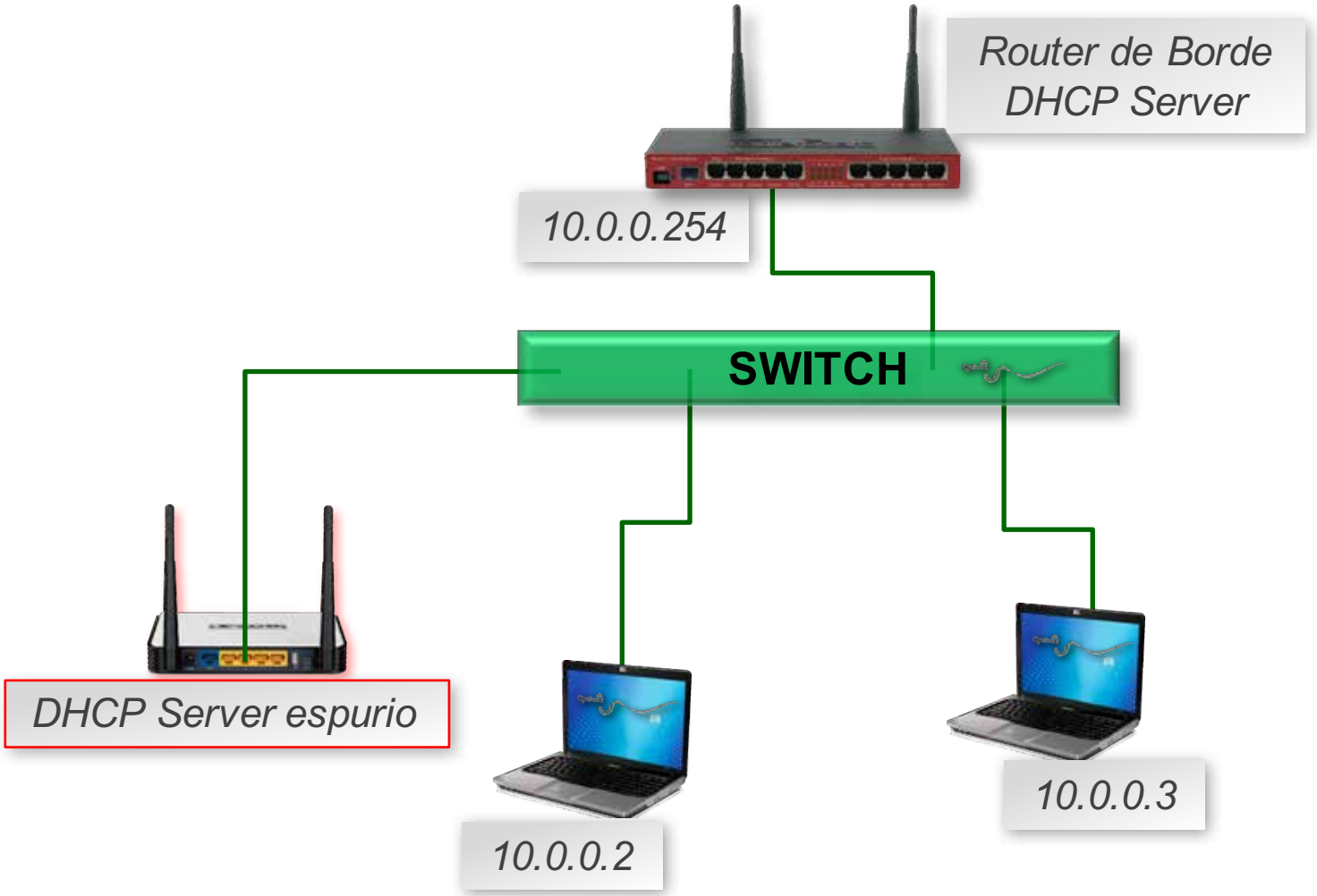
- El hecho de que el transporte se gestione en L2 (Capa 2), nos hace vulnerables a:
  - Conflicto de IP.
  - DHCP espurio.
  - Tormentas de ARP.



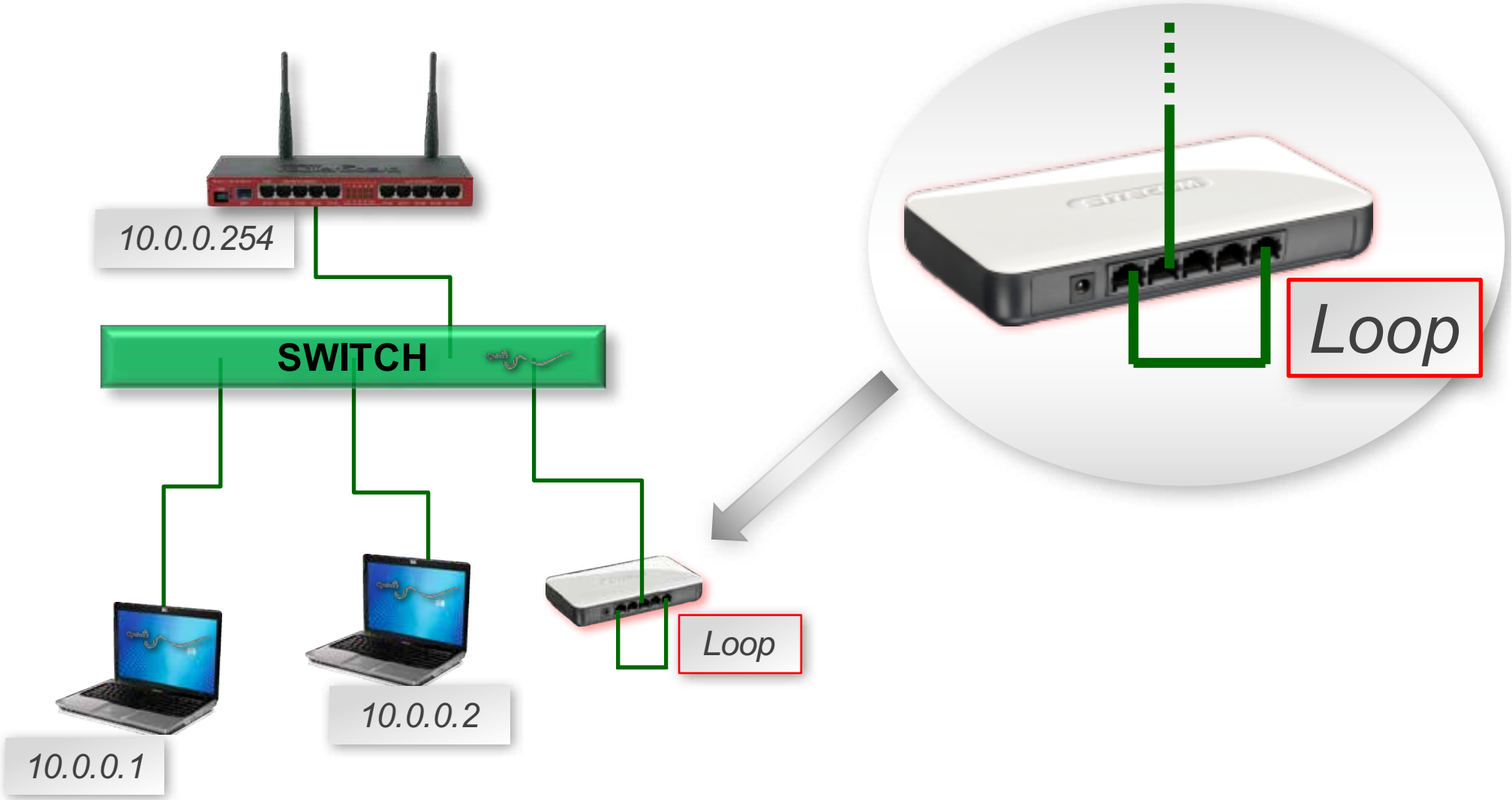
Red en L2 – Conflicto de IP



Red en L2 – DHCP espurio



Red en L2 – Tormentas de ARP



Optimix
Network Engineering

Un Gobierno Digital, nace a partir de un Gobierno Analógico!

Crear una gran red, es un gran desafío. Pero el **mayor** desafío es **transformar** lo prexistente, reuniendo muchas redes en una superior.

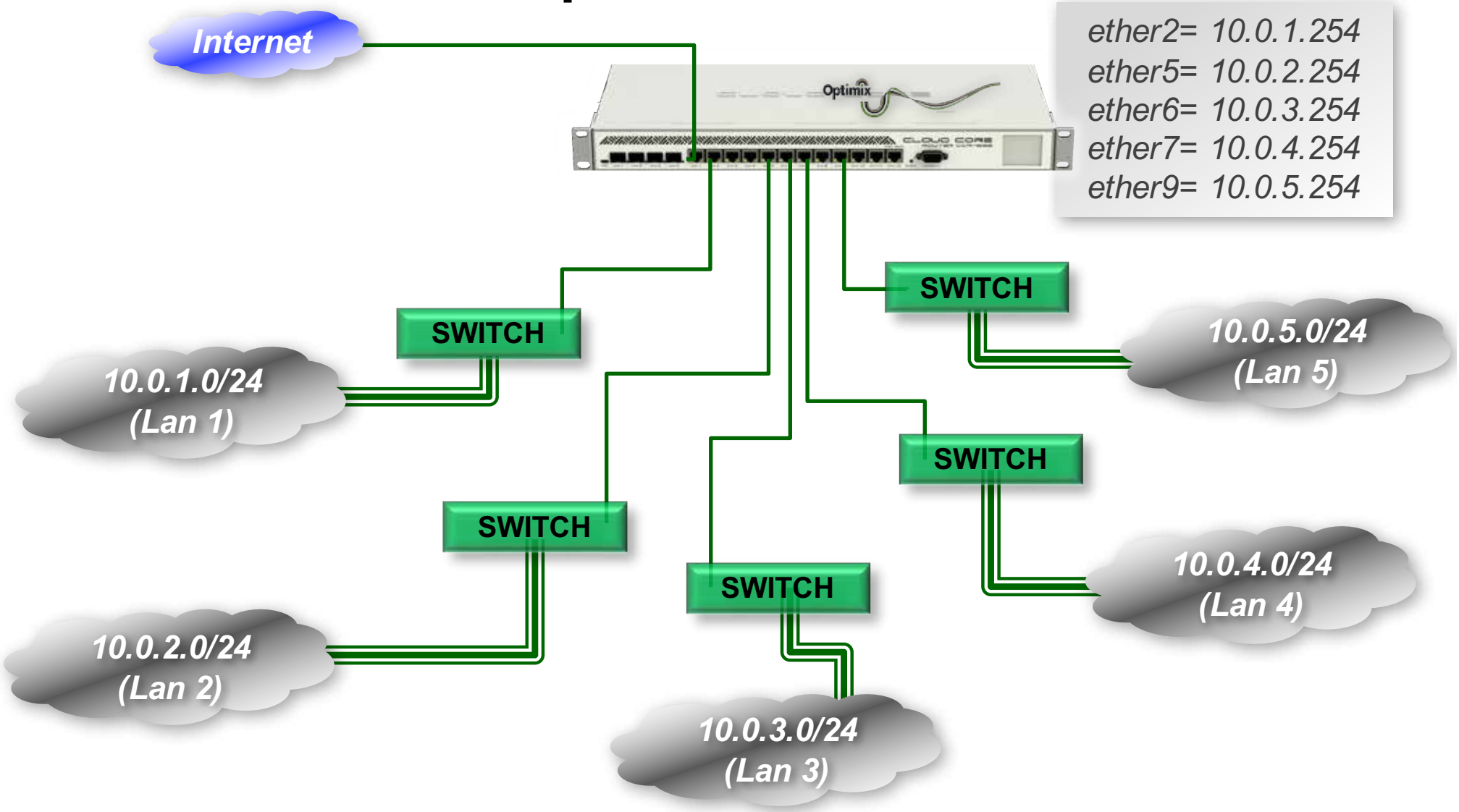
Escenario físico original

- Red urbana multiproveedores (inalámbricos, ADSLs, algunos vínculos dedicados).
- Edificios conectados mediante switches sin orden.
- Áreas con accesos a Internet propios que no quieren compartir.

Bases

- Necesidades:
  - Salvaguardar la independencia de cada area.
  - Que las agresiones afecten al área que las causa.
  - Pero sin restringir la funcionalidad.
- Solución:
  - Aislar las áreas entre sí en L2 (Capa 2).
  - Pero comunicándolas en L3 (Capa 3).

Router multipuerto



Lo mejor de los dos mundos

- Cada area está interconectada por un switch, y ese switch, está conectado a **un puerto distintivo** del Router de Borde.
- **Cada puerto distintivo** del Router de Borde, posee una IP, gateway de la LAN a la que le brinda servicio.
- Las distintas LANs, tienen broadcast interno, pero no tienen comunicación broadcast con las otras LANs.
- Las distintas LANs puede comunicarse unas con otras, a través del Router de Borde (por IP, es decir en Capa 3).
- No hay visibilidad broadcast entre distintas LANs, pero si hay comunicación IP.
- Se dice que las áreas están aisladas en Capa 2, pero comunicadas en Capa 3.

Optimix
Network Engineering

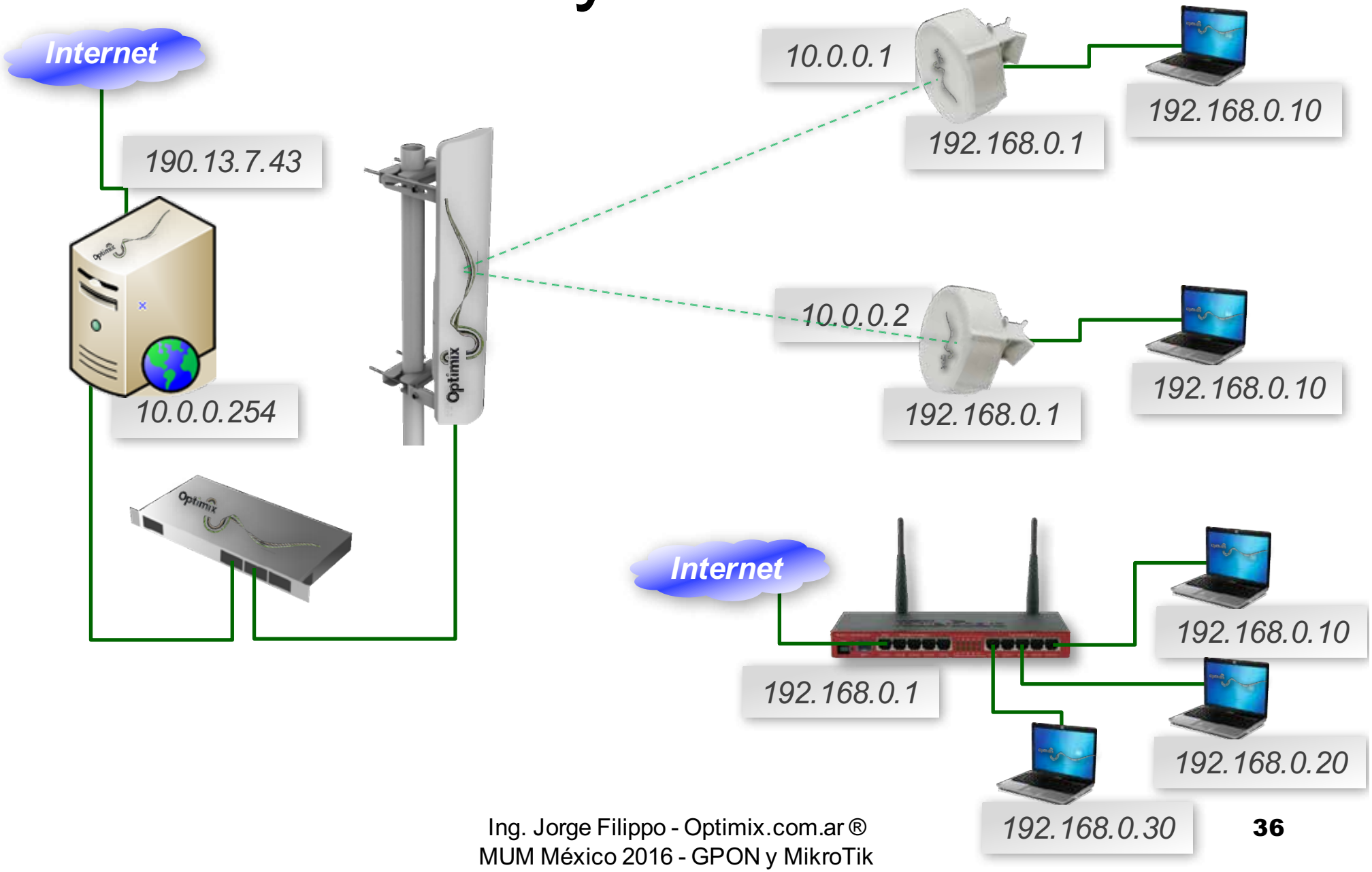
Distancias físicas entre domicilios municipales

Cuando la cobertura es urbana, nacen nuevos desafíos por la lejanía de las dependencias municipales.

Desafíos

- Los desafíos de interconectar dependencias municipales en una Ciudad Digital:
  - Desafío Técnico 1 – Enlaces inalámbricos (calidad dudosa).
  - Desafío Técnico 2 – Internet dedicado (perder el control).
  - Desafío Humano – Un gran poder, conlleva una gran...
- Con MikroTik, tenemos que poder resolver los Desafíos Técnicos, para que solo queden pendientes los Desafíos Humanos que requerirán nuestra compañía intelectual.

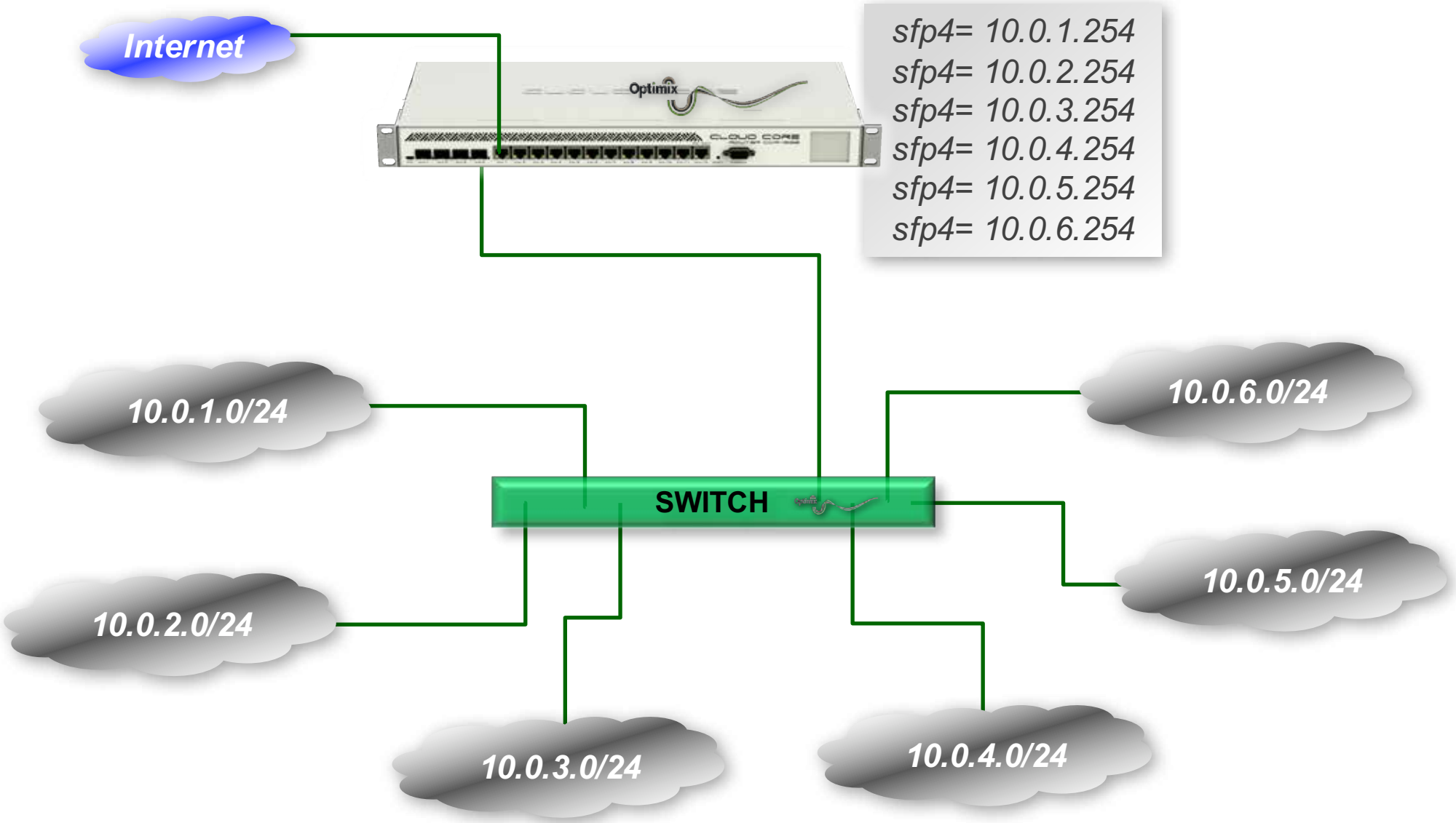
Inalámbricos y Dedicados



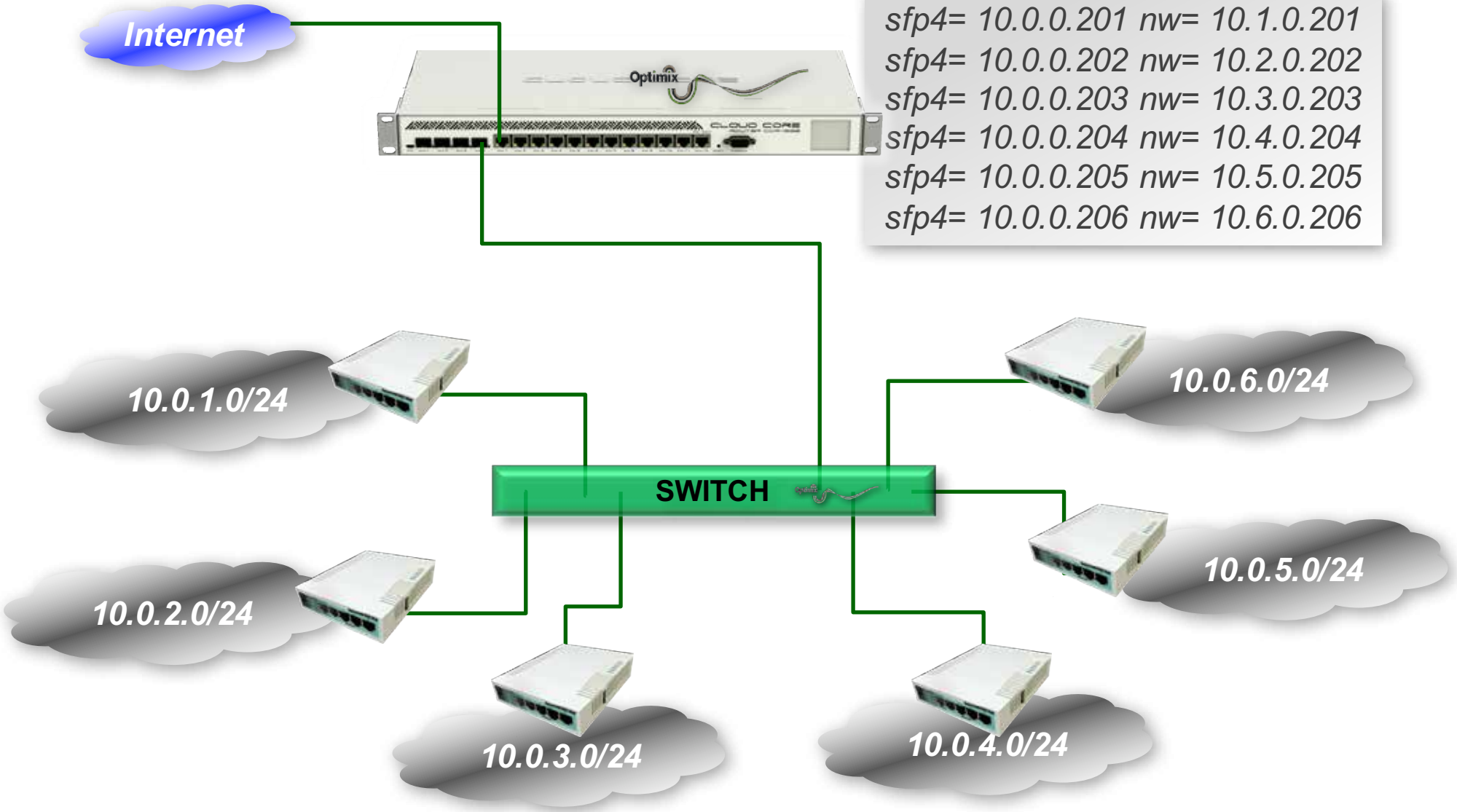
Políticas de control

- Para las dependencias remotas tenemos que:
  - Auditar todo el tráfico (proxys HTTP y HTTPS, y email interno).
  - Para eso, debe bloquearse por defecto todo tráfico saliente.
  - Si se llega por transporte propio, podremos mejorar el rendimiento económico de Internet, brindar telefonía, y cartelería digital.
- La topología de Router de Borde, que concentra todas las áreas en Capa 3, debe **subir de jerarquía, para alcanzar todos los rincones de la ciudad.**

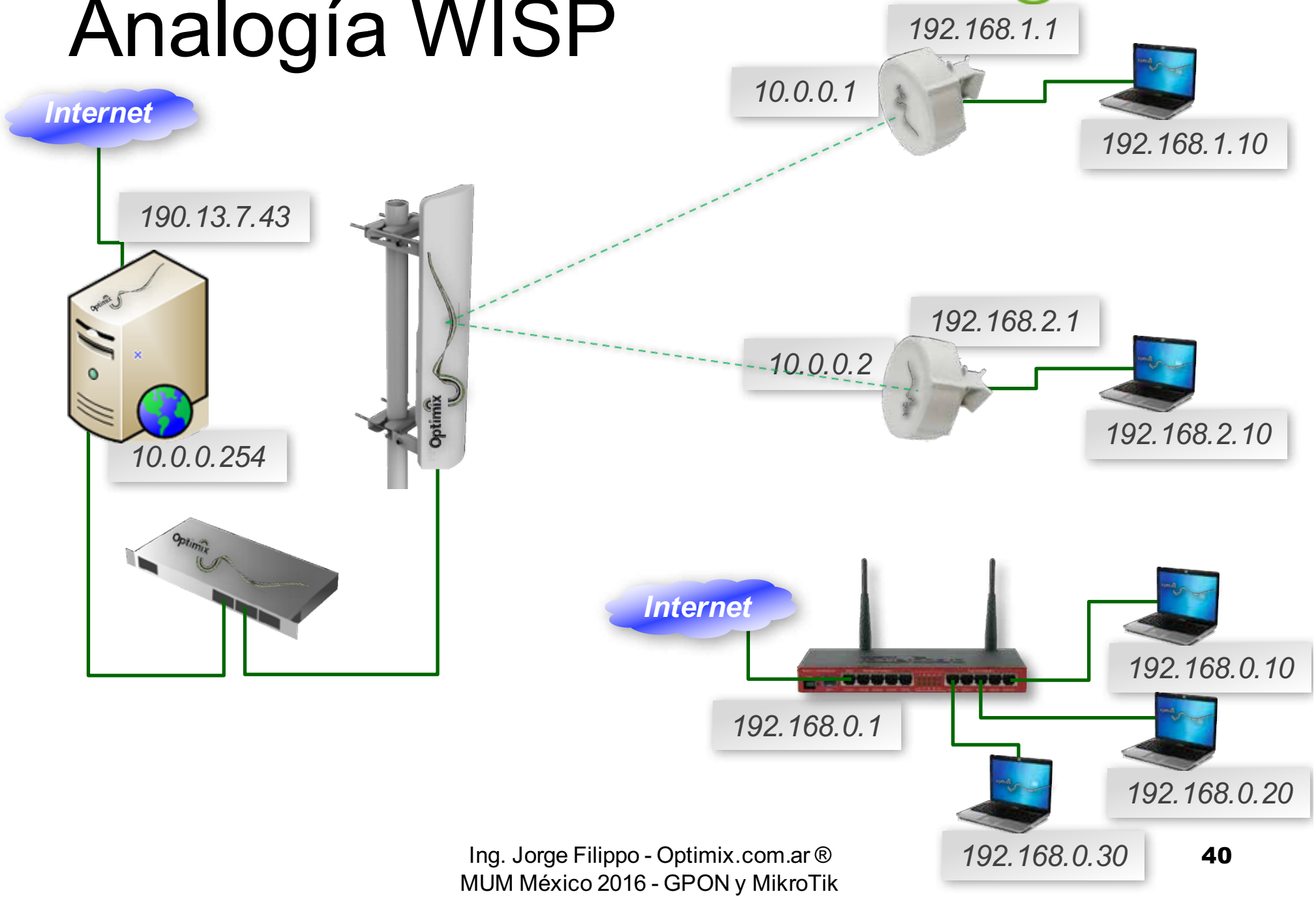
Manteniendo la lógica



Manteniendo la lógica



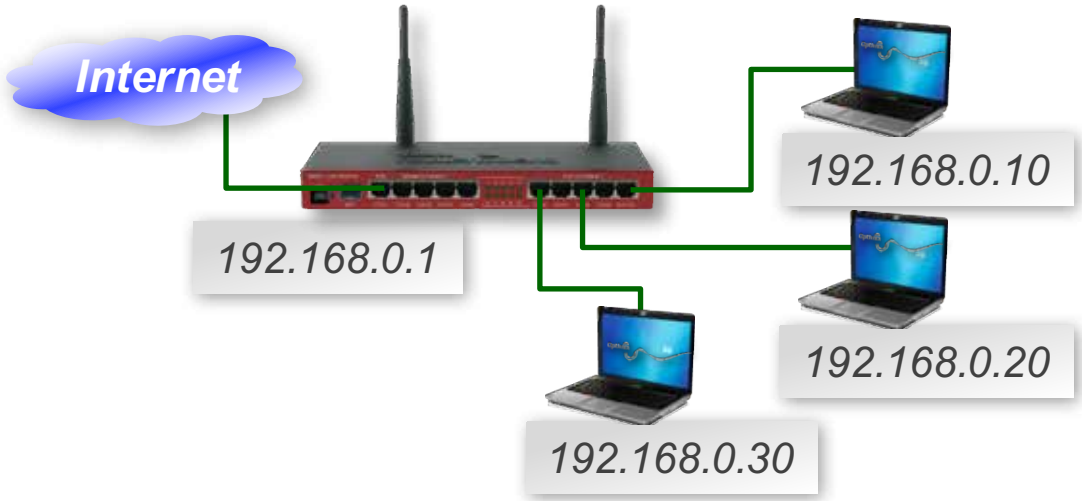
Analogía WISP



Muy lejos!...

- Para que una dependencia extremadamente lejana tenga Internet:
  - Fibra óptica PTP – Excelentes prestaciones y alto costo. Lógica controlable desde la LAN principal.
  - Punto a punto inalámbrico – Prestaciones inferiores y bajo costo. Lógica controlable desde la LAN principal.
  - Servicios de Internet propios dedicados:
    - Internet puro – Prestaciones mínimas a un costo intermedio, pero sin control. La dependencia opera en libertinaje.
    - Internet y vinculación VPN – Se logra un buen control desde la LAN principal, con prestaciones y costo intermedios.

PCQ y *Layer 7*

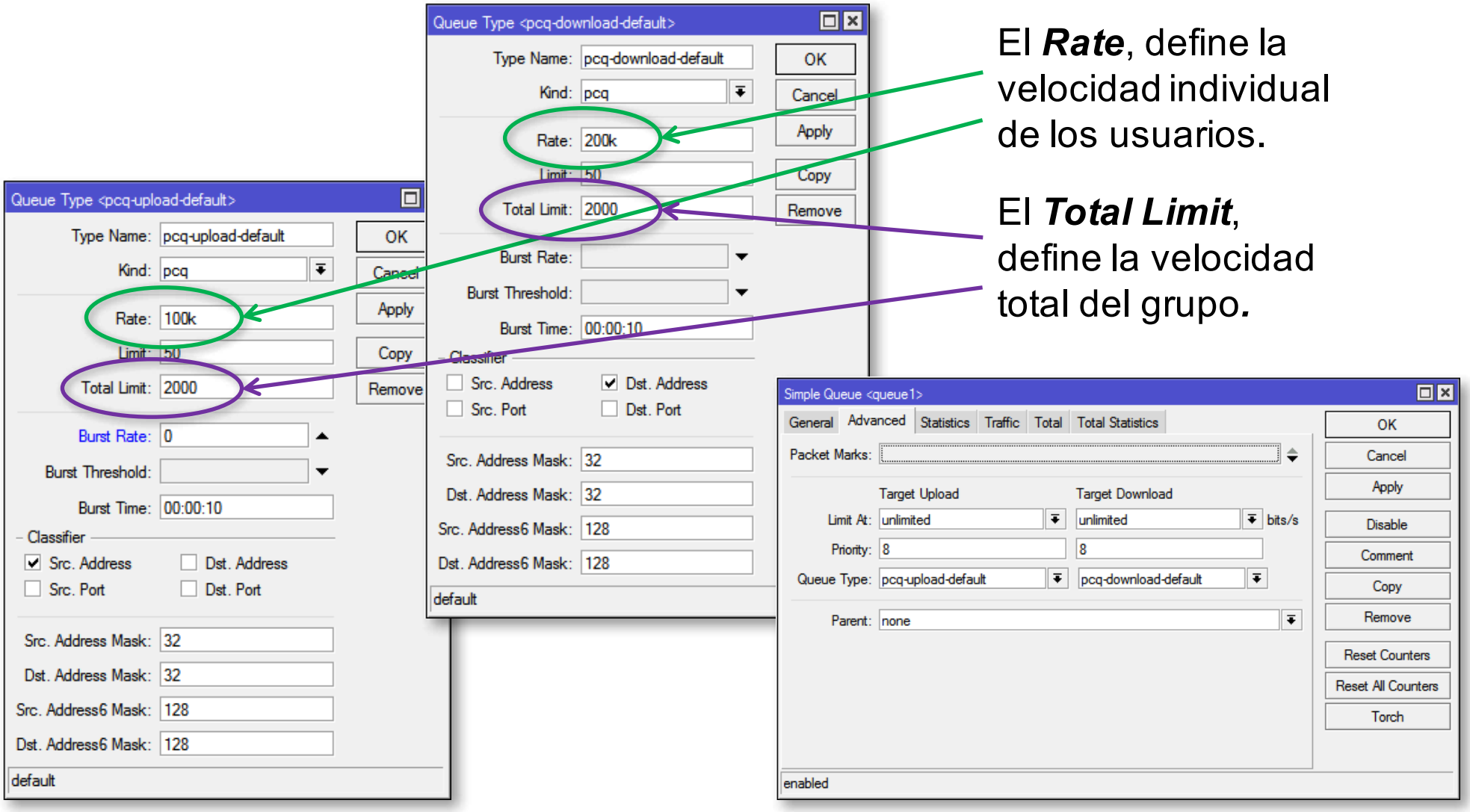


- Medidas básicas de control de dependencias remotas:
  - Control de ancho de banda con PCQ. Para que, independientemente de la cantidad de usuarios habitan la red, se pueda garantizar **que ningún dispositivo consuma los recursos de los demás**.
  - Control de contenido en Layer 7. Para que podamos implementar controles de contenidos que desde la óptica laboral, parental, y moral, no deben accederse.

Control ancho de banda ***PCQ***

- ***PCQ*** divide el tráfico en flujos. Cada flujo, es una cola FIFO, con tamaño de cola `Rate`.
- Luego, ***PCQ*** reúne a todo el grupo de flujos en otra FIFO, donde la opción `Total Limit` define el tamaño total de esa cola del grupo.

PCQ en *Simple Queues*



El ***Rate***, define la velocidad individual de los usuarios.

El ***Total Limit***, define la velocidad total del grupo.

Control ***Layer 7***

- Se pueden interceptar peticiones con el criterio “dominio destino”, para bloquear sitios como ***facebook.com***, incluso en páginas ***HTTPS***.

- Para ello, basta con crear patrones de expresiones regulares en ***Firewall*** -> ***Layer 7***, del modo:

  - **^.+(facebook.com).*$**

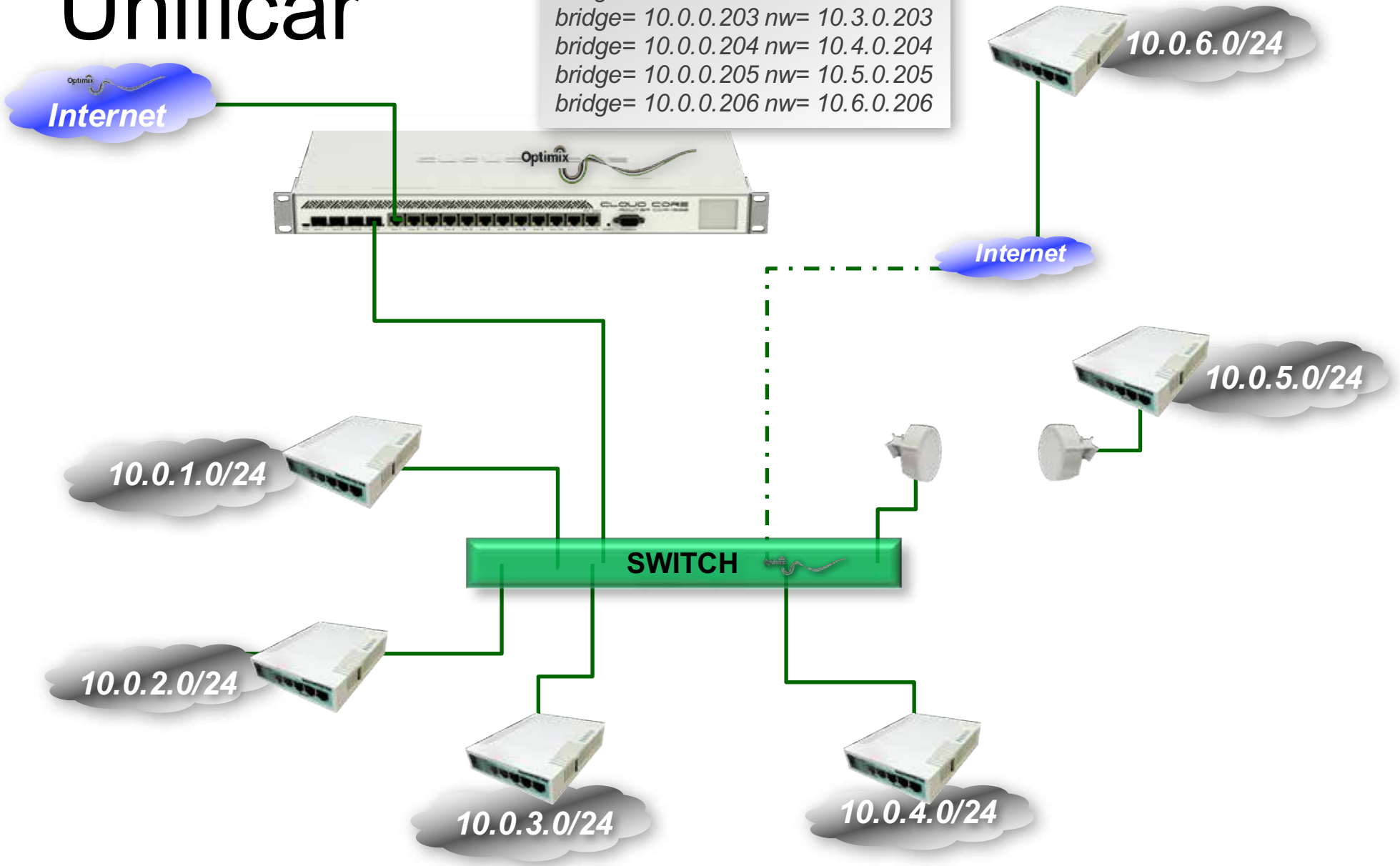
- Creado el patrón, solo resta generar una regla en ***Firewall*** -> ***Filter*** -> ***Advanced***, que intercepte el tráfico que contenga dicho patrón ***Layer 7***, y lo bloquee.

Muy lejos!..., solo Internet

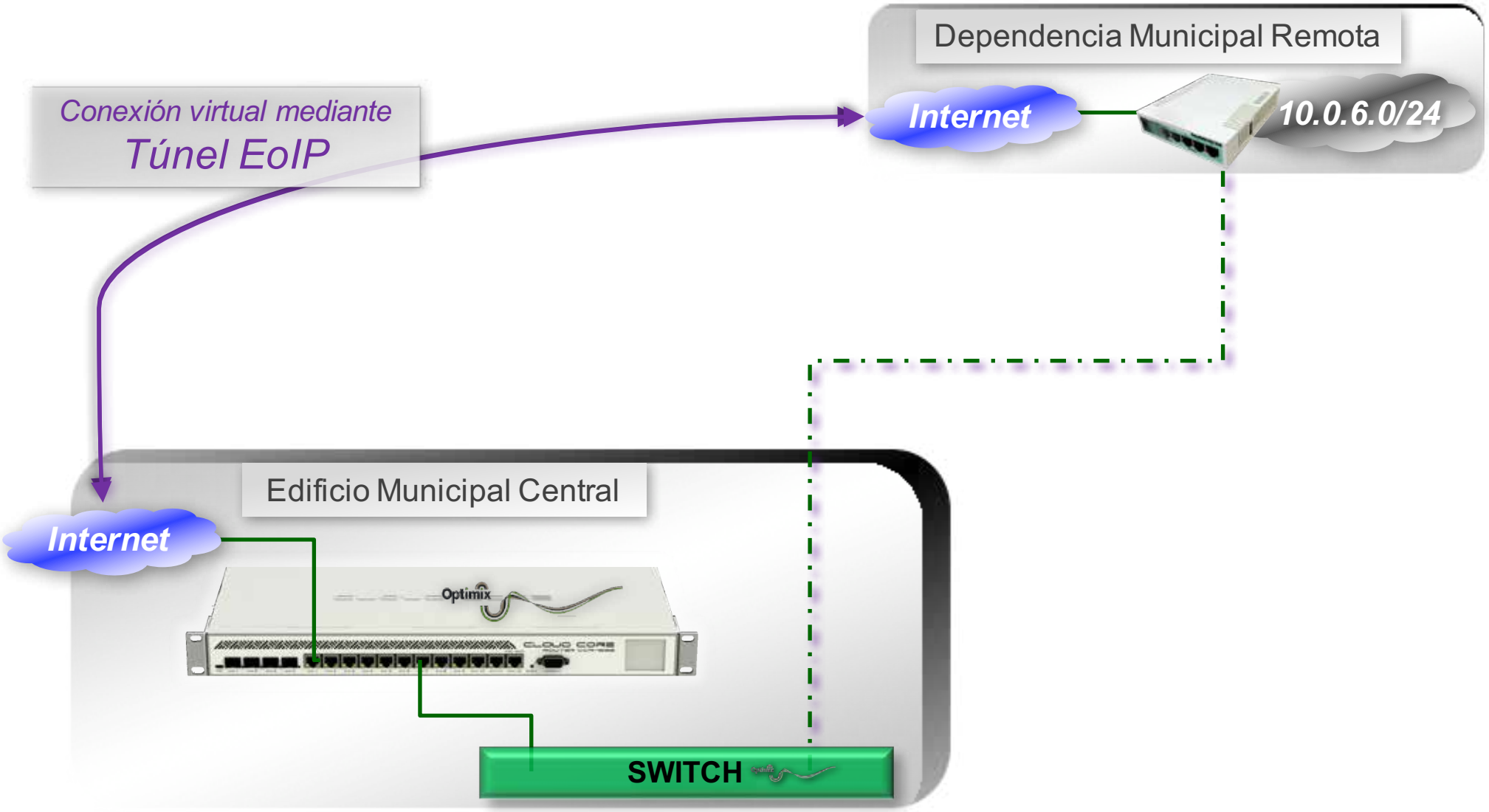
- Una dependencia con solo Internet no rinde al 100% del potencial Municipal:
  - Se dificulta controlar el ancho de banda según tráfico Internet o Municipal.
  - Se dificulta monitorear el uptime de los dispositivos LAN.
  - Se dificulta auditar acciones locales, y se fuerza la publicación de los sistemas en Internet (exponiéndonos a DOS).
- Tenemos que incorporar las redes remotas a nuestra lógica privada Municipal, y eso implica VPNs.

Unificar

bridge= 10.0.0.201 nw= 10.1.0.201
bridge= 10.0.0.202 nw= 10.2.0.202
bridge= 10.0.0.203 nw= 10.3.0.203
bridge= 10.0.0.204 nw= 10.4.0.204
bridge= 10.0.0.205 nw= 10.5.0.205
bridge= 10.0.0.206 nw= 10.6.0.206



Dependencias en Internet



Optimix
Network Engineering

GPON

Interconectar una ciudad, manteniendo un control minucioso a nivel de dispositivos.

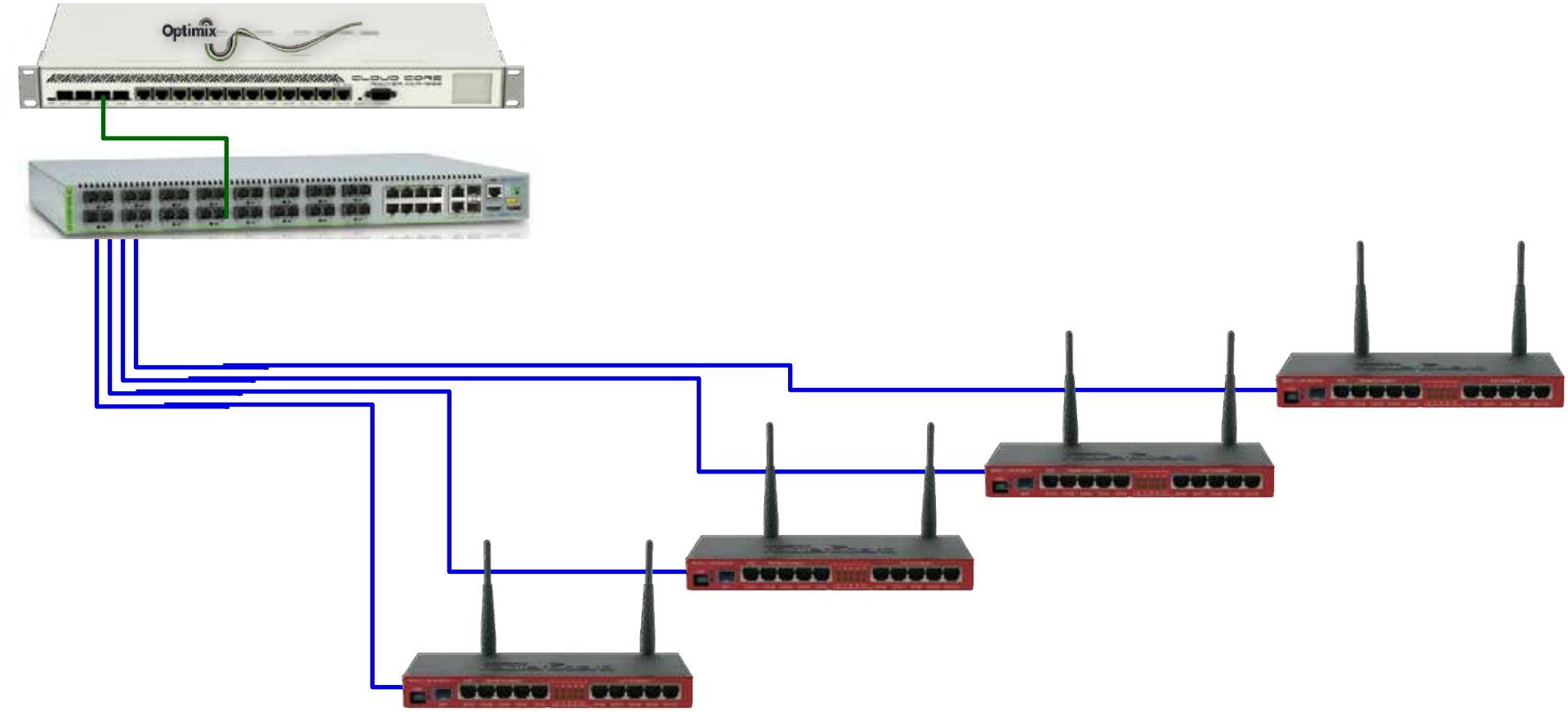
Unificar toda la ciudad

- El transporte mediante switches, nos expone a vulnerabilidades de L2.
- La gestión de fibras punto a punto, es costosa.
- Pero surge la gestión por VLANs, para que en un concentrador en L2, se puedan aislar los entornos de broadcast para proteger a cada usuario de los demás.

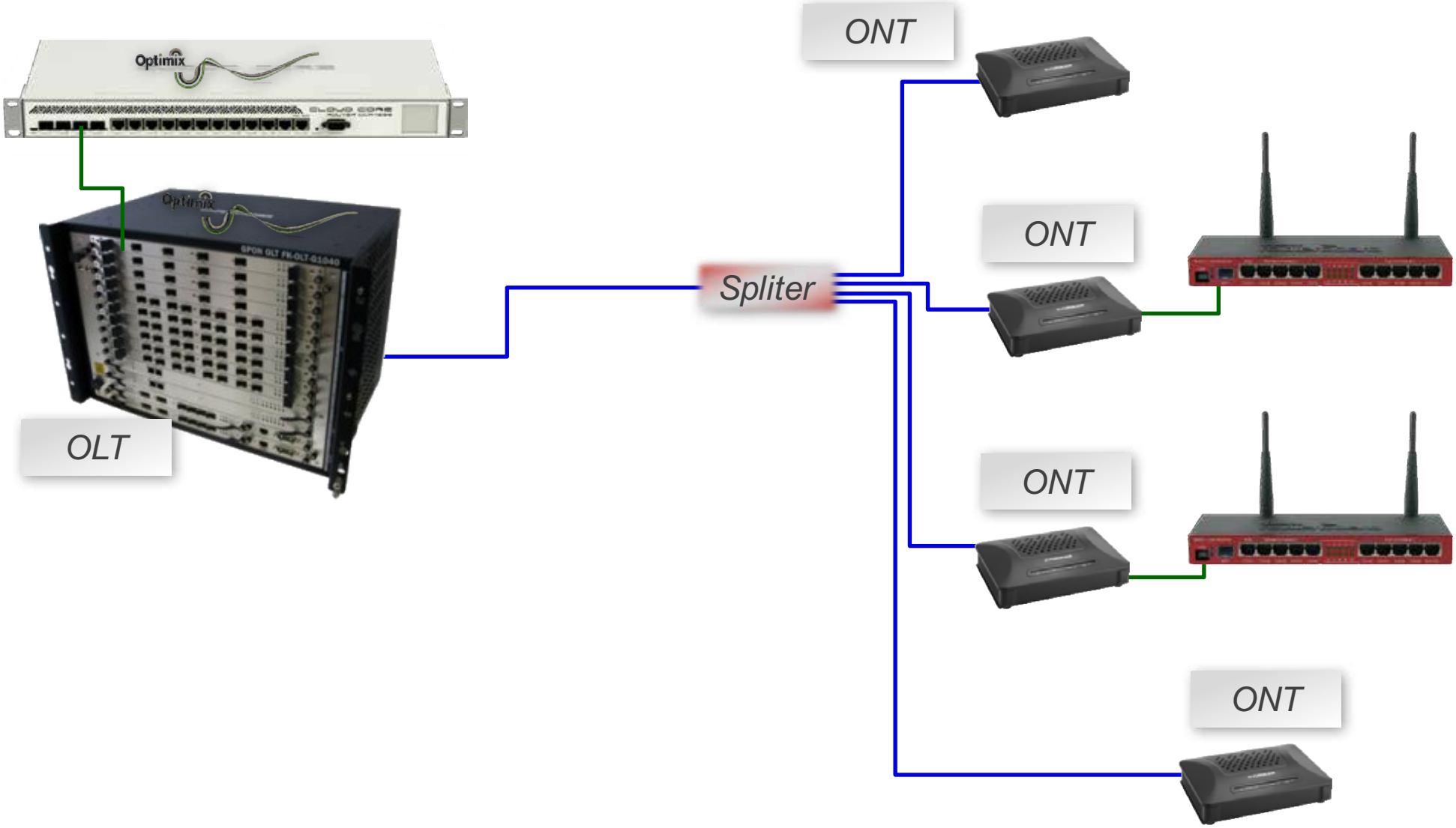
En términos explícitos

- Se conectan todas las delegaciones mediante un despliegue de fibra GPON.
- Todos los vínculos se despliegan mediante spliteo, a partir de troncales mayores en la OLT.
- Esta estructura unificada en vínculos de fibra, se administra y relaciona con VLANs.
- Estas VLANs se destaguean en el dispositivo cliente llamado ONU, que posee puertos ethernet mediante los que se trasduce al mundo.

Fibra Punto a Punto

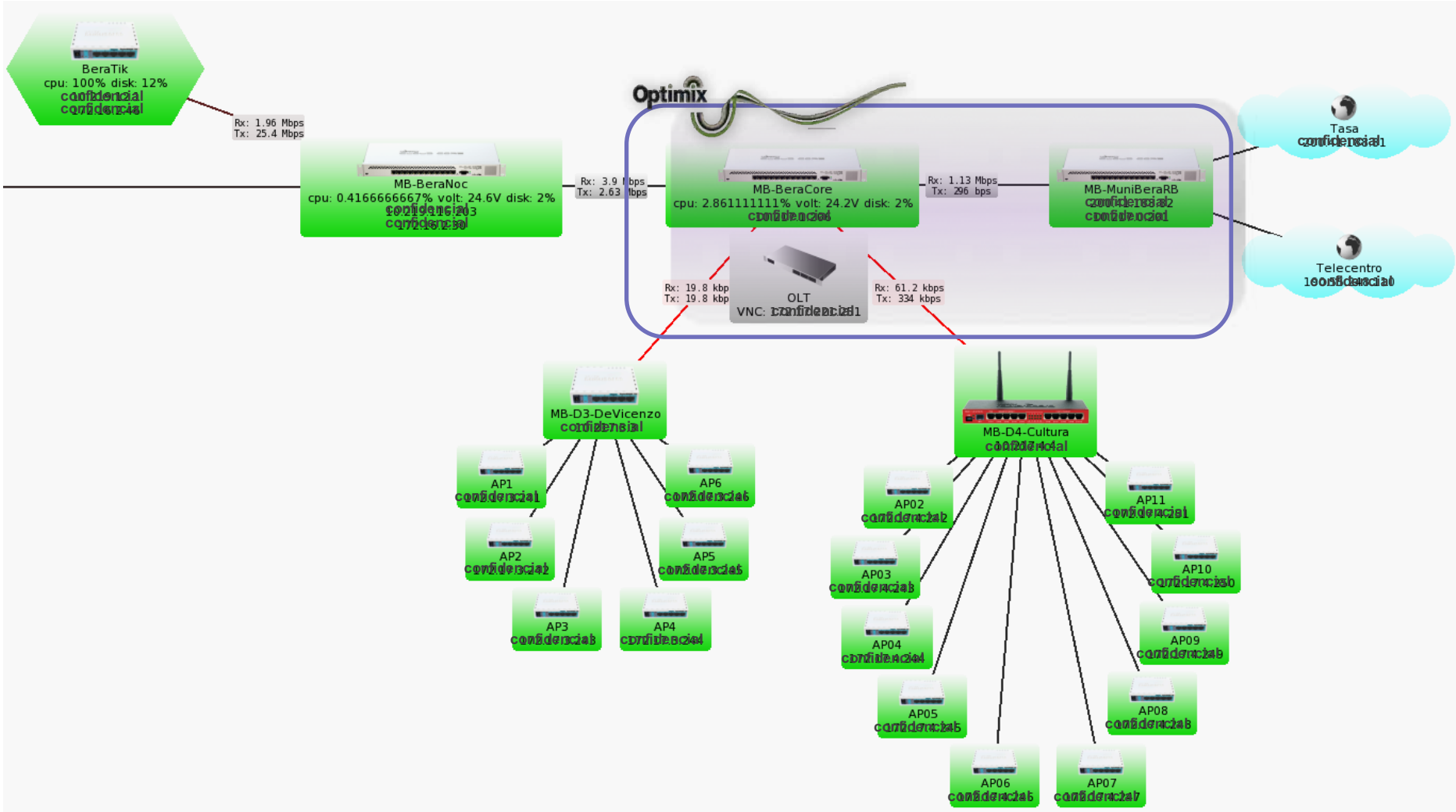


GPON – OLT y ONTs

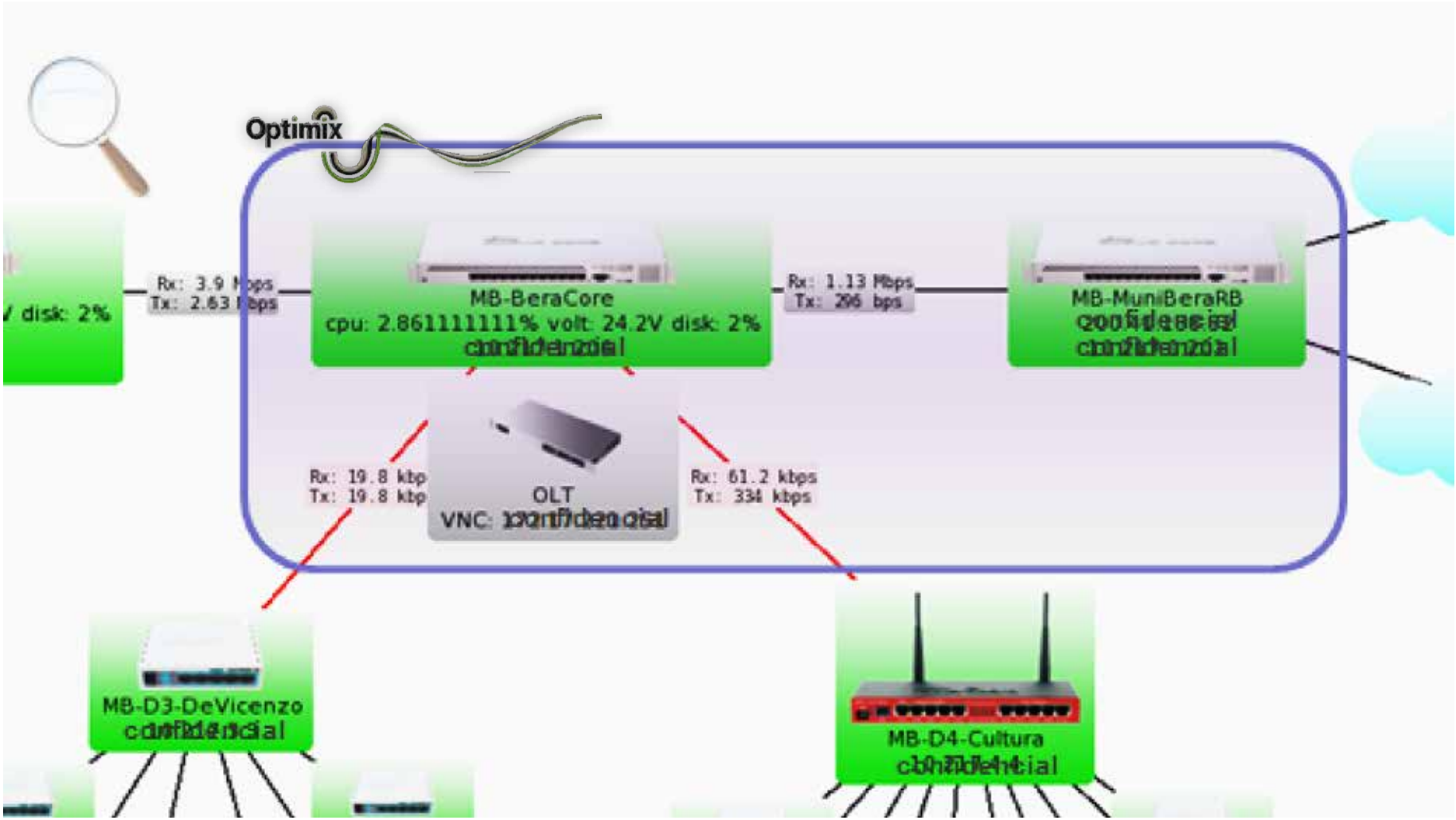



Optimix
Optimix
Optimix
GPON OLT FX-OLT-G

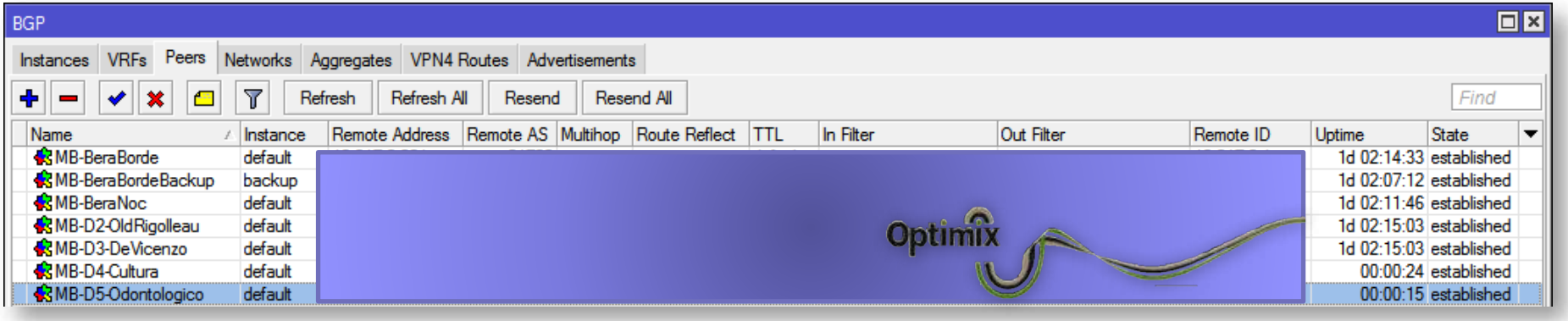
Estructura

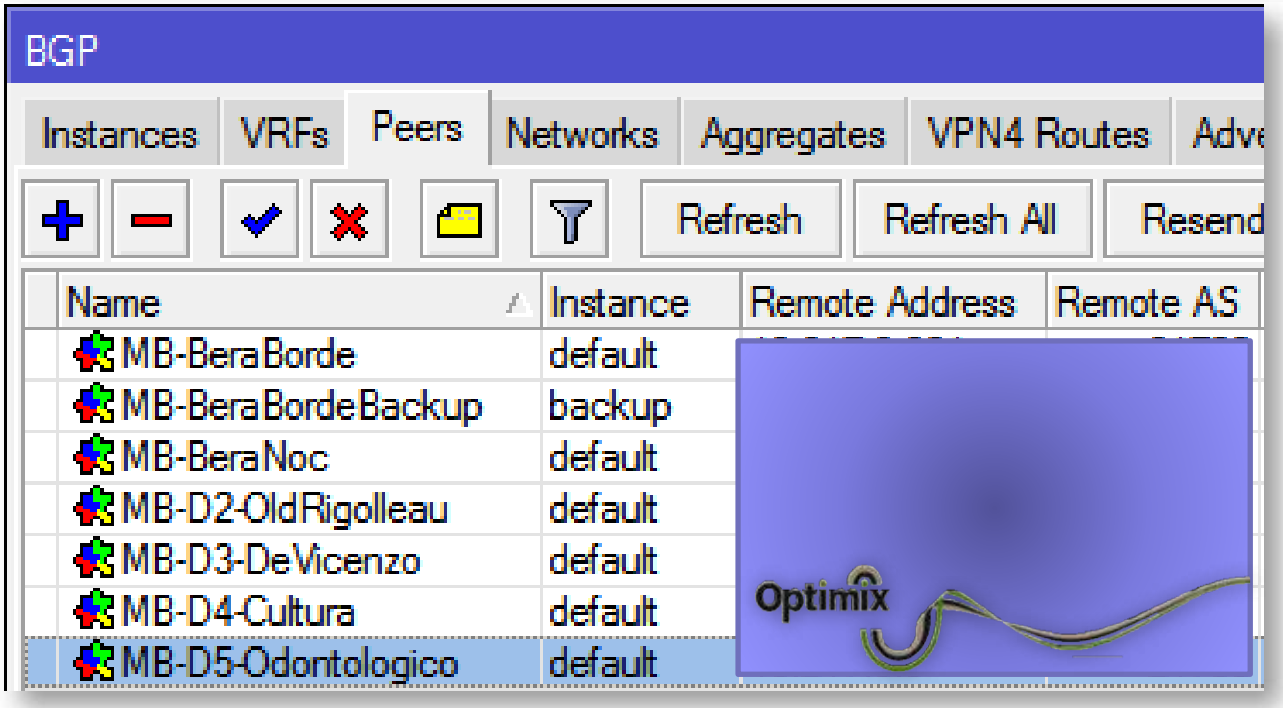

BeraTik
cpu: 100% disk: 12%
Rx: 1.96 Mbps
Tx: 25.4 Mbps
MB-BeraNoc
cpu: 0.4166666667% volt: 24.6V disk: 2%
Rx: 3.9 Mbps
Tx: 2.63 Mbps
Optimix
MB-BeraCore
cpu: 2.8611111111% volt: 24.2V disk: 2%
Rx: 1.13 Mbps
Tx: 296 bps
MB-MuniBeraRB
Tasa
Telecentro
Rx: 19.8 kbp
Tx: 19.8 kbp
OLT
Rx: 61.2 kbps
Tx: 334 kbps
MB-D3-DeVicenzo
MB-D4-Cultura
AP1
AP2
AP3
AP4
AP5
AP6
AP02
AP03
AP04
AP05
AP06
AP07
AP08
AP09
AP10
AP11

Estructura

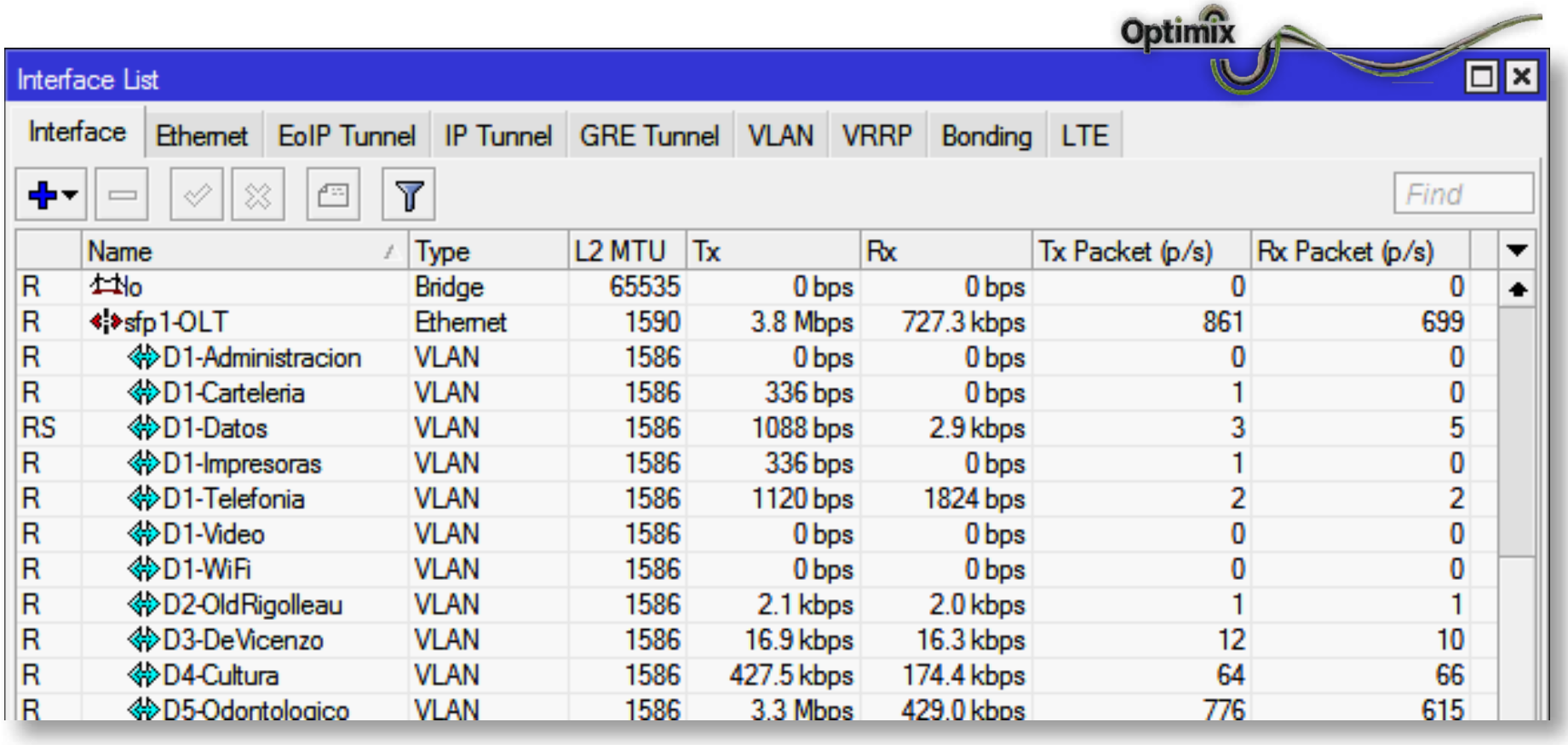

Optimix
Rx: 3.9 Mbps
Tx: 2.63 Mbps
MB-BeraCore
cpu: 2.861111111% volt: 24.2V disk: 2%
Rx: 1.13 Mbps
Tx: 296 bps
MB-MuniBeraRB
Rx: 19.8 kbps
Tx: 19.8 kbps
OLT
Rx: 61.2 kbps
Tx: 334 kbps
MB-D3-DeVicenzo
MB-D4-Cultura

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

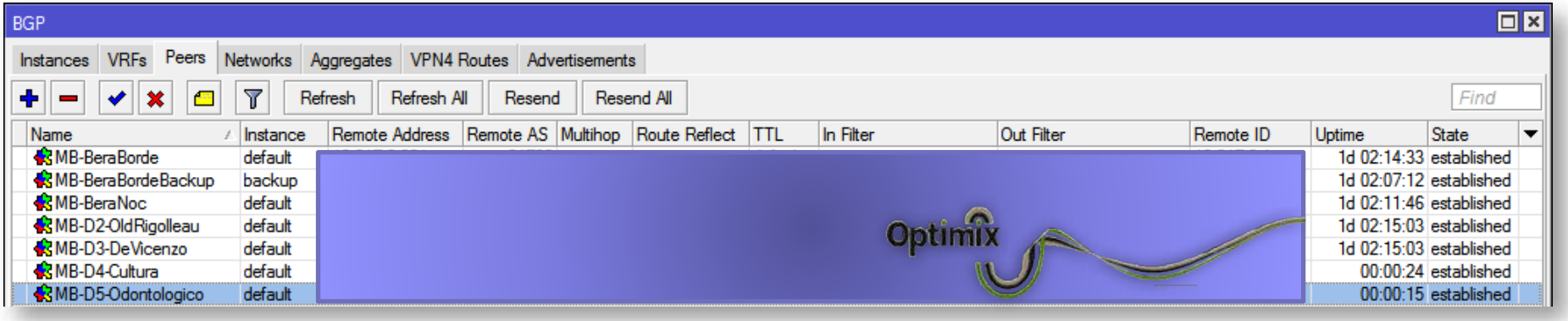

BGP
Instances
VRFs
Peers
Networks
Aggregates
VPN4 Routes
Refresh
Refresh All
Resend
Name
Instance
Remote Address
Remote AS
MB-BeraBorde default
MB-BeraBordeBackup backup
MB-BeraNoc default
MB-D2-OldRigolleau default
MB-D3-DeVicenzo default
MB-D4-Cultura default
MB-D5-Odontologico default
Optimix

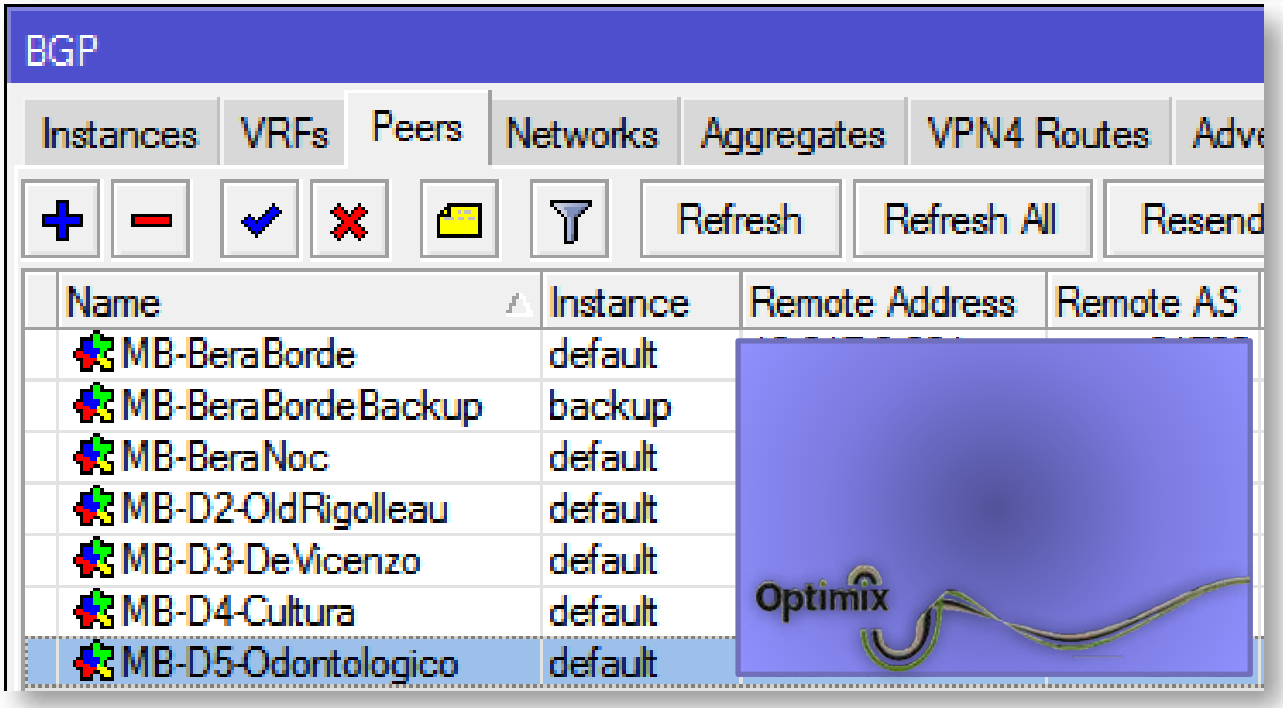
Router Core – VLANs



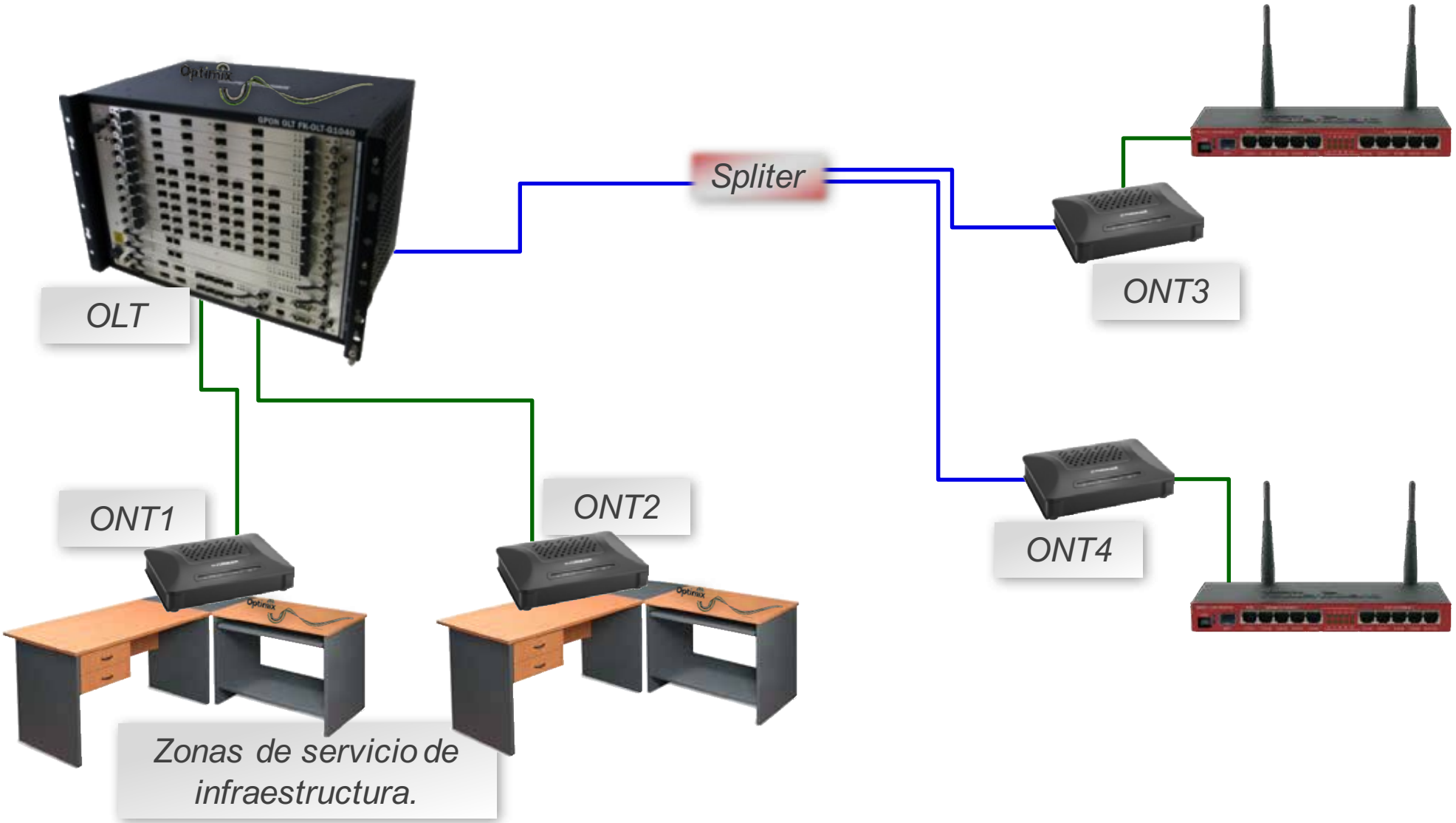
	Name	Type	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)
R	lo	Bridge	65535	0 bps	0 bps	0	0
R	sfp1-OLT	Ethernet	1590	3.8 Mbps	727.3 kbps	861	699
R	D1-Administracion	VLAN	1586	0 bps	0 bps	0	0
R	D1-Carteleria	VLAN	1586	336 bps	0 bps	1	0
RS	D1-Datos	VLAN	1586	1088 bps	2.9 kbps	3	5
R	D1-Impresoras	VLAN	1586	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





GPON

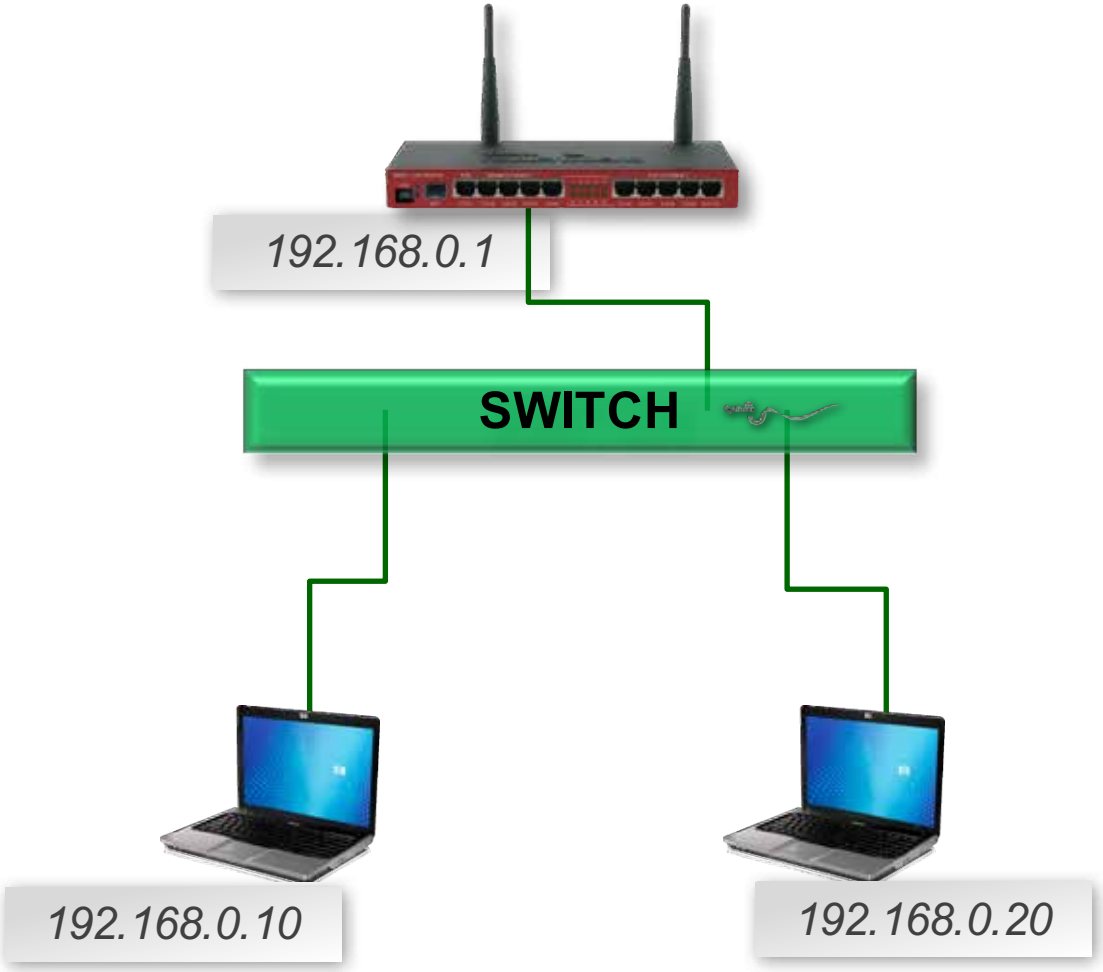

OLT
Spliter
ONT1
ONT2
ONT3
ONT4
Zonas de servicio de infraestructura.

Optimix
Network Engineering

Conceptos fundamentales de una arquitectura segura

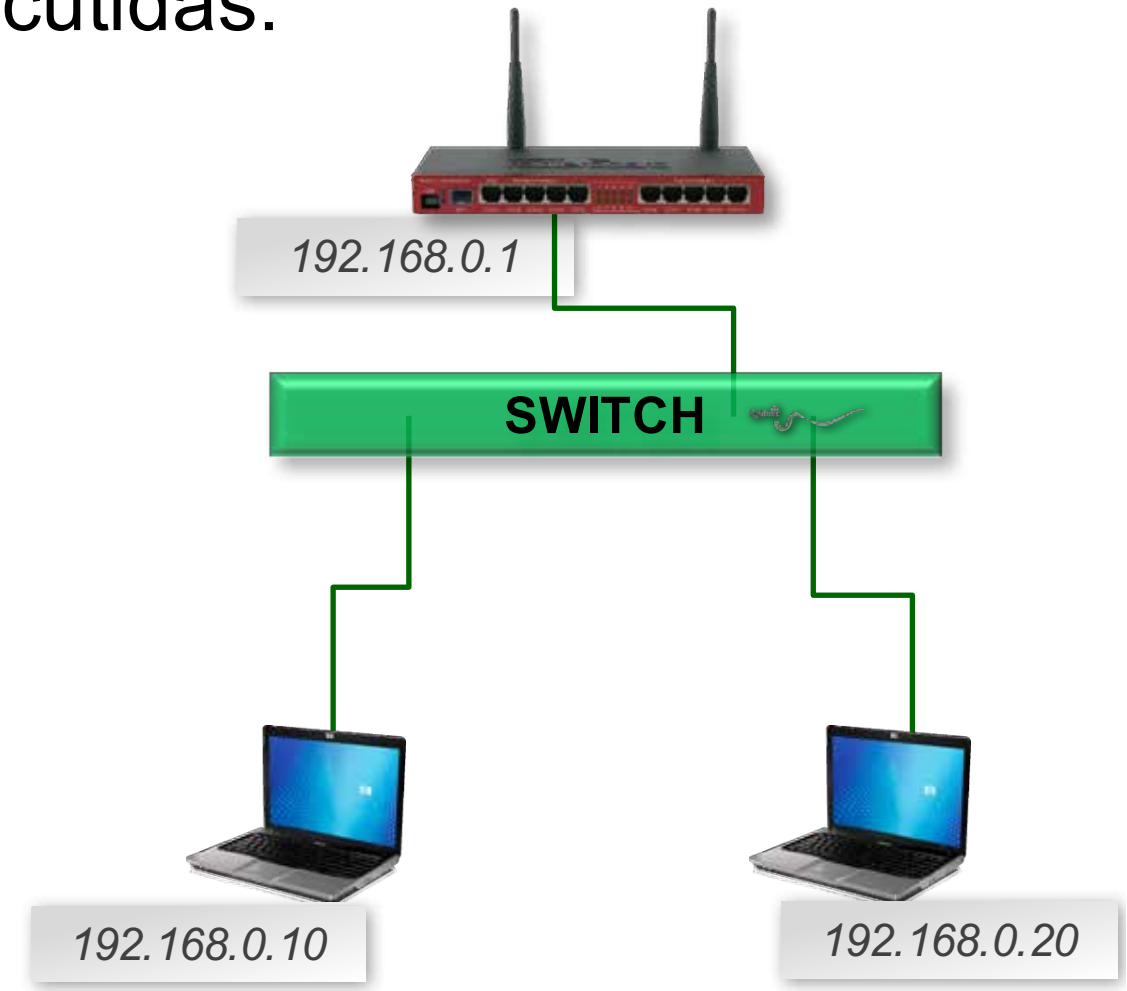
Causas y consecuencias de las distintas arquitecturas que nos guían hacia la red de Berazategui.

Red en L2

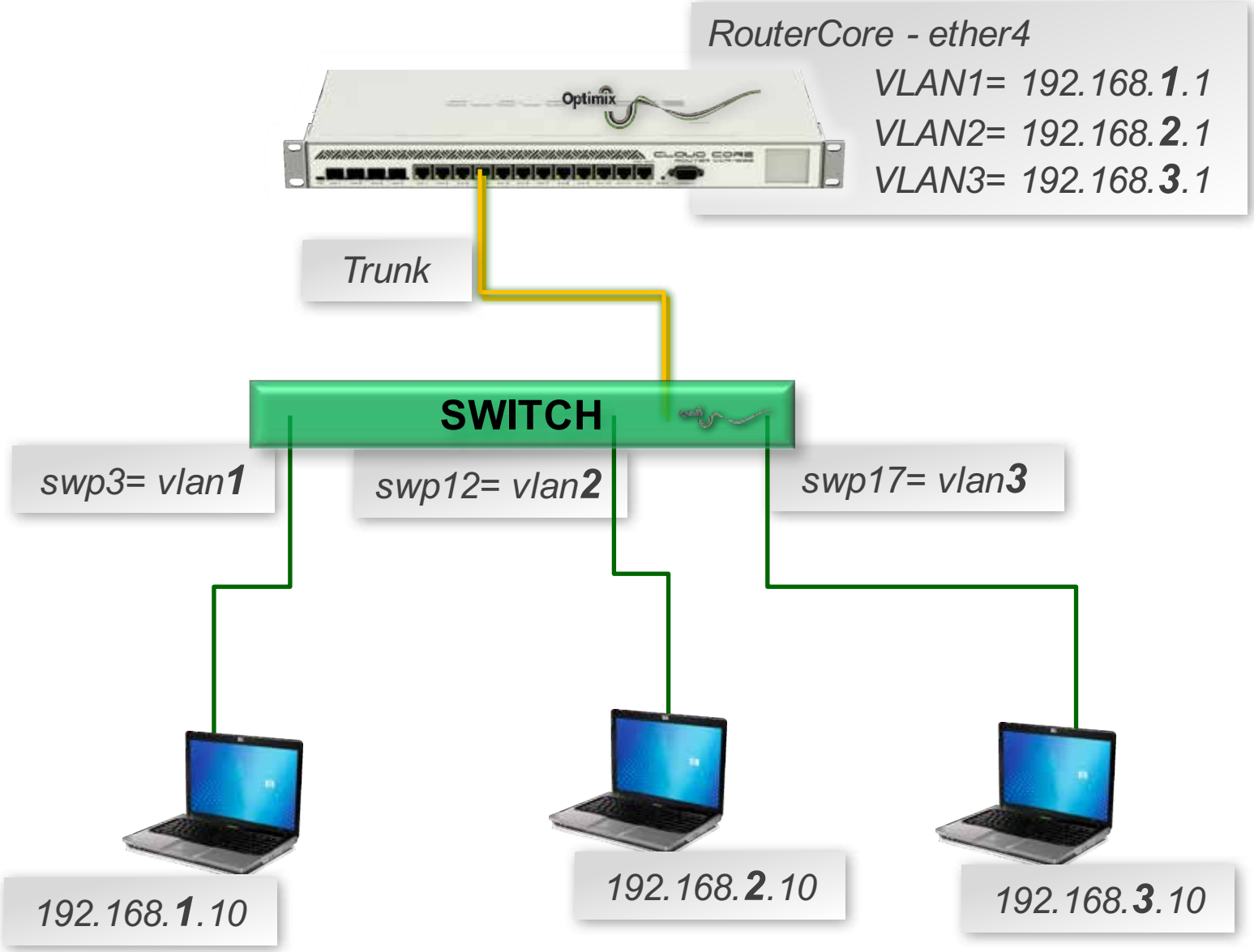


Red en L2

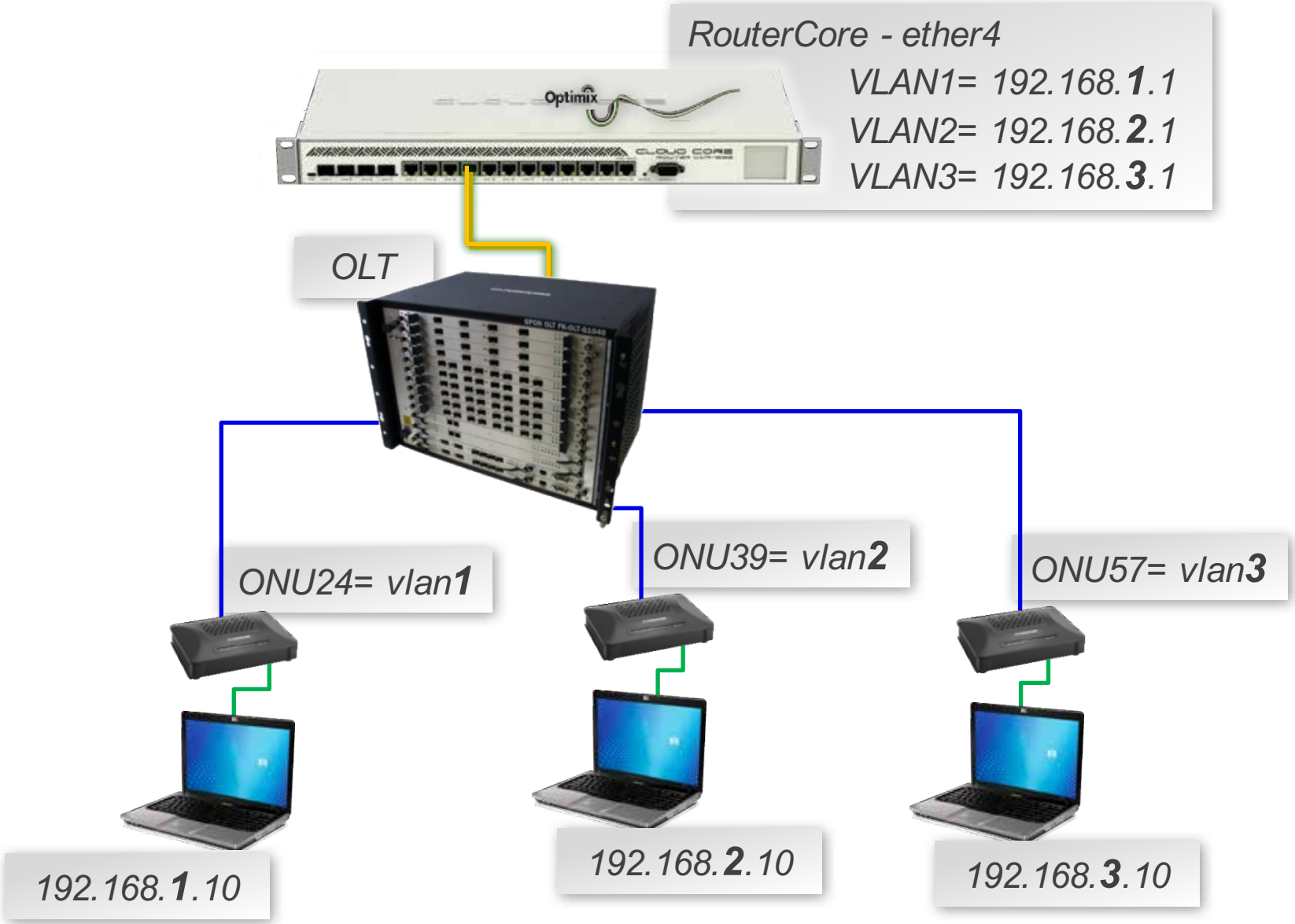
- Vulnerabilidades discutidas:
  - Conflicto de IP.
  - DHCP espurio.
  - Tormentas de ARP.
- Soluciones:
  - Una red por puerto.
  - Una red por VLAN.



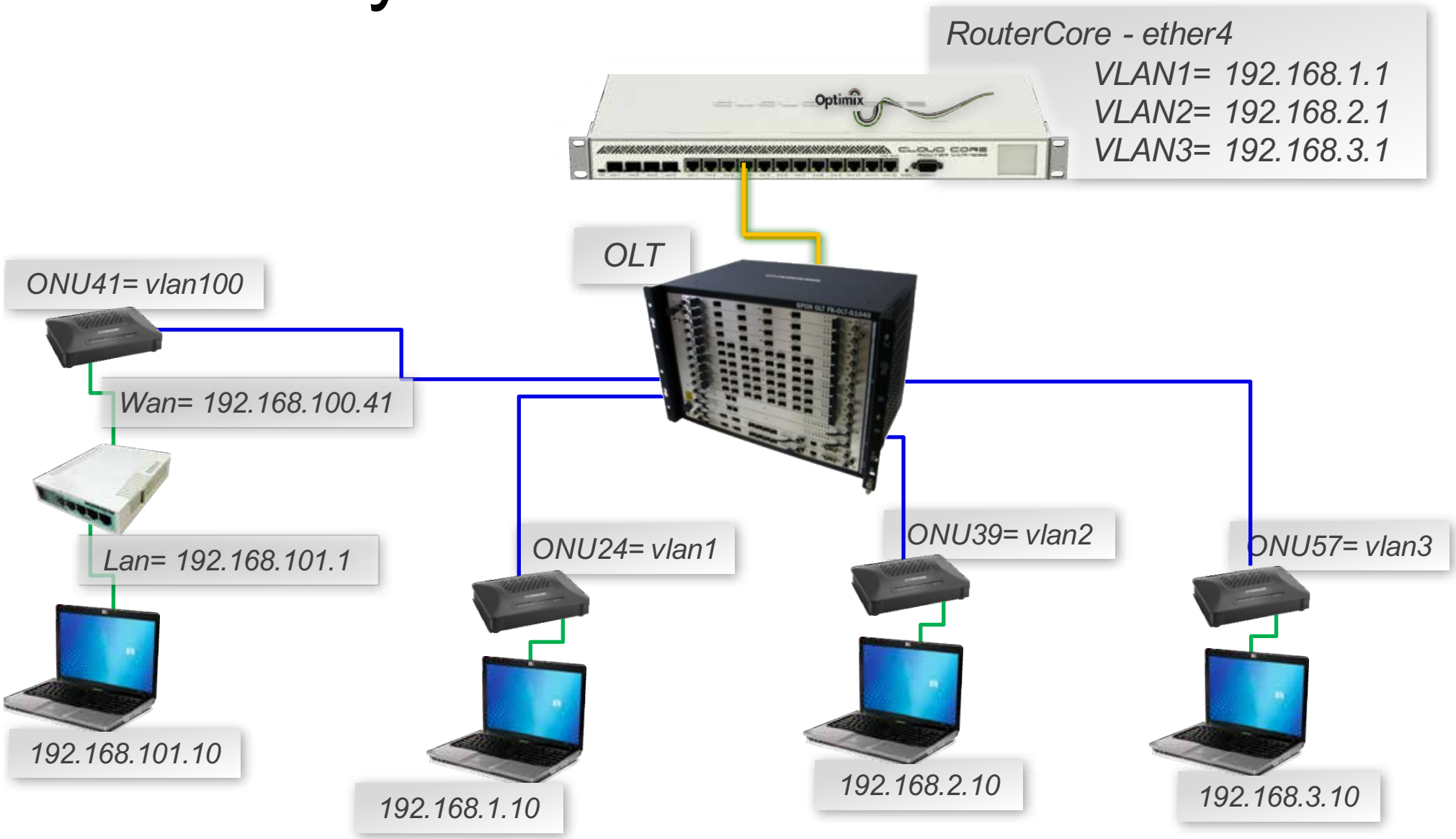
Una red por puerto con VLANs



Una red por puerto con VLANs



VLANs y RSs


RouterCore - ether4
VLAN1= 192.168.1.1
VLAN2= 192.168.2.1
VLAN3= 192.168.3.1
OLT
ONU41= vlan100
Wan= 192.168.100.41
Lan= 192.168.101.1
192.168.101.10
ONU24= vlan1
192.168.1.10
ONU39= vlan2
192.168.2.10
ONU57= vlan3
192.168.3.10

Conclusiones

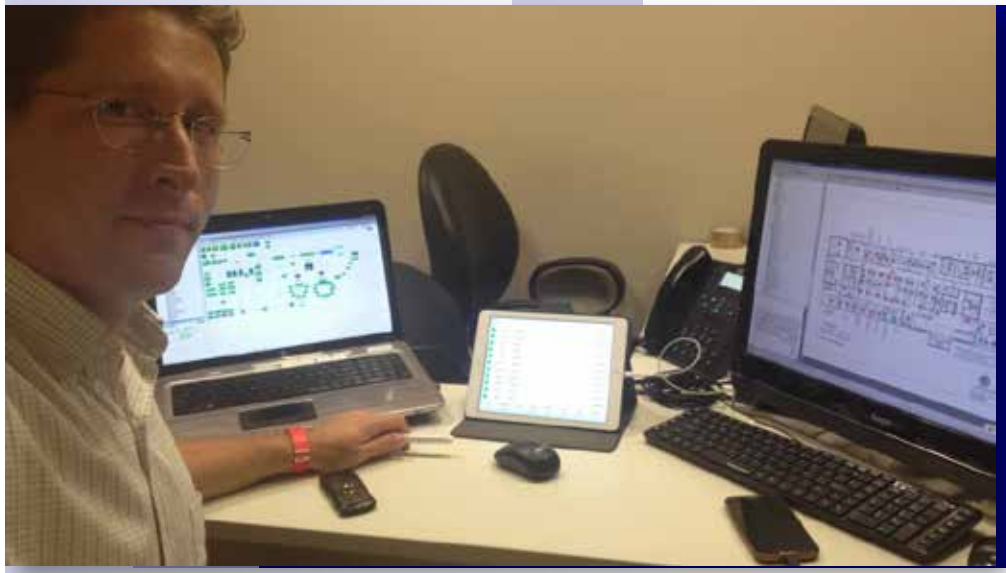
- La gestión de VLANs, nos permite segmentar las delegaciones que viajan por la infraestructura de transporte.
- El resto, sigue siendo MikroTik, con lo que ya nos sentimos cómodos.
- Podemos plantear en cada destino, el concepto de Router de Servicio, para mayor control local.
- Así, la red se extiende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

Inauguración 2015

Optimix
Network Engineering



Gracias!

Ing. Jorge Filippo

INDEX SOLUCIONES IP

MikroTik MEXICO
Enrutamiento y Soluciones Inalámbricas