ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA DE TELCOMUNICACIÓN
UNIVERSIDAD POLITÉCNICA DE CARTAGENA

Trabajo Fin de Grado

Estudio sobre la modernización de la red de una PyME y su adaptación a IPv6

AUTOR: Félix Reverte Hernández

DIRECTORES: Alejandro Martínez Sala

Juan Carlos Sánchez Aarnoutse

OCTUBRE 2014

Autor	Félix Reverte Hernández
E-mail del autor	felix@felixreverte.com
Director(es)	Alejandro Martínez Sala Juan Carlos Sánchez Aarnoutse
Título del TFG	Estudio sobre la modernización de la red de una PyME y su adaptación a IPv6

Resumen:

En este trabajo se van a estudiar y ofrecer soluciones para mejorar la red de las PyMEs.

A lo largo de esta memoria se describirá la situación actual de las PyMEs, las tecnologías existentes, las opciones que ofrecen los operadores de telecomunicaciones y los distintos protocolos y estándares que se han tenido en cuenta en la realización del presente trabajo.

Se elegirán las mejores soluciones para abaratar costes, seleccionando electrónica de red, software de monitorización y gestión de red y servidores. Se aportarán las configuraciones óptimas.
Además, se proporcionarán configuraciones para la mejora de la red de una PyME adaptándola a IPv6.

Se pretende ofrecer una solución genérica para conseguir una buena red por un coste mínimo utilizando software libre y virtualización.

Titulación	Grado en Ingeniería Telemática
Departamento	Tecnologías de la Información y las Comunicaciones
Fecha de Presentación	Octubre 2014

Índice

Capítulo 1

1. Introducción 6
1.1 Motivación 6
1.2 Objetivos 7
1.3 Descripción del trabajo 8

Capítulo 2

2. Introducción a IPv6 10
2.1. Cabecera 10
2.2. Direccionamiento 12

Capítulo 3

3. Situación actual 19
3.1. Introducción 19
3.2. Contexto 19
3.3. Ofertas de las principales operadoras para las PyMEs 20

Capítulo 4

4. Entorno de trabajo 24
4.1. Introducción 24
4.2. Entorno en la PyME 24
4.3. Pruebas en laboratorio 27
4.3.1- Equipos 27
4.3.2- Pruebas 30
4.3.2.1- Prueba de streaming de audio 35
4.3.2.2- Maqueta completa con pruebas de protocolos 37
4.3.2.3- VLAN Asimétricas 40

Capítulo 5

5. Soluciones 41
5.1. Introducción 41
5.2. Solución utilizando únicamente IPv4 42
5.3. Solución utilizando únicamente IPv6 49
5.4. Solución de convivencia IPv4 – IPv6 53

Capítulo 6

6. Conclusiones 64
Líneas de desarrollo futuro 65

Bibliografía 66

Anexos 67
Manual de instalación de PfSense 67
Manual de emulación de un router con IOS CISCO 76
Manual de instalación de Nagwin 78
Manual de instalación de OpenNMS 80
Manual de instalación de Cacti 82
Manual de configuración de IPv6 en Windows XP/Debian 83

Glosario de términos. 85

Capítulo 1

1. Introducción

Es bien sabido que a fecha de 2014, tiempos en los que la economía no está en una de sus mejores épocas, los usuarios, y como no las empresas, necesitan seguir evolucionado y mejorando, pero con más cautela. Estas últimas necesitan un equipamiento informático y de red a la altura de los tiempos que corren pero sin poder permitirse grandes desembolsos para ser productivos y competentes.

Por esto, en este trabajo se pretende dar soluciones de redes que, utilizando bajo coste, proporcionen a las PyMEs una red óptima y actual. Todo esto partiendo de una red básica genérica y supuesta.

En este primer capítulo se van a presentar los motivos para la realización de este trabajo así como los objetivos que se pretenden alcanzar. Finalmente se describirá sucintamente el resto de los capítulos que componen esta memoria.

1.1 Motivación

La realización de este trabajo busca aportar a las PyMEs una red eficiente, segura y económica. Para ello será necesario, en primer lugar, conocer el equipamiento y los servicios que los principales operadores ofrecen actualmente a las empresas, tratando de buscar sus principales carencias y deficiencias.

Teniendo en cuenta que las PyMEs cuentan con pocos recursos y pocos departamentos, pero necesitan una red moderna y eficiente, se busca un sistema que minimice los costes de implantación.

En estos últimos años se ha producido un desarrollo de la informática tanto de consumo como profesional. Este avance ha provocado al mismo tiempo el abaratamiento de los componentes informáticos, poniendo a la disposición de los profesionales un amplio abanico de opciones, tanto de equipos como de configuraciones.

Por tanto, se pueden conseguir equipos económicos para las PyMEs gracias al menor coste de los componentes para emplear la virtualización de sistemas.

Debido a que los ordenadores son cada vez más potentes y asequibles se pueden emplear pocos equipos y en ellos montar varios servicios virtualizados como pueden ser: Servidores DNS, DHCP, LDAP, Firewall, RADIUS, gestión y monitorización.

Además, se pretende aportar un salto de calidad proporcionando distribuciones de red compatibles y adaptables a IPv6. Se aportarán maquetas con distintas configuraciones dando solución a los problemas que la convivencia de IPv4 e IPv6 conlleva.

Con el desarrollo de este trabajo se obtendrá una solución de red asequible pero eficiente a las empresas. Un trabajo económico que usa software libre con múltiples opciones de configuración y fiable, que aporta un salto de calidad respecto a las soluciones que ofrecen los operadores.

1.2 Objetivos

Los objetivos globales del trabajo son la búsqueda, desarrollo e implantación de un prototipo de red para una PyME que cumpla con las siguientes características que se suponen mínimas para tener una red eficiente:

- Proporcionar soluciones red de una PyME, manteniéndola actualizada con adaptación a IPv6.

- Ofrecer a las PyMEs una arquitectura de red moderna (arquitectura en tres capas) con VLANs, gestión de red, seguridad (firewall) y control de acceso con ACL. Y en WiFi utilizando un servidor LDAP.
Aplicando para todo ello soluciones de bajo coste.

- Proporcionar herramientas gratuitas para la monitorización de la red como son Cacti, Nagios u OpenNMS, con el fin de controlar los problemas de red.

- Analizar los tipos de servicios usados y adaptar la configuración de la red para obtener la mayor eficiencia, observando qué protocolos ayudan con la QoS.

- Diseñar, implementar y poner en marcha un enrutador basado en software libre como es PfSense, de manera que se obtenga buen rendimiento en la red con un bajo coste.

- Virtualizar todo lo posible, ya sea PfSense, servidores DHCP y DNS, LDAP y RADIUS, haciendo valer el descenso del coste en los equipos informáticos.

Para comprender mejor estos objetivos se elaborarán maquetas de ejemplo con las características probadas y sugeridas.

1.3 Descripción del trabajo

En esta sección se va a proceder a enumerar el contenido de cada uno de los siguientes capítulos.

En el capítulo 2 se realiza una explicación completa sobre el protocolo IPv6, donde se explica la cabecera y el direccionamiento que utiliza.

En el capítulo 3 se define una suposición del estado actual de la red de una PyME y se enumeran las opciones, equipos y servicios que ofrecen las principales operadoras (Telefónica, ONO y Vodafone) a empresas.

En el capítulo 4 se propone una hipótesis de partida para la que se supone es la red mínima necesaria para una PyME, con sus servicios y equipos.

En el capítulo 5 se definen diferentes soluciones para la red de una PyME, desde las configuraciones más sencillas (ofreciendo soluciones que implementan únicamente IPv4 o IPv6) a las más complejas, (soluciones mixtas o de convivencia entre ambas versiones). Asimismo, se aportan maquetas y configuraciones para las diferentes soluciones descritas.

Por último, en el capítulo 6 se exponen las conclusiones extraídas en el desarrollo del trabajo y las posibles líneas futuras.

Para concluir este primer capítulo se explica de forma esquemática la consistencia del trabajo:

- Suponer una hipótesis sobre la red actual de las PyMEs.
- Comprobar las soluciones que ofrecen los proveedores de servicios (ISP).
- Proporcionar soluciones económicas.
- Encontrar un software libre para virtualizar un enrutador y configurarlo.
- Configurar un software de monitorización y gestión de red de libre distribución.
- Comprobar el funcionamiento de estándares y protocolos de la electrónica de red para optimizar el rendimiento de la red interna de una empresa.
- Proporcionar soluciones para la adaptación de la red para la convivencia de IPv4 con IPv6.

Capítulo 2

2. Introducción a IPv6

En el presente capítulo se realiza una explicación sobre el protocolo IPv6, profundizando en su definición y uso. La información ha sido recopilada de varias páginas de Wikipedia que se añaden en la bibliografía.

Se ha considerado interesante la inclusión de IPv6 en este trabajo debido a que este protocolo se está utilizando por operadores y grandes empresas como Facebook y Google, así que las PyMEs deben estar dispuestas a convivir con esta tecnología y adaptarse a ella.

2.1. Cabecera

Para empezar, se explica el formato de cabecera que tiene este protocolo para conocer mejor que opciones nos brinda.

El paquete en IPv6 está compuesto por la cabecera (que tiene una parte fija y otra parte con las opciones) y la carga útil, éstos últimos serán los datos que se transmitan.

En la figura 2.1.1 se pueden observar los campos de la cabecera fija, donde los primeros 40 bytes son la cabecera del paquete donde se tienen los campos:

- Dirección origen (128 bits).
- Dirección destino (128 bits).
- Versión del protocolo IP (4 bits).
- Tipo de tráfico (8 bits, Prioridad del Paquete).
- Etiqueta de flujo (20 bits, Calidad de Servicio).
- Tamaño del campo de datos (16 bits).

- Cabecera siguiente (8 bits).
- Límite de saltos (8 bits, Tiempo de Vida, TTL de IPv4).

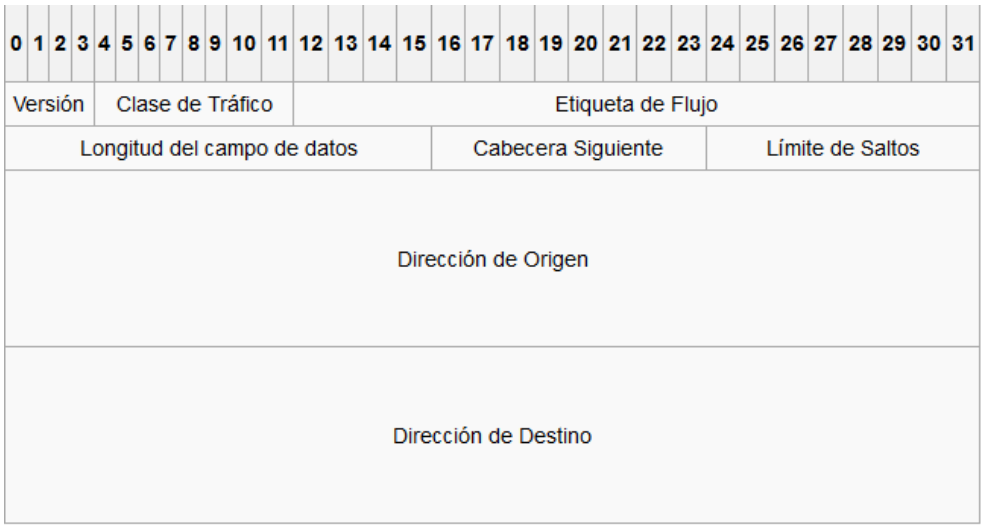


Figura 2.1.1. Cabecera fija de IPv6.

Cabecera de Extensión	Tipo	Tamaño	Descripción
Opciones salto a salto (*Hop-By-Hop Options*)	0	variable	Contiene datos que deben ser examinados por cada nodo a través de la ruta de envío de un paquete.
Enrutamiento (*Routing*)	43	variable	Métodos para especificar la forma de rutear un datagrama. (Usado con IPv6 móvil)
Cabecera de fragmentación (*Fragment*)	44	64 bits	Contiene parámetros para la fragmentación de los datagramas.
Cabecera de autenticación (*Authentication Header (AH)*)	51	variable	Contiene información para verificar la autenticación de la mayor parte de los datos del paquete (Ver IPsec)
Encapsulado de seguridad de la carga útil (*Encapsulating Security Payload (ESP)*)	50	variable	Lleva la información cifrada para comunicación segura (Ver IPsec).
Opciones para el destino (*Destination Options*)	60	variable	Información que necesita ser examinada solamente por los nodos de destino del paquete.
No Next Header	59	vacío	Indica que no hay más cabeceras

Figura 2.1.2. Cabeceras de extensión de IPv6.

En la figura 2.1.2 se pueden ver las partes de la cabecera de extensión, debiendo ubicarse en el datagrama en el orden especificado.

Por último y para dejar de explicar los campos de la cabecera, hay que decir que la carga útil dispone de 64 KB en modo estándar, pudiendo aumentar con la opción de carga jumbo (jumbo payload), alcanzando los 4 GB.

2.2. Direccionamiento

Ahora se pasa a explicar el direccionamiento en IPv6.

Al igual que en IPv4, se siguen usando direcciones unicast, anycast y multicast pero no se implementan en IPv6 las direcciones broadcast. En lugar de éstas se usa un grupo multicast de enlace local exclusivo. Las direcciones en IPv6 están formadas por 128 bits, disponiendo de 2^{128} direcciones.

Los formatos de dirección son:

- **Unicast y anycast**

  Los primeros 64 bits (usados para encaminamiento) identifican el prefijo de red junto al identificador de subred, siendo 48 bits o más para el prefijo de red y 16 o menos para el identificador de subred, y los últimos 64 bits identifican el interfaz de red del host.

  La dirección de enlace local (usada como broadcast) es una dirección unicast que usa un valor especifico del prefijo de red, está compuesto por los 10 primeros bits que son el prefijo, 54 bits a cero que consiguen que el prefijo de red sea el mismo para todas las direcciones locales y no sea enrutable y los últimos 64 bits que son el identificador de interfaz. Un ejemplo de este tipo de direcciones sería: fe80::/10

- **Multicast**

  En este tipo de direcciones los primeros 8 bits son el prefijo, que siempre será 8 bits a 1 para cualquier dirección, 4 bits para flags, que son R (Rendezvous), P (Prefijo, dirección basada en prefijo de red) y T (Transitoria, dirección asignada dinámicamente), 4 bits para scope que se utilizan para indicar donde la dirección es válida y única, y los 112 bits restantes para identificador del grupo multicast.

Una dirección en IPv6 se muestra mediante 8 grupos de 4 dígitos hexadecimales, cada grupo representa 16 bits. Los grupos se separan por el carácter ":" y un ejemplo de dirección valida podría ser:

2000:0a0b:3456:0000:0000:ae23:0789:1357

Se pueden utilizar mayúsculas y minúsculas pero se recomienda el uso de minúsculas, además, existen formas de simplificación para acortar las direcciones.

Una forma de simplificación es eliminar los ceros "0" iniciales de cada grupo, dejando en cada grupo un digito hexadecimal, de esta forma la dirección de ejemplo anterior quedaría:

2000:a0b:3456:0:0:ae23:789:1357

Otra manera de simplificar es omitir los grupos de ceros y dejar espacios en blanco, esto solo se puede dar una vez en la dirección ya que si se eliminan grupos de ceros alternos no sabremos cuantos grupos hay, además, como regla, si pueden hacerse varias sustituciones se debe realizar la de mayor número de grupos y si el número de grupos es igual debemos simplificar la de más a la izquierda. La dirección ejemplo anterior quedaría:

2000:a0b:3456::ae23:789:1357

Como direcciones especiales tendremos la dirección loopback, 0:0:0:0:0:0:0:1 y la dirección IPv6 indefinida, 0:0:0:0:0:0:0:0, que quedarían simplificadas de la siguiente manera: ::1 y :: respectivamente.

De cara a la transición y convivencia de IPv4 e IPv6 con la que se trabajará en entornos de doble direccionamiento, como veremos más adelante, existe una notación para expresar direcciones IPv6 que sean mapeadas o compatibles con IPv4 representando los últimos 32 bits de la dirección IPv6 en el formato decimal con puntos de IPv4. Como ejemplo de esto tenemos la dirección IPv6 ::ffff:c000:280 mapeada en IPv4 como ::ffff:192.0.2.128, siendo su conversión la siguiente:

Se tiene c000:0280 que en binario queda 11000000000000000000001010000000, las direcciones IPv4 son de 4 bloques de 8 bits, así que separando de la ristra de 0's y 1's anterior en trozos de 8 bits nos resulta 11000000 = 192, 00000000 = 0, 00000010 = 2 y 10000000 = 128.

Las direcciones IPv6 se escriben, al igual que las direcciones IPv4, en notación CIDR. Por ejemplo la red 2000:ac8:1234::/48 comienza con en la dirección 2000:0ac8:1234:0000:0000:0000:0000:0001, cuya dirección de red es 2000:0ac8:1234:0000:0000:0000:0000:0000 y finaliza en 2000:0ac8:1234:ffff:ffff:ffff:ffff:ffff. Un grupo de direcciones /48 contiene $2^{128} - 2^{48} = 2^{80}$ direcciones.

El scope (ámbito), comentado en la cabecera, determina las partes en las que la dirección es válida, por ejemplo, las direcciones de enlace local y la dirección de loopback tienen un ámbito de enlace local, el resto de direcciones excepto las privadas tienen un ámbito global, es decir, son enrutables globalmente.

Los ámbitos definidos son:

Valor	Ámbito (*scope*)	Descripción
0x0	*reserved*	
0x1	interface-local	El ámbito *interface-local* abarca sólo un único interfaz de un nodo, y es útil sólo para la transmisión loopback del tráfico multicast.
0x2	link-local	Los ámbitos de *enlace-local* y *site-local* abarcan las mismas regiones que los ámbitos unicast correspondientes.
0x4	admin-local	El ámbito *admin-local* es el más pequeño que debe ser configurado manualmente, es decir, no deriva automáticamente de la conexión física sin relación alguna con multicast.
0x5	site-local	Los ámbitos de *enlace-local* y *site-local* abarcan las mismas regiones que los ámbitos unicast correspondientes.
0x8	organization-local	El ámbito de *organization-local* abarca multiples ubicaciones que pertenecen a la misma organización.
0xe	global	
0xf	*reserved*	

Figura 2.2.1. Ámbito de direcciones multicast IPv6

Las 128 direcciones más altas de cada subred /64 están reservadas como direcciones anycast, contienen los primeros 57 bits a 1 seguidos de 7 bits de identificador anycast.

Además, existen en IPv6 direcciones con un significado especial, las cuales se comentan a continuación:

- Direcciones Unicast:
  - Dirección indefinida.
    ::/128. Similar a la dirección 0.0.0.0 en IPv4.

  - Ruta por defecto.
    ::/0. Ruta por de defecto para tráfico unicast, correspondiente a la ruta 0.0.0.0/0 de IPv4.

- Direcciones locales.
  ::1/128. Dirección loopback.

  fe80::/10. Dirección de prefijo enlace-local utilizable y única solo en la red local. Dentro de este rango de enlace local solo se utiliza una subred dando lugar a un formato eficaz fe80::/64. Estas direcciones son requeridas en todos los interfaces con IPv6 habilitado, son comparables a las direcciones 169.254.0.0/15 auto-configurables de IPv4.

- Dirección local única.
  fc00::/7. Utilizadas en comunicaciones locales y enrutables solo dentro de un ámbito cooperativo (similar a los rangos de direcciones privadas 10/8, 172.16/12 y 192.168/16 en IPv4). Aunque el uso de estas direcciones está restringido y es local se usan en ámbito global y se espera que no se repitan en todo el mundo.

- Transición de IPv4.
  ::ffff:0:0/96. Con este prefijo se designa una dirección IPv6 mapeada en IPv4, permite el funcionamiento de protocolos de transporte IPv4 en IPv6. Las aplicaciones servidoras abren un socket que escucha para aceptar peticiones de conexión de clientes que usan IPv6 o IPv4, por otra lado, los clientes IPv6 se gestionan de modo nativo y los clientes IPv4 aparecen como clientes IPv6 pero con una dirección IPv6 mapeada en IPv4.

  ::ffff:0:0:0/96. Reservado para direcciones IPv4 traducidas utilizadas por el protocolo Stateless IP/ICMP Translation.

  64:ff9b::/96. Utilizado para traducciones automáticas IPv4/IPv6.

  2002::/16. Se utiliza para el direccionamiento de IPv6 a IPv4, se utiliza además una dirección de la red IPv4 192.88.99.0/24.

- Direcciones de uso especial.

  La IANA ha reservado un bloque de direcciones llamado Sub-TLA ID que son 64 prefijos de red desde 2001:0000::/29 hasta 2001:01f8::/29, asignando los bloques en tres partes:

  - 2001::/32. Utilizado por el protocolo de túneles Teredo (también usado como mecanismo de transición IPv6).
  - 2001:2::/48. Asignado a Benchmarking Methodology Working Group (BMWG) para realizar comparativas y test en IPv6 (similar a la red 198.18.0.0/15 de IPv4).
  - 2001:10::/28. ORCHID (Overlay Routable Cryptographic Hash Identifiers) son direcciones IPv6 no enrutables que se utilizan para identificadores criptográficos de Hash.

- Documentación.

  2001:db8::/32. Es un prefijo reservado para documentación. Estas direcciones se deben usar siempre que se quiera escribir un ejemplo de dirección IPv6 o se creen modelos de red (similar a las redes 192.0.2.0/24, 198.51.100.0/24 y 203.0.113.0/24 en IPv4).

- Direcciones Multicast:

Las direcciones multicast ff00::0/12 están reservadas y no se deben utilizar para ningún grupo multicast. A continuación, en la figura 2.2.2, se muestra una lista con algunas de las más usuales:

Dirección	Descripción	Ámbitos disponibles
`ff0x::1`	Dirección *all-nodes* (todos los nodos). Identifica al grupo de todos los nodos IPv6	Disponible en el ámbito (*scope*) 1 (*interface-local*) y 2 (*link-local*): • `ff01::1` → Todos los nodos en el interface local • `ff02::1` → Todos los nodos en el enlace local
`ff0x::2`	Dirección *all-routers* (todos los routers). Identifica al grupo de todos los routers IPv6	Disponible en el ámbito (*scope*) 1 (*interface-local*), 2 (*link-local*) y 5 (*site-local*): • `ff01::2` → Todos los routers en el interface local • `ff02::2` → Todos los routers en el enlace local • `ff05::2` → Todos los routers en el site-local
`ff02::5`	OSPFIGP	2 (enlace-local)
`ff02::6`	OSPFIGP Designated Routers	2 (enlace-local)
`ff02::9`	Routers RIP	2 (enlace-local)
`ff02::a`	Routers EIGRP	2 (enlace-local)
`ff02::d`	Todos los routers PIM	2 (enlace-local)
`ff0x::fb`	mDNSv6	Disponible en todos los ámbitos
`ff0x::101`	Todos los servidores de NTP (*Network Time Protocol*)	Disponible en todos los ámbitos
`ff02::1:1`	Link Name	2 (enlace-local)
`ff02::1:2`	All-dhcp-agents	2 (enlace-local)
`ff02::1:3`	Link-local Multicast Name Resolution	2 (enlace-local)
`ff05::1:3`	All-dhcp-servers	5 (site-local)
`FF02::1:FF00:0000/104`	Dirección *Solicited-Node*. Véase explicación más abajo	2 (enlace-local)
`FF02:0:0:0:0:2:FF00::/104`	Node Information Queries	2 (enlace-local)

Figura 2.2.2. Direcciones multicast reservadas.

- Dirección multicast solicited-node.
  En una dirección solicited-node los 24 bits menos significativos del ID de grupo se rellenan con los 24 bits menos significativos de la dirección unicast o anycast. Este tipo de direcciones permiten la resolución de la dirección de red por medio de NDP (*Neighbor Discovery Protocol*) en la red sin necesidad de molestar a todos los hosts conectados (como ocurría con ARP en IPv4). Por último, añadir que un host debe unirse a un grupo multicast solicited-node para cada una de las direcciones unicast o anycast.

Para finalizar con el repaso a IPv6 queda añadir que existen direcciones de configuración automática sin estado, en las que, aunque se tenga una dirección configurada manualmente o asignada por DHCPv6, un nodo crea una dirección de enlace-local en cada interfaz con IPv6 habilitado. Esta dirección tendrá el prefijo fe80::/64.

Capítulo 3

3. Situación actual

3.1. Introducción

En este capítulo se va a suponer una hipótesis de red de una PyME. De este modo se puede tener una base sobre la que evolucionar, proponer mejoras y soluciones, ya que se necesita saber con qué elementos iniciales cuenta la red actual. Por otra parte, se debe conocer la oferta de los operadores para empresas y con ello poder aportar una solución alternativa basada en bajo coste.

3.2. Contexto

Partiendo de que la red actual de una PyME es muy parecida a la red doméstica común, esto es, se tiene contratado un acceso básico con un ISP y un router neutro al que se conectan todos los equipos, estando éstos en la misma red.

Dicho esto, se supone que la red que se utiliza en una PyME en la actualidad será como la de la figura 3.2.1; en la que el router proporciona direcciones IP mediante DHCP a los diferentes dispositivos que se conecten, no se dispone de seguridad adicional al antivirus de cada equipo, no se controla el acceso a sitios web ni a los diferentes equipos de la red y no se monitoriza el uso de la red.

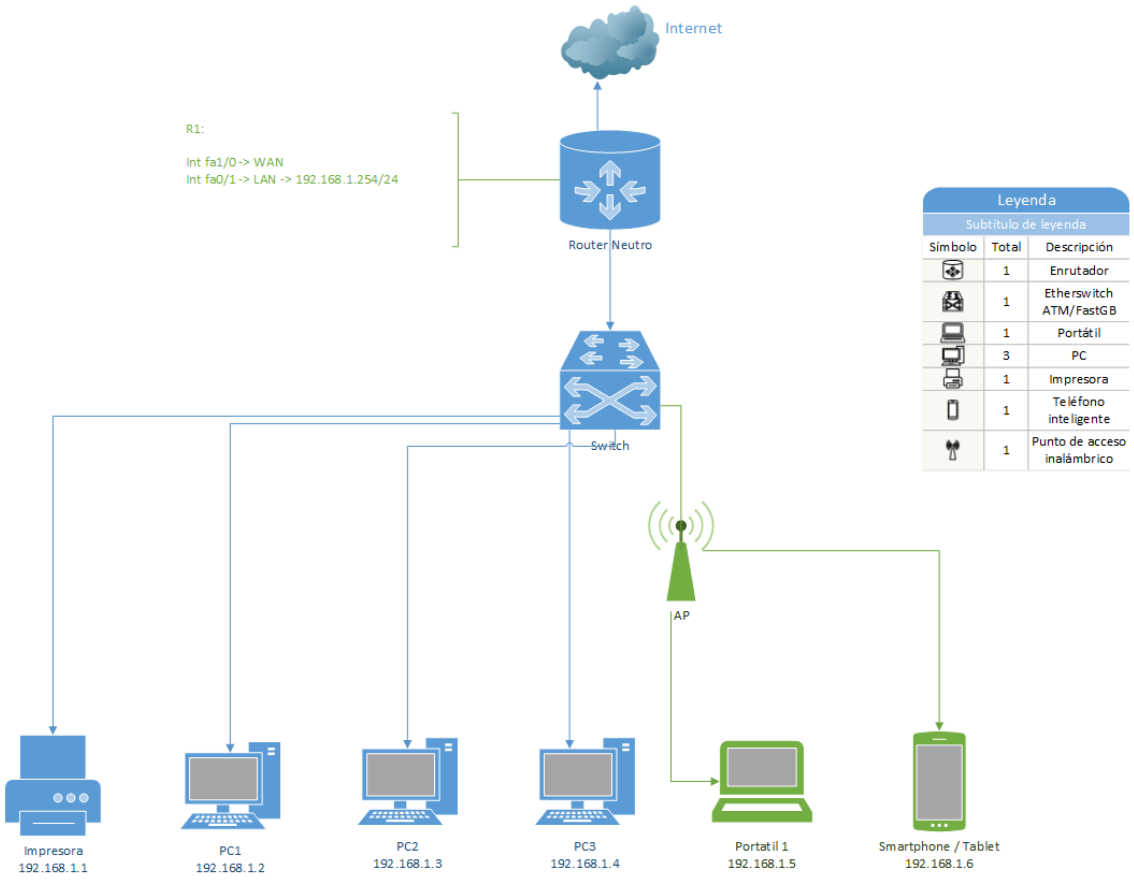


Figura 3.2.1. Ejemplo de suposición de la red actual de una PyME.

3.3. Ofertas de las principales operadoras para las PyMEs

En este punto se analiza qué ofrecen en la actualidad los principales operadores de Telecomunicaciones a las empresas, enunciando qué servicios, velocidades de acceso y equipos aportan.

Dicho esto, se van a tener en cuenta los proveedores de servicios más relevantes, como son Telefónica, ONO y Vodafone.

Cabe añadir que en la documentación adjunta a este trabajo se aportan los manuales de configuración que proporcionan los operadores mencionados. Además, se debe mencionar que es difícil de encontrar y que aporta información muy básica.

Telefónica

Ofrece en versiones ADSL (hasta 10/1 Mb) y Fibra (100/10 Mb) las mismas ofertas que para usuarios domésticos, además incluye espacio web y correo.

Para encontrar ofertas con buenos servicios hay que buscar en la sección de ofertas para "Grandes Empresas". Estos servicios aportan seguridad (MPLS), cloud computing, VPN IP (MacroLan) y comunicación máquina a máquina.

Se encuentra en este caso que es la misma oferta que para usuarios domésticos de fibra FTTH a 100/10 Mb, pero se abonan los servicios extras de empresa por separado.

Respecto a los equipos que proporciona Telefónica para las distintas conexiones, se puede apreciar que no aportan nada óptimo para la red de una empresa, siendo también unas características limitadas para usuarios exigentes.

En concreto, para la opción de ADSL ofrecen un Zyxel P2302HWDLP1 y para la opción FTTH un Huawei Echolife HG520V, notando que en la opción de fibra el router tiene puertos 10/100, desaprovechando la velocidad dada por la fibra y haciendo que esto no sea lo mejor.

ONO

Este operador ofrece los mismos servicios que para usuarios domésticos, pero añadiendo una opción de hasta 500Mb, además de los servicios:

- Microsoft Office 365
- Office Small Business Premium
- Correo
- Gestión de tiendas

- Iliwallet
- Centralita virtual
- Secretaria virtual
- Almacenamiento en nube
- Gestión de punto de venta
- Creador de páginas web
- Seguridad
- Audio conferencia

En cuanto al equipo físico en sí, proporciona un router Compal CH6640E/CG6640E o un Hitron CDE-30364 a empresas.

Vodafone

Por último, esta empresa ofrece conexiones de hasta 100 Mb y sí ofrece un router con puertos Gigabit (10/100/1000), favoreciendo en este caso el aprovechamiento de la velocidad dada por la conexión.

Ofrece los servicios:

- Microsoft Office 365
- Centralita virtual
- Disco en red
- Comunicación máquina a máquina (M2M).

Los equipos proporcionados por Vodafone son Huawei HG556a y Huawei HG253s V2, este último cuenta con interfaces Gigabit Ethernet.

En resumen, los operadores ofrecen equipos muy parecidos para servicios casi idénticos. Los routers que ofrecen no son las mejores opciones para empresas, tanto en servicios, capacidad, ni velocidad, ya que son equipos que tienen las funcionalidades básicas para hogares que cualquier router comercial tiene, como son: Firewall, Wireless, cuatro puertos Ethernet a 10/100 Mb y DMZ. Incluso routers neutros de otras marcas ofrecen mejores servicios que estos, aunque no por bajos precios.

Cabe añadir que es complicado encontrar información de los equipos que ofrecen los operadores, requiriendo búsqueda exhaustiva debido a que los operadores no proporcionan fácilmente el manual del equipo con sus especificaciones. Solamente proporcionan manuales muy básicos para usuarios, en los que aparecen configuraciones mínimas.

Capítulo 4

4. Entorno de trabajo

4.1. Introducción

En este capítulo se escribe sobre la red que se encuentra en una PyME y las mejoras que se puedan implementar para optimizarla. También se comenta qué pruebas se han realizado en el laboratorio y con qué equipos, explicando las maquetas y configuraciones utilizadas.

4.2. Entorno en la PYME

Como se comentaba en el capítulo 3 sobre la situación actual de una PyME, éstas parten de una situación con pocos medios económicos, se podrían considerar como redes "caseras", con pocos servicios y poco optimizadas. Además, como se ha visto en el mismo capítulo, los operadores no ofrecen gran variedad de servicios.

Por esto, en este trabajo propone una red que al menos disponga de los elementos que se comentan a continuación. Estos elementos se suponen mínimos en una red que sea óptima y aporte variedad de servicios y seguridad.

Partiendo de que una PyME necesita:

- **Firewall** para controlar el acceso a determinados contenidos y evitar ataques desde el exterior que supongan problemas a la empresa o comprometan la información de la misma.
- **Servidor DHCP** para proporcionar direcciones IP dinámicamente a los equipos. Así el uso de la red y la configuración de equipos será más cómoda para el empresario y los empleados.
- **Servidor DNS** local para proporcionar una salida rápida a Internet y mejorar el tráfico.

- **Servidor LDAP y/o RADIUS** para obtener seguridad internamente, por ejemplo, separando privilegios de acceso con LDAP o proporcionando claves de visitante para acceder a la conexión WiFi mediante un servidor RADIUS.
- Configurar **VLAN** con el fin de separar flujos de tráfico en la red interna. Así se evitan accesos indeseados de empleados y visitantes a zonas privadas o protegidas.
- **Servidor HTTP** (si dispone de web) para proporcionar hosting al sitio web de la empresa localmente. Esto también puede ocasionar problemas de tráfico en la red de la empresa o que la web no esté disponible por cortes de suministro eléctrico por ejemplo. Debido a estos problemas no es recomendable.
- **Servidor SMTP** para proveer correo a la empresa.
- **Servidor de Backup** con el fin de realizar copias de seguridad periódicas y evitar pérdidas de datos.
- **Monitor y gestor de red** (la información quedará en local o se enviará a un responsable). Para poder controlar la red y advertir sobre problemas de seguridad o fallos en la misma, y solventarlos con la mayor rapidez evitando que den lugar a problemas mayores.
- **Servicio de VoIP** para proveer telefonía en toda la empresa.
- **Puntos de acceso WiFi** para proporcionar conexión inalámbrica a visitantes o a los empleados en dispositivos móviles y favorecer la movilidad de los mismos en la empresa.

Se intenta conseguir una red que al menos disponga de los elementos comentados anteriormente. Estos elementos se suponen mínimos en una red que sea óptima y aporte variedad de servicios y sea segura.

Aplicando configuraciones y virtualización se pretende obtener una red completa como la mostrada en la figura 4.2.1.

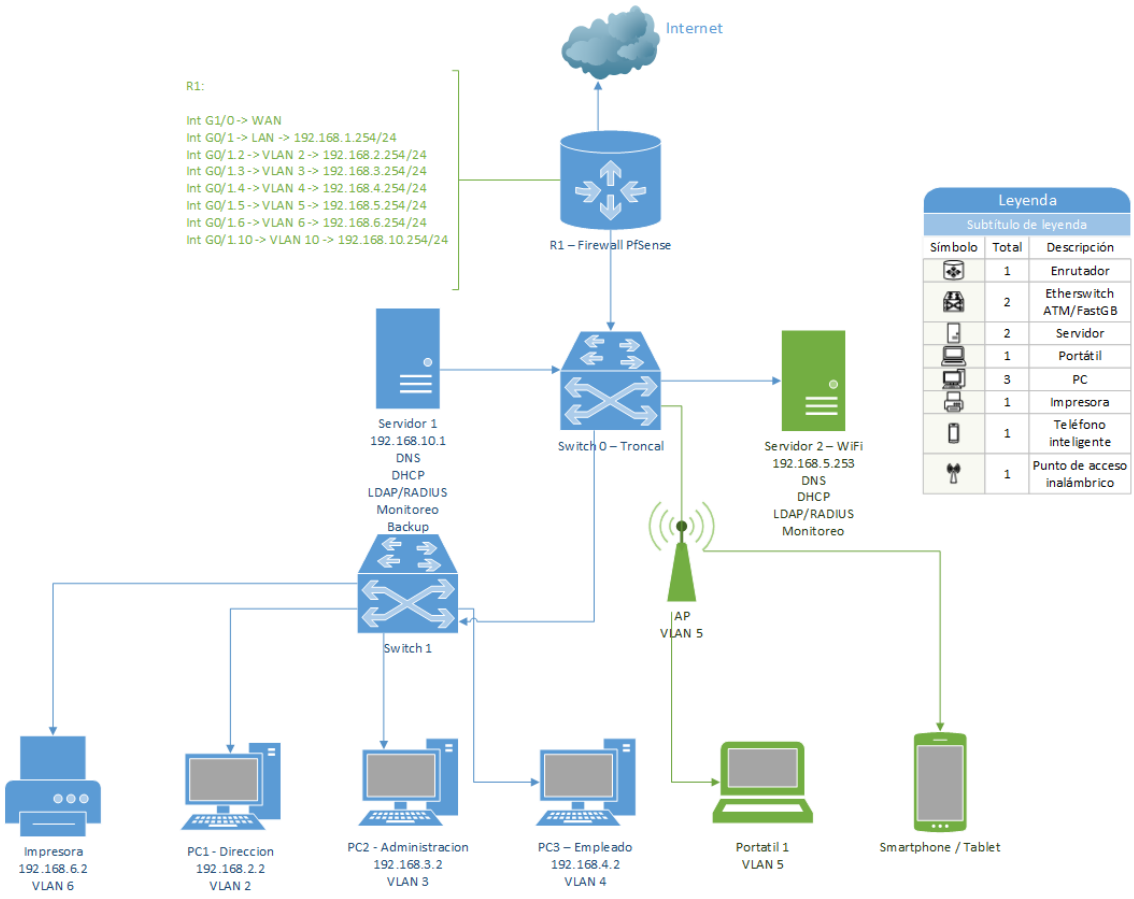


Figura 4.2.1. Maqueta de red mínima de una PyME.

Como se puede apreciar en la figura 4.2.1, la red mostrada está segmentada en VLAN por departamentos o servicios, estando los servidores en otra VLAN, al igual que los equipos de cada departamento, las impresoras y el acceso inalámbrico.

Los servidores, tanto para la red WiFi como para la red cableada, se pueden virtualizar abaratando costes, y separándolos para evitar sobrecargas.

4.3. Pruebas en laboratorio

En esta sección se van a presentar los equipos utilizados en las pruebas de laboratorio (dos switches, un punto de acceso y varios ordenadores) y posteriormente las pruebas realizadas.

4.3.1- Equipos

En el desarrollo de este trabajo se han usado los dispositivos que se comentarán a continuación, además de sus características. Los manuales de los switches utilizados se adjuntan a la documentación de este trabajo.

Para las pruebas se han usado los dos tipos de switches siguientes, habiendo comprobado el funcionamiento de los protocolos que implementan.

Switch D-Link DES-3200-10

Figura 4.3.1.1. D-Link DES-3200-10

Especificaciones:

- 8 puertos 10/100BASE-TX.
- 1 puerto 100/1000SPF.
- 1 puerto10/100/1000BASE-T/100/1000SPF.

- Tabla de direcciones MAC de 16 K.
- Capacidad de 5.6 Gbps.
- Ratio de reenvío de paquetes de 64 Bytes de 4.2 Mpps.
- Buffer de paquetes de 1.5 MB.
- Switch L2/L3.
- Soportan IPv6.

Switch D-Link DGS-3200-10

Figura 4.3.1.2. D-Link DGS-3200-10

Especificaciones:

- 8 puertos 10/100/1000BASE-TX.
- 2 puertos 1000BASE-T/SPF.
- 1 puerto RS-232 para consola.
- Tabla de direcciones MAC de 8 K.
- Capacidad de 20 Gbps.
- Ratio de reenvío de paquetes de 64 Bytes de 14.88 Mpps.
- Buffer de paquetes de 128 Kbytes.
- Switch L2/L3.
- Soportan IPv6.

Punto de acceso Tp-Link TL-WA5110G

Figura 4.3.1.3. Tp-Link TL-WA5110G

Especificaciones:

- 1 puerto 10/100 con PoE.
- Soporta los estándares IEEE 802.11b/g.
- Antena desmontable de 4 dBi.
- Frecuencia 2.4 - 2.4835 GHz.
- Encriptación WEP de 64/128/152 WPA/WPA2/WPA-PSK/WPA2-PSK (AES / TKIP)
- Servidor DHCP.
- Multi SSID.
- Modos AP / Cliente / WDS Bridge / Repetidor.

Además, para las pruebas realizadas se utilizaron 6 PCs virtualizados en 2 ordenadores, 3 máquinas virtuales en cada uno. Estos PC virtualizados tenían sistema operativo Linux. Como se va a poder comprobar a continuación no se necesitan equipos muy potentes para virtualizar servidores.

La máquina donde se virtualizaban era un ordenador con CPU Core 2 Duo a 2.2 GHz y 2 GB de RAM.

El router CISCO se emuló en un PC como el anterior, pero con el sistema operativo Windows XP.

El router PfSense se emuló sobre Debian en un PC con 4 GB de RAM y un Core 2 Duo a 3 GHz.

Por último, para monitorizar y configurar los equipos se usaba un portátil con un Core 2 Duo a 1.6 GHz y 4 GB de RAM.

4.3.2- Pruebas

En este punto se comentan algunas de las pruebas que se llevaron a cabo en el laboratorio para comprobar la viabilidad de la emulación de router y su funcionamiento. En todas las pruebas se usó el router CISCO emulado con la versión del IOS c7200-p-mz.122-2.T4.

En cuanto al enrutador, se probaron las opciones de virtualizar sobre Debian un software libre como es PfSense y por otra parte emular en Windows 7 o XP un router CISCO mediante el uso de imágenes IOS de libre distribución.

En esta parte, a la hora de virtualizar PfSense hay que tener especial cuidado, ya que si se instala directamente en el disco duro utiliza todo el espacio en disco, por tanto, es mejor opción virtualizar una máquina con Debian, dando el espacio que se comenta en el Anexo de instalación de esta parte. Por otro lado, a la hora de emular una IOS CISCO no se han encontrado problemas a la hora de instalarlo y configurarlo, pero hay que tener en cuenta que es difícil encontrar en Internet imágenes IOS y las que se encuentran, al ser distribuidas gratuitamente y para estudio, tienen el ancho de banda limitado a 2 Mb.

La funcionalidad del enrutador se comprueba sobre la maqueta de la figura 4.3.2.1, sobre la que se realiza la configuración que se comenta a continuación.

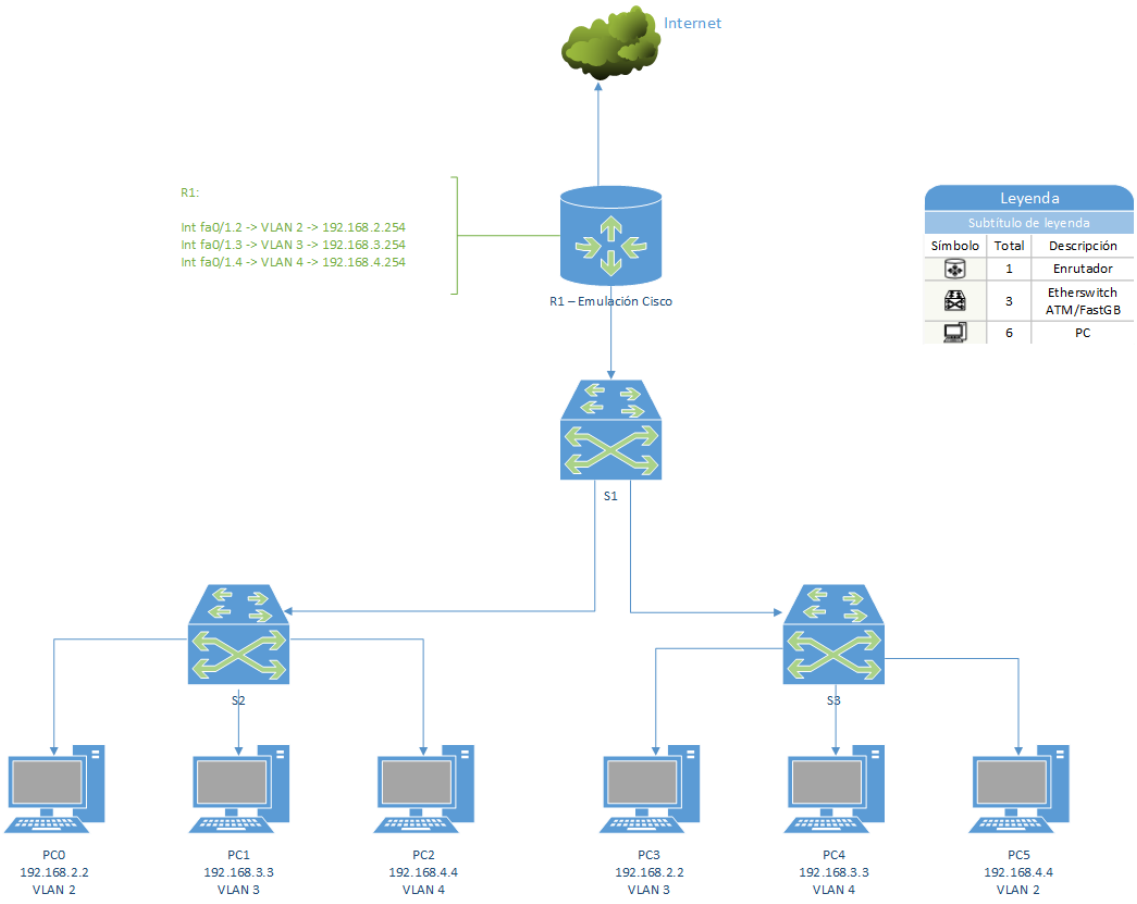


Figura 4.3.2.1. Maqueta de comprobación del funcionamiento del enrutador.

Para comprobar el funcionamiento del router emulado con la imagen IOS se configuraron ACL, VLAN y NAT. En la figura 4.3.2.2 se muestra dicha configuración.

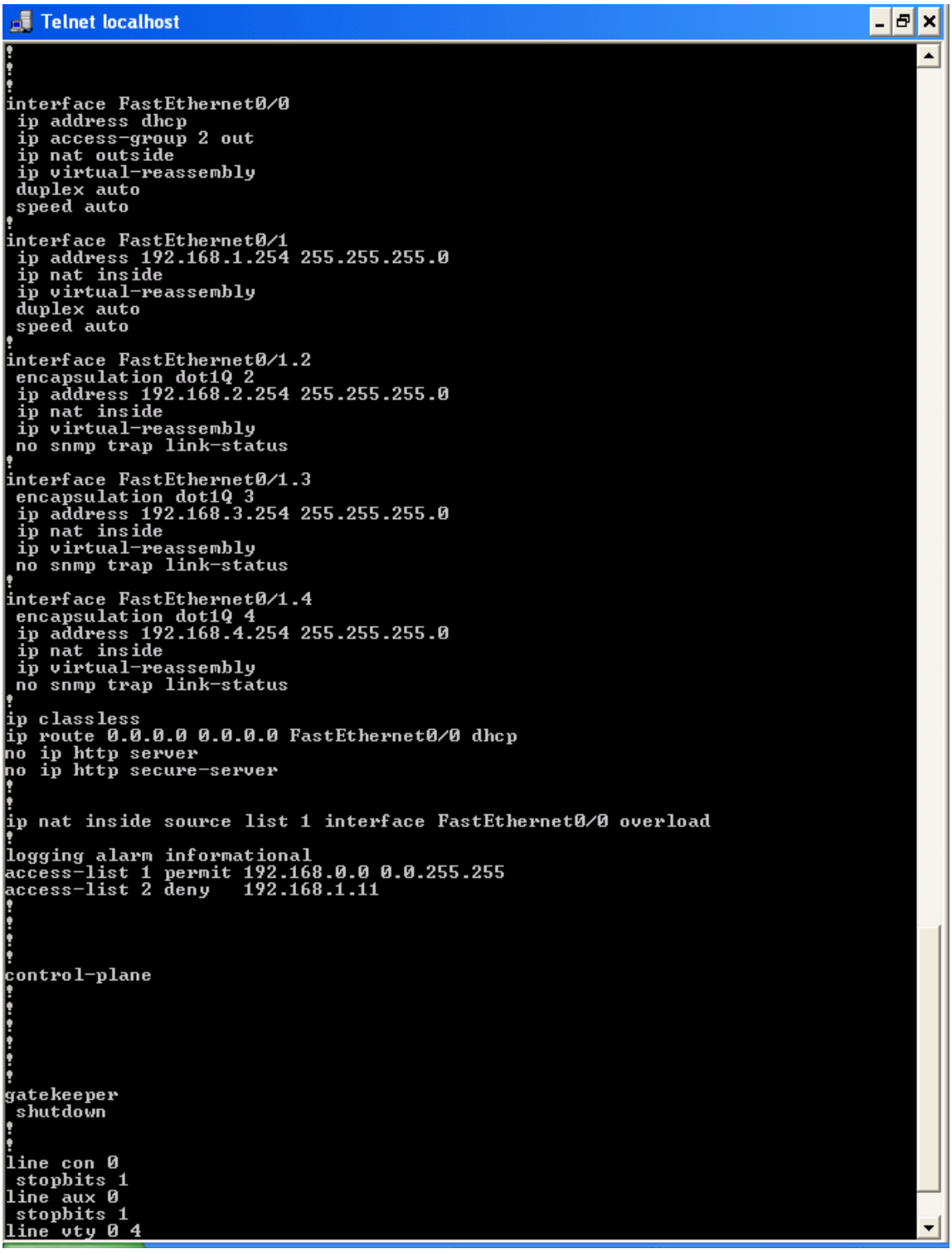


Figura 4.3.2.2. Configuración router CISCO emulado.

En la figura 4.3.2.3 se comprueba que el NAT funciona, dando salida hacia Google.

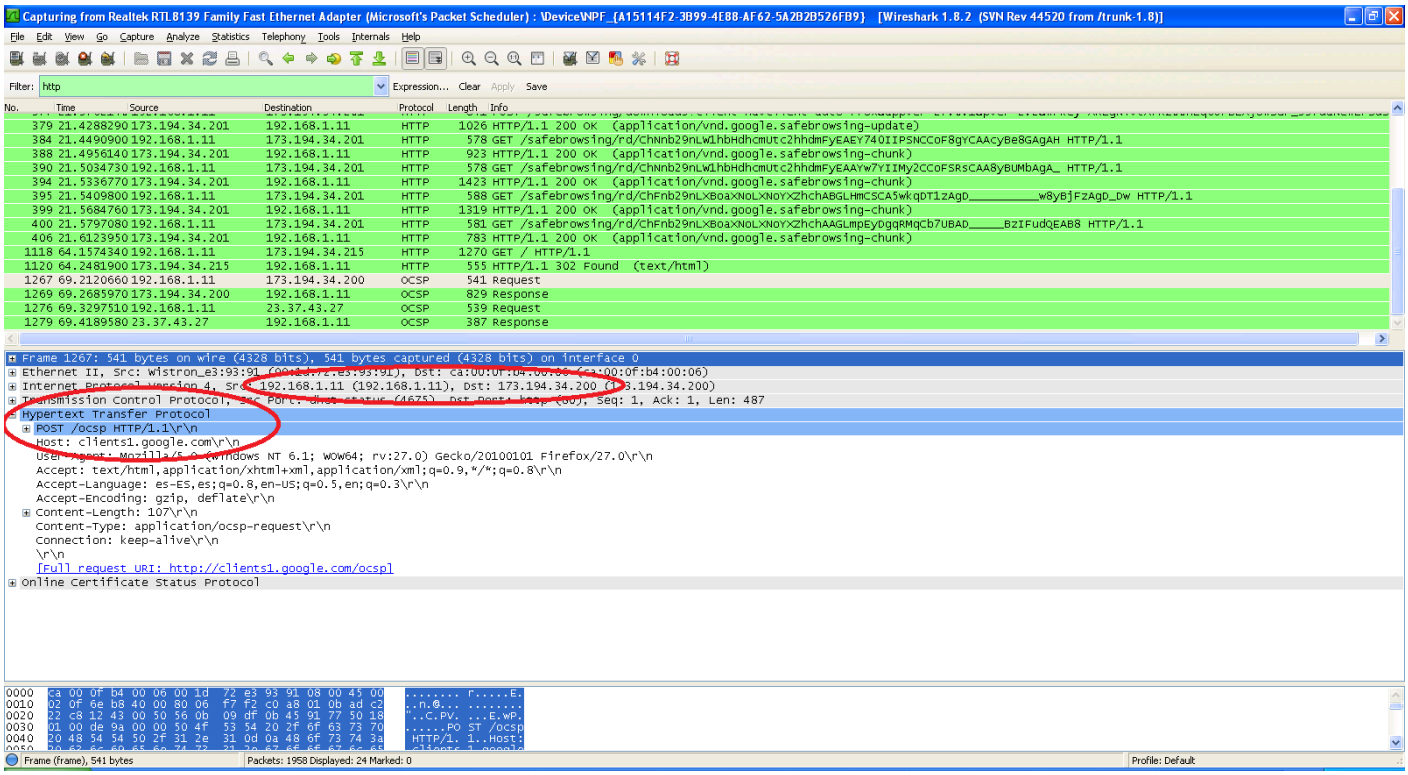


Figura 4.3.2.3. Captura de tráfico con salida a Google.

En la figura 4.3.2.4 se comprueba el funcionamiento de las ACL, certificando que se deniega.

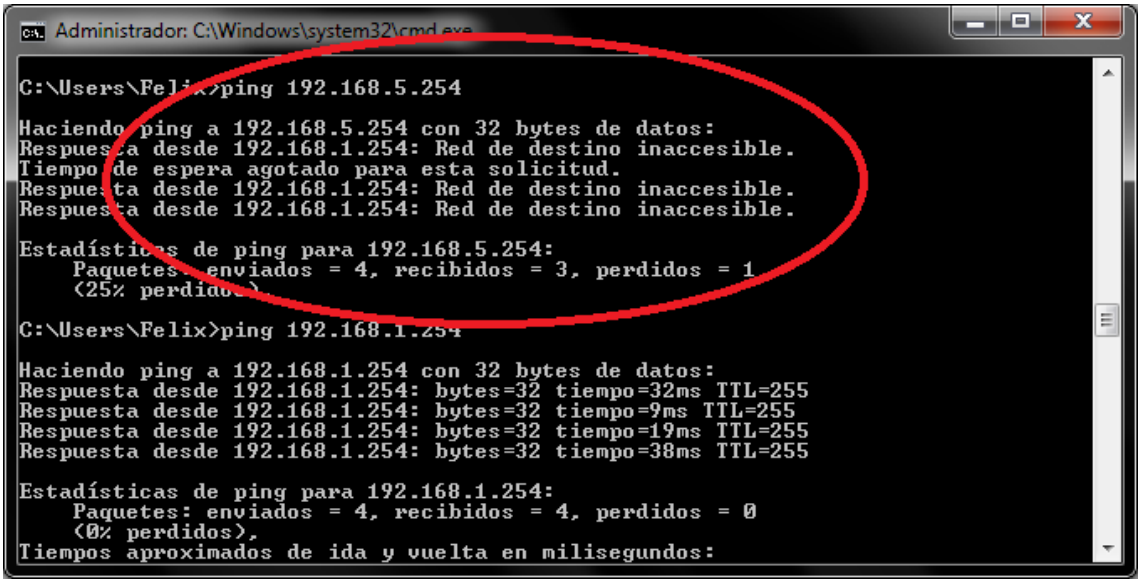


Figura 4.3.2.4. Ping denegado por ACL.

Respecto a los monitores y gestores de red probados (Cacti, Nagios y OpenNMS) cabe destacar que el equipo donde está instalada la emulación de router CISCO es Windows XP, en el que no se consigue que ninguno de los mencionados softwares de monitoreo reconozcan los host, solo reconocen la interfaz del router. Las pruebas que se han hecho han sido con un portátil con Windows 7, donde sí se reconocen los host.

Probado también con Nagios y Cacti, donde encontramos que estos no funcionan en Windows XP al tener una versión antigua de PHP.

Por último, se ha probado con OpenNMS, notando que funciona tanto en Windows XP como en Windows 7.

En la figura 4.3.2.5 se muestra una captura de tráfico sobre el enlace Trunk entre ambos switches, en la que se observan los bits de entrada/salida.

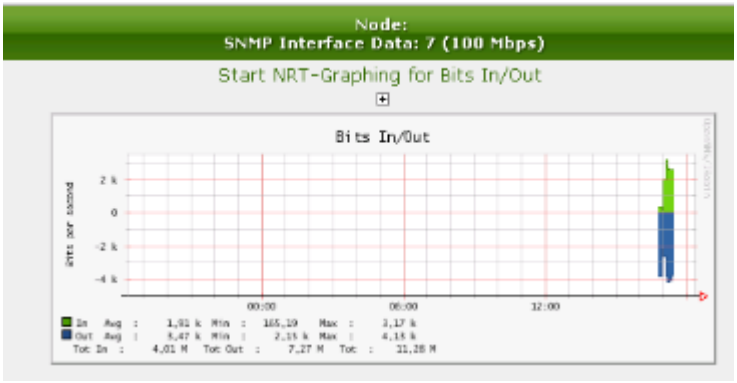


Figura 4.3.2.5. Tráfico sobre el enlace Trunk.

En la figura 4.3.2.6 se aprecia el tráfico del portátil capturado mediante OpenNMS.

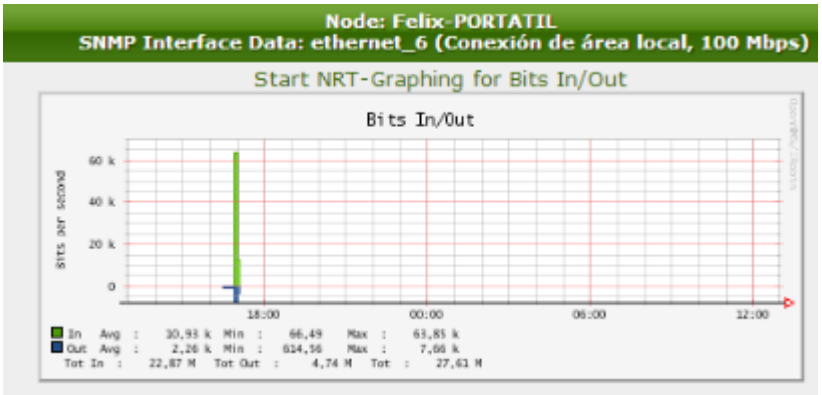


Figura 4.3.2.6. Tráfico capturado con OpenNMS.

A continuación se explican las pruebas realizadas y las conclusiones sacadas de las mismas. Estas pruebas listadas son las siguientes:

- Pruebas de streaming de audio.
- Maqueta completa con pruebas de protocolos.
- VLAN Asimétricas.

4.3.2.1- Prueba de streaming de audio

Una de las pruebas que se realizaron fue comprobar cómo mejorar la calidad de conversaciones sobre VoIP mediante una comunicación en streaming de audio entre equipos en la misma red, aplicando diferentes configuraciones de red. Las pruebas se realizaron sobre la maqueta mostrada en la figura 4.3.2.1.1:

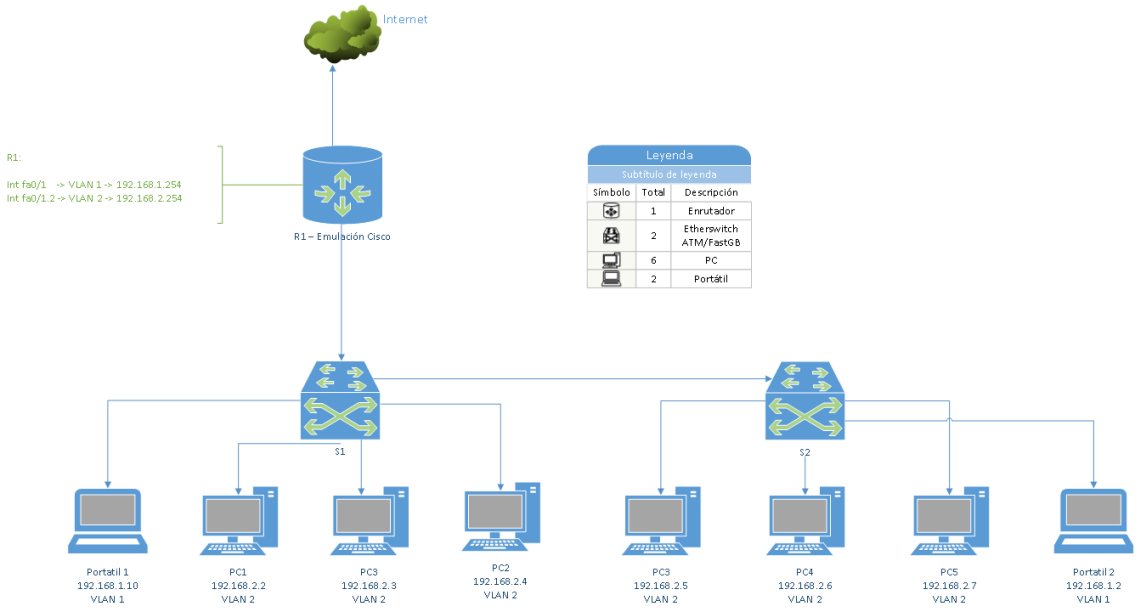


Figura 4.3.2.1.1. Maqueta de prueba con streaming de audio.

Se establecerá la comunicación en streaming entre ambos portátiles. El resto de equipos se encontrarán con las diferentes configuraciones desglosadas a continuación:

Misma red, sin QoS.

a. Con tráfico multicast.

   Se puede comprobar que el streaming empeora al estar enviando tráfico multicast el resto de equipos.

b. Sin tráfico multicast.

   En este caso la calidad del sonido es buena, no se percibe ningún problema ya que ningún equipo está generando tráfico.

Misma red, con QoS.

En este caso se ha dado máxima prioridad al puerto de enlace entre switches y a los puertos de los equipos que hacen streaming. Los puertos del resto de equipos están con prioridad estándar y con un ancho de banda máximo de 1024 kbps.

a. Con tráfico multicast.
b. Sin tráfico multicast.

   Al aplicar QoS no se aprecia ninguna diferencia entre introducir tráfico multicast y hacerlo sin dicho tráfico, el sonido es mejor que en el primer caso.

VLAN, sin QoS.

Se han separado en dos VLAN ambos flujos de tráfico, una VLAN para los equipos que hacen streaming y otra para los demás (los que generan tráfico multicast).

Para esta prueba se han dejado las prioridades de todos los puertos por defecto (nivel 0) y se han desactivado todas las opciones de QoS.

a. Con tráfico multicast.
b. Sin tráfico multicast.

   Se ha podido comprobar en este caso que al estar el flujo de tráfico multicast separado en otra VLAN no interfiere en el streaming y se escucha perfectamente, como en la prueba 2.

VLAN, con QoS.

Se ha separado en dos VLAN ambos flujos de tráfico, una VLAN para los equipos que hacen streaming y otra para los demás (los que generan tráfico multicast).

En este caso se ha dado máxima prioridad al puerto de enlace entre switches y a los puertos de los equipos que hacen streaming, los puertos del resto de equipos están con prioridad estándar y con un ancho de banda máximo de 1024 kbps.

a. Con tráfico multicast.
b. Sin tráfico multicast.

   No se aprecia ninguna diferencia en la calidad del sonido al aplicar o no VLAN con QoS.

Se puede apreciar con estas pruebas que es muy útil y necesario aplicar tanto VLAN como QoS a la red para mejorar el rendimiento. Aplicando VLAN se separan los flujos y se tiene el tráfico confinado, evitando así que el ancho de banda baje demasiado. Por otra parte, al aplicar QoS se da prioridad a los puertos donde se encuentran los flujos streaming haciendo que el audio sea mucho mejor.

Se concluye que al menos se debe aplicar VLAN para mejorar las comunicaciones en general, en especial el streaming de audio, como en este caso.

4.3.2.2- Maqueta completa con pruebas de protocolos

En este punto se van a explicar las pruebas que se realizaron sobre una maqueta en el laboratorio. Se llevaron a cabo con el fin de comprobar en un entorno real el comportamiento de diferentes protocolos. Dichos protocolos son los siguientes:

- **802.1Q.** Protocolo para configurar VLAN.
- **QinQ (802.1ad).** Encapsula etiquetas 802.1Q en otra etiqueta 802.1Q. Usado para agrupar VLAN. Soporta clientes con múltiples VLANs utilizando una

única VLAN para transportar el tráfico de estos clientes. Utilizado por los operadores.

- **802.1v.** Permite al usuario crear grupos de VLAN por protocolo y añadir protocolos al grupo. Soporta múltiples VLANs para cada protocolo y permite configurar puertos untagged o diferentes protocolos en el mismo puerto físico.
- **802.1p.** Permite aplicar prioridades por puerto.
- **STP.** *Spanning-Tree Protocol*, gestiona la presencia de bucles en la red debido a enlaces redundantes, eliminando dichos bucles.
- **LACP.** Agregación de puertos, agrupa varios puertos en uno para aumentar el ancho de banda.
- **ERPS.** *Ethernet Ring Protection Switching*, usado para asegurar que no hay bucles en la capa Ethernet
- **LLDP.** Usado por los dispositivos para informar de su capacidad, disponibilidad, identidad y vecinos.
- **BW control.** Limita por puerto el ancho de banda efectivo. Se puede limitar solo TX, solo RX o ambos. Se puede aplicar también a colas.
- **IGMP snooping.** Usado para eliminar tráfico IGMP multicast innecesario. El switch conoce la MAC a la que está conectado cada puerto y envía por éste sólo los paquetes IGMP multicast destinados al mismo.
- **DSCP.** *Differentiated Services Code Point*. Byte de la cabecera IP que sirve para diferenciar la prioridad de los paquetes.

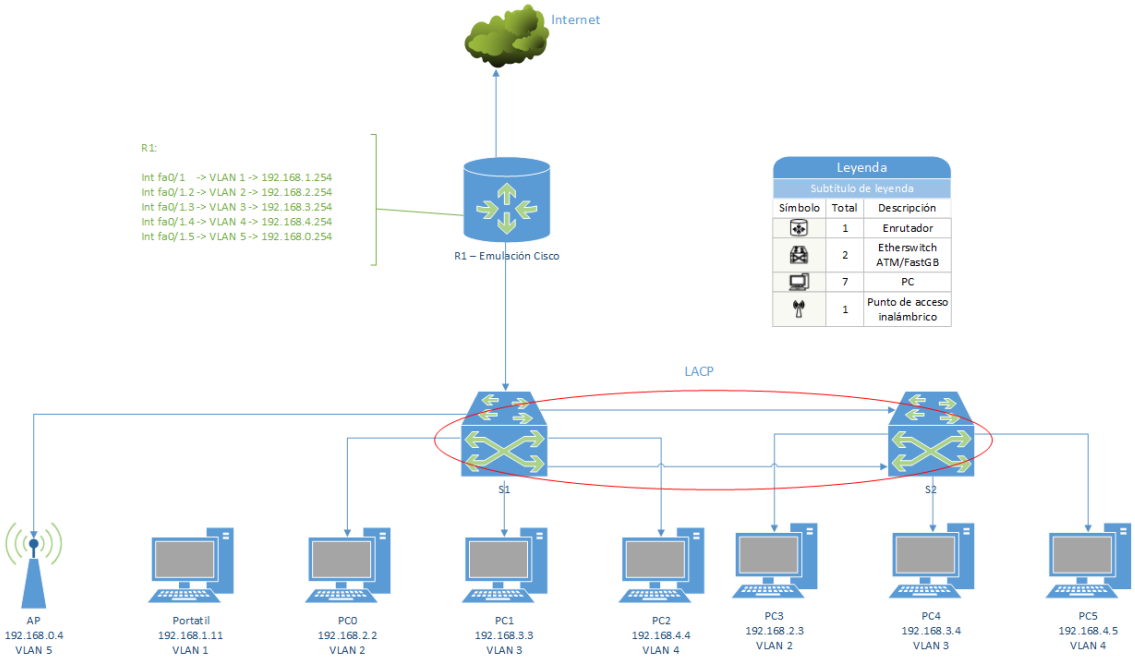


Figura 4.3.2.2.1. Maqueta de aplicación de protocolos.

Los protocolos mencionados anteriormente se aplican en los switches en la maqueta de la figura 4.3.2.2.1.

Tras realizar las pruebas y mediciones oportunas se concluye que:

- El protocolo 802.1v sería útil si hubiese una VLAN para VoIP o streaming de video/audio ya que se confina todo ese tráfico en una red. Además se aplicaría control de ancho de banda y el protocolo 802.1p para dar prioridad y mejorar la QoS de dichos servicios (protocolos RTP, RTSP, RTCP).
- Al hacer LACP y agregar prioridades a puertos, los tiempos de los paquetes ICMP han bajado (de 1.2 ms antes a 0.7 ms después de aplicarlo) y son más constantes.
- Limitando el ancho de banda a la VLAN2 y priorizando el tráfico de la VLAN3 se ve que el tráfico de esta última tiene tiempos más bajos.
- Se debe aplicar control de tráfico: si queremos evitar ataques DDoS.
- Aplicado DSCP a VLAN3, no se aprecia diferencia.
- Probado multiSSID y VLAN en el AP, configurando para ello DHCP en cada interfaz virtual de las VLAN. Se obtiene un SSID para cada IP en el DHCP, asimilándose a VLAN en WiFi.

4.3.2.3- VLAN Asimétricas

En este apartado se pretende aprender acerca de esta configuración, ya que es sencilla y útil. Ésta es una tecnología introducida por D-Link, que posteriormente CISCO y HP implementaron en sus dispositivos.

Los pasos para conseguir esta configuración son los siguientes:

- Crear las VLAN que se necesiten y aplicarlas a los puertos indicados.
- Crear otra VLAN que englobe todos los puertos.
- Configurar el router sin 802.1Q, es decir, sin interfaces virtuales asociadas a una VLAN. Solo configurar una puerta de enlace y todas las redes en la misma red pero con diferentes VLAN.

En la figura 4.3.2.3.1 se muestra un ejemplo de configuración de una red con VLAN Asimétricas.

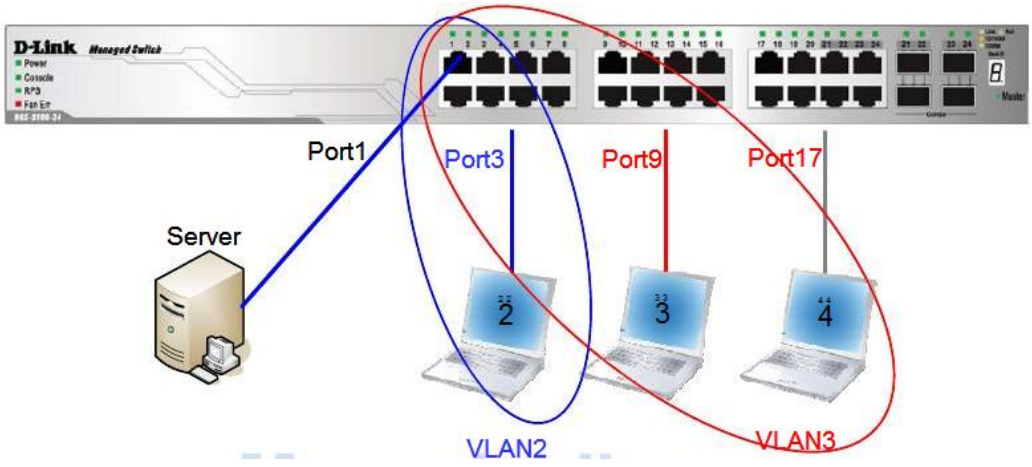


Figura 4.3.2.3.1. Ejemplo de VLAN Asimétrica.

Cabe señalar que los switches D-Link DGS-3200 y DES-3200 del laboratorio no permiten utilizar VLAN asimétricas, ya que solo usan 802.1Q, pero por ejemplo, los switches D-Link DGS-3100 si disponen de esta funcionalidad.

Capítulo 5

5. Soluciones

5.1. Introducción

En este capítulo se explican las soluciones que se pueden aplicar a la mejora de la red de una PyME, contemplando las necesidades y servicios que se consideran mínimos para un óptimo funcionamiento en un entorno empresarial.

Para ello se parte de la hipótesis de la red actual de las PYMES supuesta anteriormente y se asume que disponen de acceso a Internet con cualquier operador. Como se explicó previamente en el capítulo 3, los operadores no aportan servicios relevantes ni equipos óptimos para las PyMEs.

Para solventar el problema del enrutador se propone la utilización de uno que aporte más opciones que los ofrecidos por los operadores. En este trabajo se hace uso para todas las soluciones de PfSense (un software libre basado en Linux) que se virtualizará y se configurará como sea necesario en cada caso, ya sea con IPv4, con IPv6 o con ambas, además de aplicar VLAN, ACL (listas de acceso) y NAT.

A continuación se explica en primer lugar una solución en la que se aplica únicamente IPv4, después una solución en la que se utiliza solamente IPv6 y para finalizar se proponen varias soluciones para la convivencia entre IPv4 e IPv6.

5.2. Solución utilizando únicamente IPv4

Una primera solución sería configurar la red con IPv4 solamente, sin tener en cuenta la adaptación con IPv6.

- Utilizando PfSense como enrutador y configurándole una interfaz WAN que obtenga la dirección IP automáticamente del operador y una interfaz LAN.
- Se configuran interfaces virtuales para poder utilizar las VLAN de cada departamento, con el fin de tenerlos separados pero que se puedan acceder entre ellos y aplicando listas de acceso para evitar accesos no deseados entre departamentos.
- Se virtualizan todos los servidores y se intenta instalar toda virtualización en el menor número de equipos, dependiendo de las interfaces que tengan cada uno.

Resulta la maqueta de la figura 5.2.1:

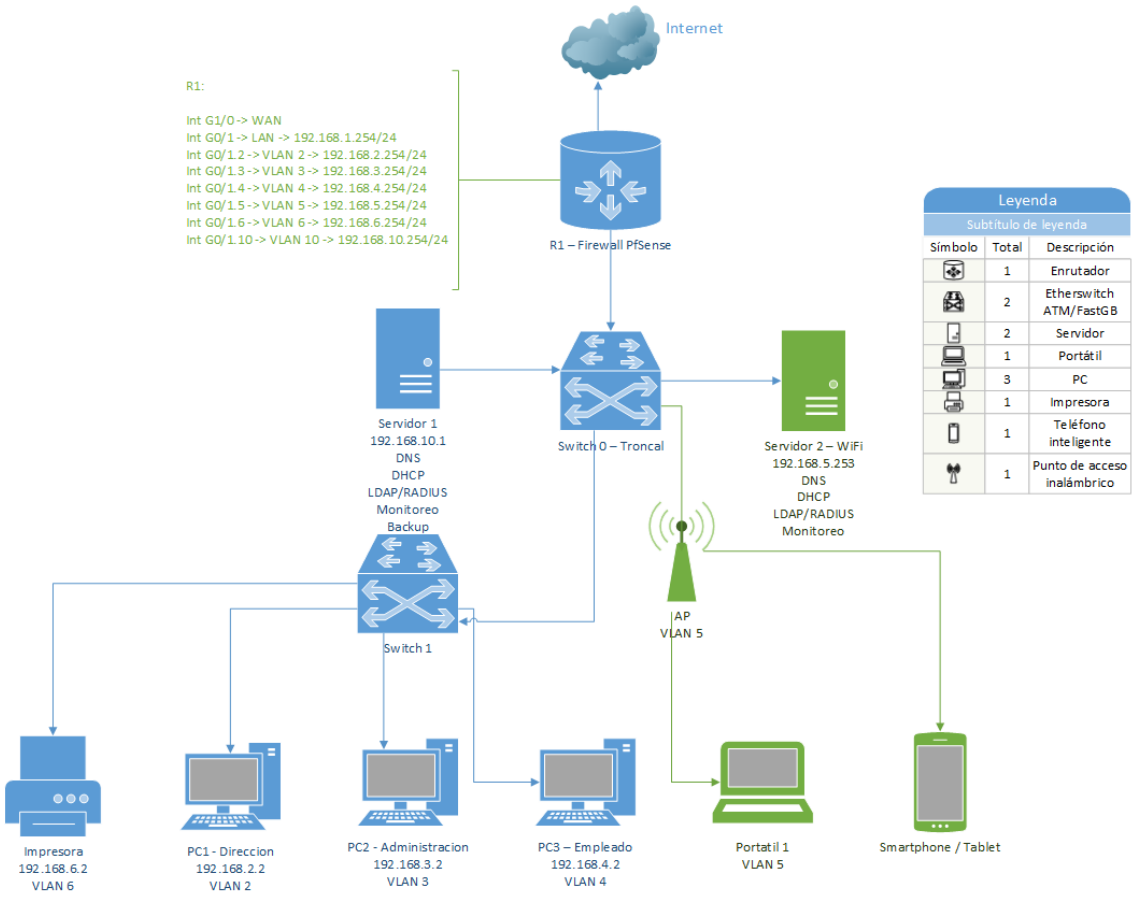


Figura 5.2.1. Maqueta configurada solo con IPv4.

En la red completa de la figura 5.2.1 se pueden ver los servidores 1 y 2 y el router R1 por separado, pero se intentará virtualizar todo en el menor número de equipos. Dependemos del número de interfaces del que disponga cada equipo, teniendo en cuenta que hay placas base que disponen de 2 tarjetas Ethernet a velocidad de 1 Gbps y con ranuras PCI para pinchar tarjetas Ethernet de la misma velocidad, pudiendo tener sin problemas 6 tarjetas Ethernet en un mismo equipo.

El router consumirá dos interfaces, una para WAN y otra para LAN, mientras que el resto de servicios utilizarán una para cada uno.

Se aprecia también en la red que todos los departamentos están separados por VLAN, y con interfaces virtuales, se consigue que puedan acceder todos a la VLAN de impresoras. Implementando listas de acceso se evita que desde un departamento o desde la conexión inalámbrica se pueda acceder al resto de departamentos.

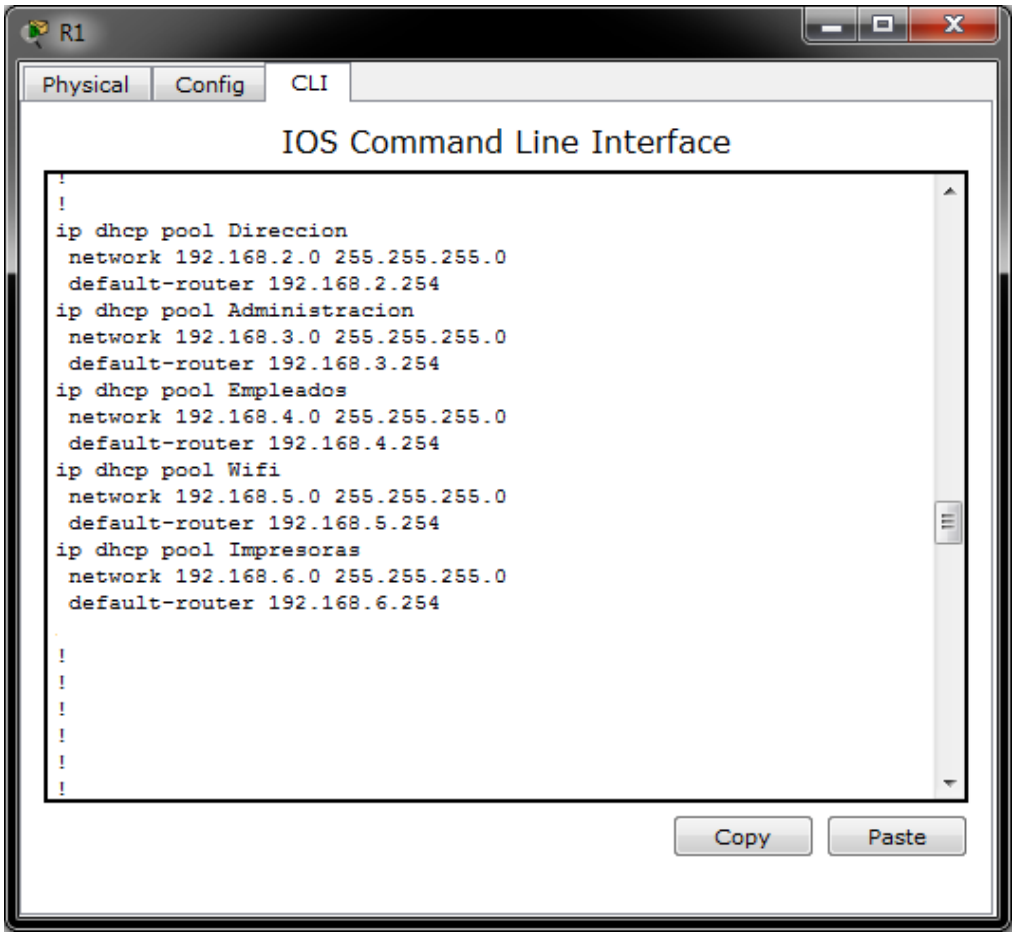


Figura 5.2.2. Configuración DHCP del router.

En la figura 5.2.2 se ve la configuración de un pool de direcciones para cada VLAN, haciendo uso de los siguientes comandos:

Router(config)#ip dhcp pool Direccion

Router(dhcp-config)#network 192.168.2.0 255.255.255.0

Router(dhcp-config)#default-router 192.168.2.254

Con la primera línea de comandos se crea un pool de direcciones DHCP para la VLAN con el nombre "Direccion", creada previamente. En la segunda línea se da una IP de red al pool de direcciones. Y para finalizar, con la última línea se indica la dirección IP del Gateway de ese pool de direcciones.

En la siguiente imagen, la figura 5.2.3, se observan las configuraciones de las interfaces.

- La interfaz WAN del router se configura para que obtenga de manera automática la dirección IP que proporcione el operador.

  Router(config)#int g 0/0
  Router(config-if)#ip address dhcp

- La interfaz LAN se configura con una IP por defecto.

  Router(config)#int g 0/1
  Router(config-if)#ip add 192.168.1.254 255.255.255.0

- Se crean interfaces virtuales, se activan las VLAN con la encapsulación 802.1Q, se le aplica el número de la VLAN que corresponda, se le asigna la IP de Gatewa.y se aplican las reglas de acceso de las ACL que haya configuradas.

Router(config)#int g 0/1.2
Router(config-subif)#enc dot1Q 2
Router(config-subif)#ip add 192.168.2.254 255.255.255.0
Router(config-subif)#ip access-group 2 out

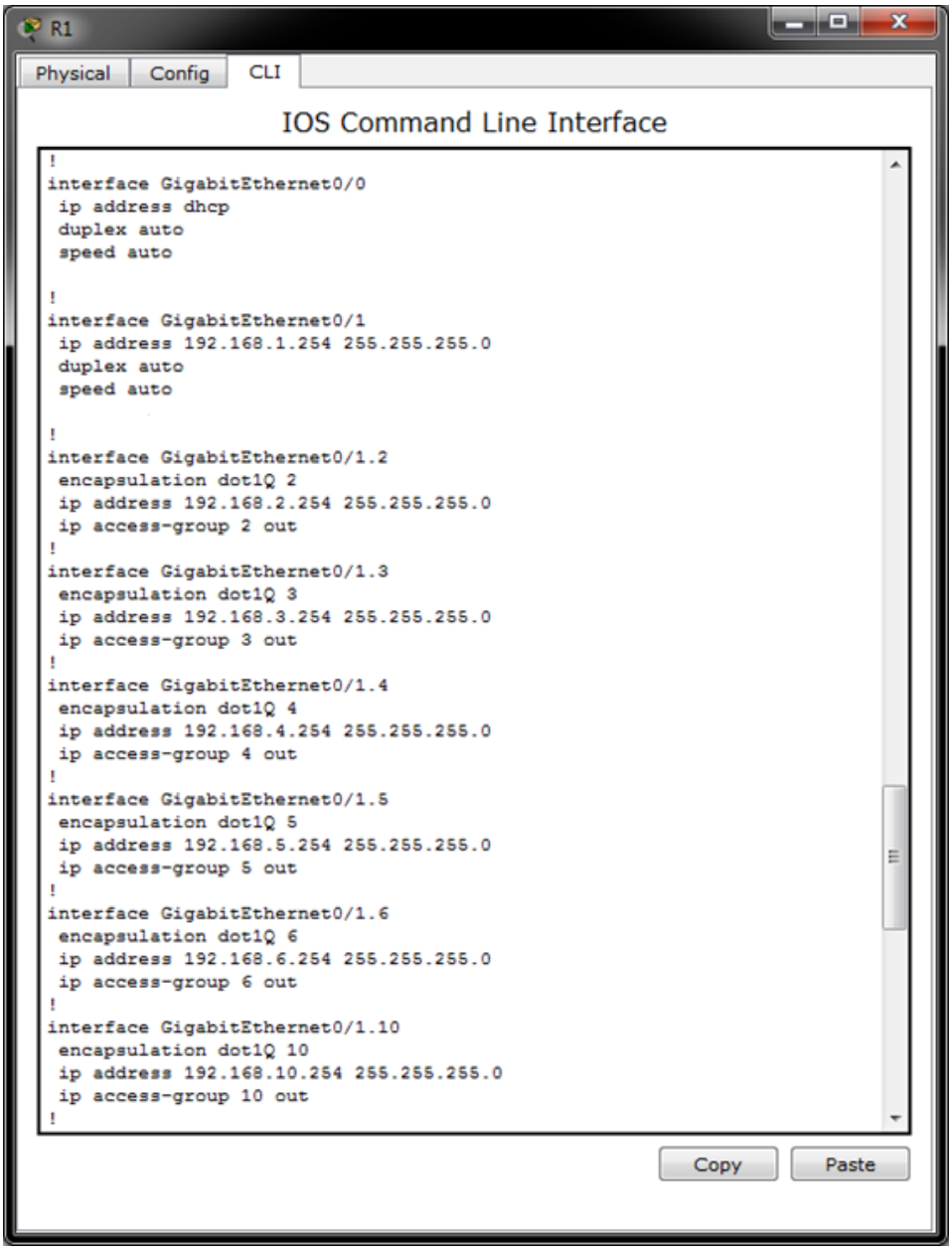


Figura 5.2.3. Configuración de las interfaces.

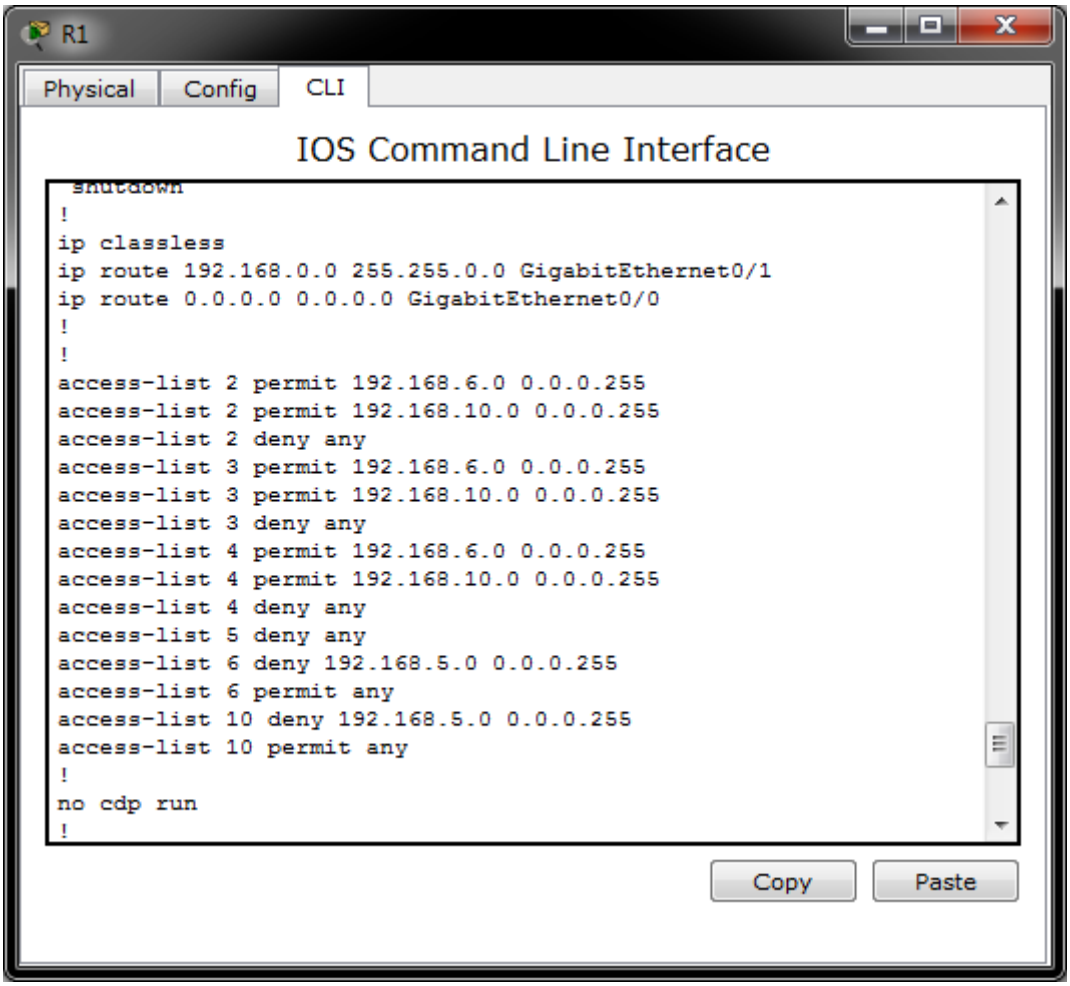


Figura 5.2.4. Configuración de las rutas de encaminamiento y de las listas de acceso.

En la figura 5.2.4 se muestran las rutas de encaminamiento estáticas y las listas de acceso que se configuran.

El formato de configuración de una lista de acceso es el siguiente:

Router(config)#access-list N permit/deny IP Wildcard

Donde N es el número de la VLAN a la que se va a aplicar, aunque se podría dar también un nombre, se permite o deniega el acceso con permit/deny, se indica la IP que se permite o deniega y por último, una Wildcard para definir el número de direcciones a las que se aplica la lista de acceso.

Como se aprecia en las figuras anteriores, se configurará para cada red un servidor DHCP, bien en el router o bien en un servidor virtualizado, dando direcciones IP dinámicamente a los equipos. De esta forma se facilita a la empresa añadir equipos nuevos a los distintos departamentos.

En las listas de acceso ningún equipo puede acceder a ningún departamento. Todos los departamentos, salvo la conexión WiFi, pueden acceder a la VLAN de impresoras y a los servidores. De este modo sólo se proporciona conexión a Internet y al servidor DHCP propio de su conexión (de su VLAN) a los equipos conectados inalámbricamente, evitando así accesos indeseados.

En la parte de seguridad, la red debe contar con los servicios de un servidor RADIUS o LDAP para controlar el acceso, un Firewall, servidor de monitoreo y punto de acceso con contraseña o simplemente controlado con los servidores RADIUS o LDAP. En la figura 5.2.5 se presenta una maqueta con dichos componentes.

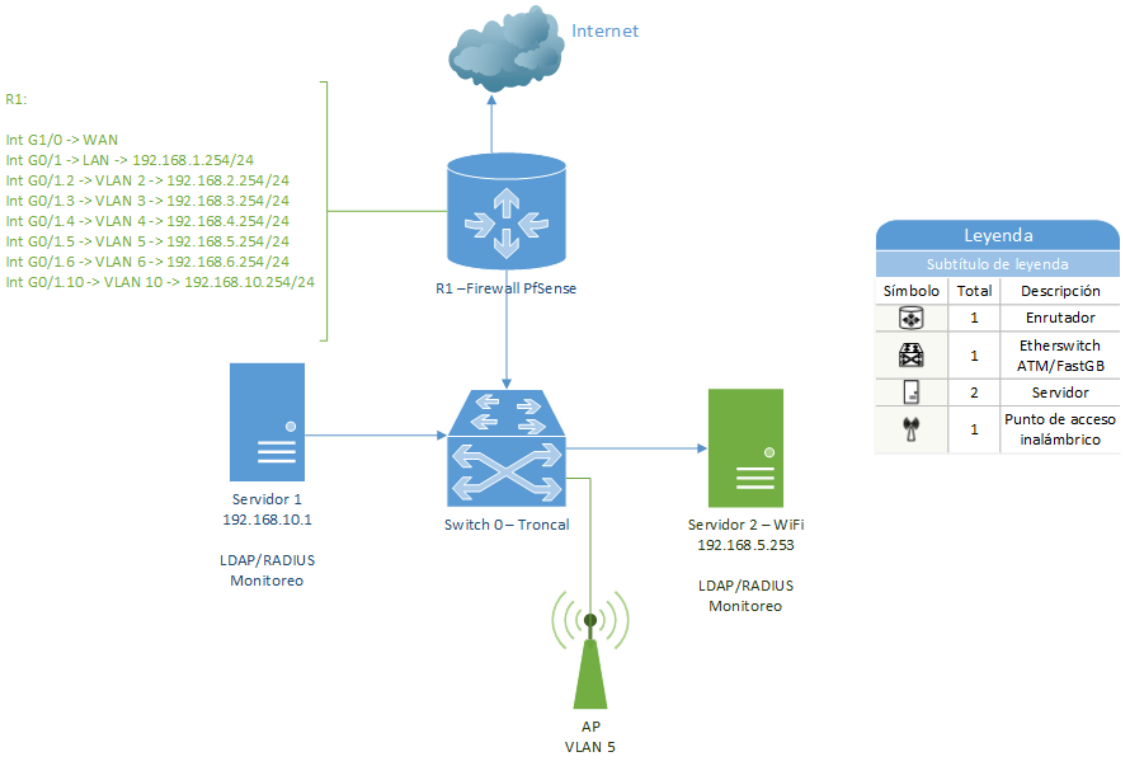


Figura 5.2.5. Servicios de seguridad.

Por último, los servicios que debe ofrecer la red se muestran en la figura 5.2.6. Estos serán al menos: DHCP, DNS, servidor de Backup, conexión inalámbrica, SMTP y si es necesario un servidor Web, estando todos ellos también virtualizados.

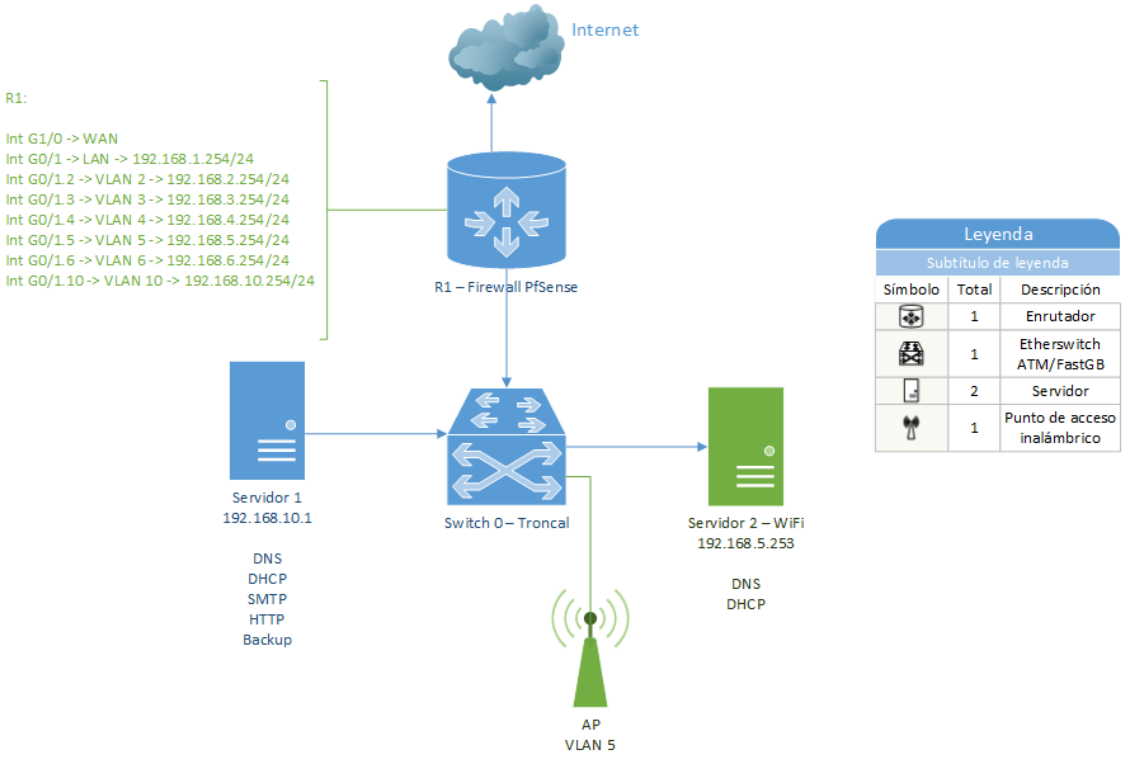


Figura 5.2.6. Servicios de la red.

En resumen, con esta solución se tiene una red completa y sencilla de configurar, funcional y segura, además de que cuenta con todos los servicios necesarios. Cabe añadir también que se reducen costes al virtualizar servidores y equipos, ya que además se utiliza software libre.

5.3. Solución utilizando únicamente IPv6

En este punto se va a proporcionar una solución sobre la red anterior pero en este caso configurada solo con el protocolo IPv6, sin tener configurado nada en IPv4.

Esta es una opción a tener en cuenta debido a la expansión del nuevo protocolo, pero será más conveniente aplicar soluciones en las que convivan ambas tecnologías, cuyos casos se explicarán en el siguiente punto.

Con esta solución se tienen los mismos equipos y servicios que en la solución anterior, solamente varían las direcciones IP, que en este caso son direcciones IPv6 configuradas manualmente, resultando la maqueta completa siguiente:

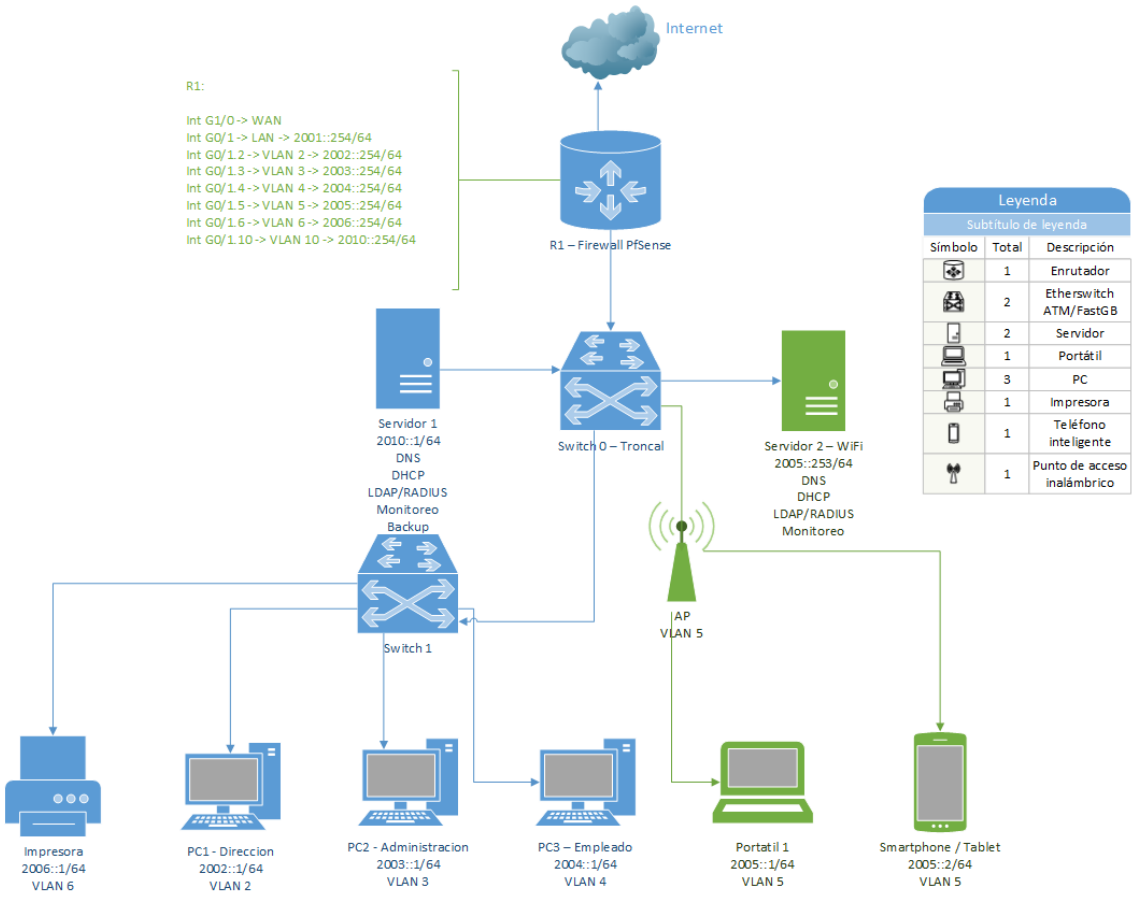


Figura 5.3.1. Maqueta configurada solo con IPv6

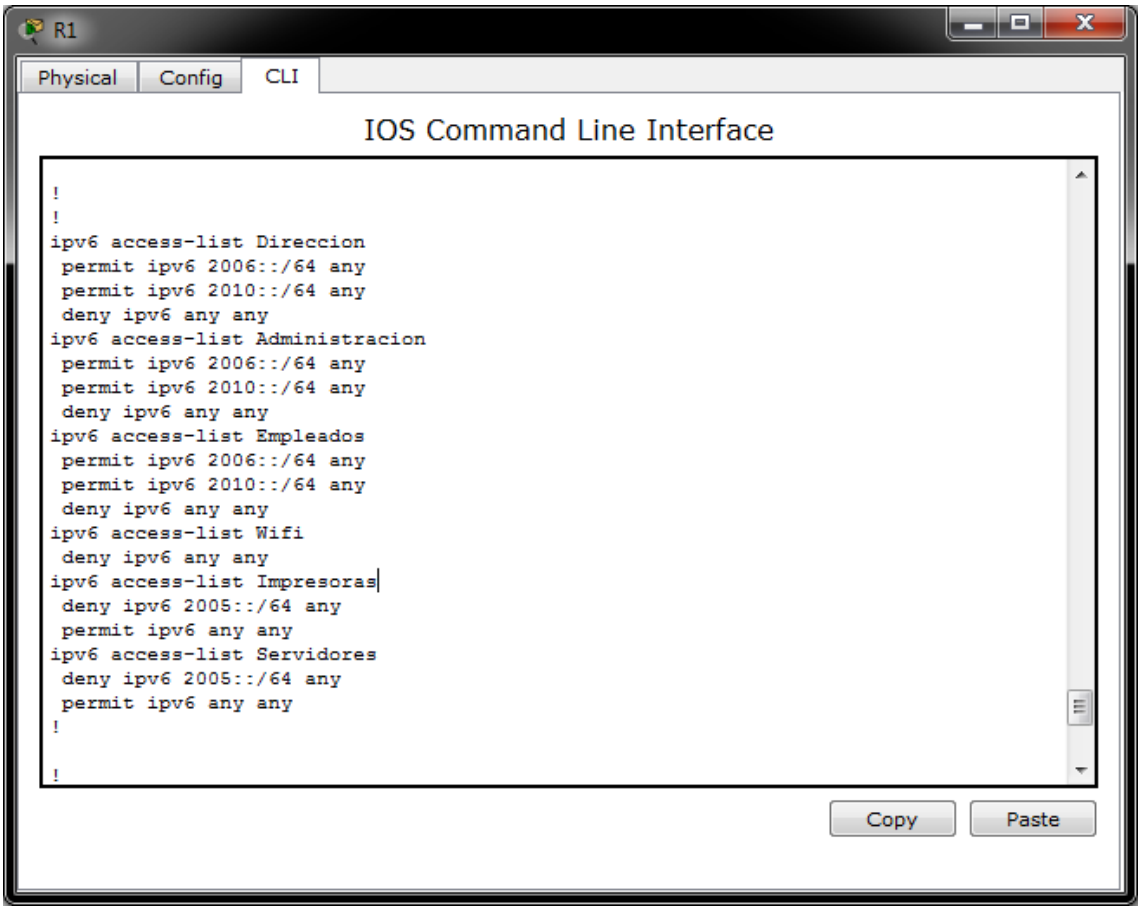


Figura 5.3.2. Configuración de las listas de acceso en IPv6.

En la figura 5.3.2 se observa la configuración de listas de acceso en formato IPv6, donde los comandos son los siguientes:

Router(config)#ipv6 access-list Nombre

Router(config-ipv6-acl)#permit/deny ipv6 IP Wildcard

En la primera línea de comando "Nombre" indica el número o nombre de la VLAN a la que se aplica, mientras que en la segunda línea se permite o deniega la dirección IP que indiquemos y la Wildcard con el valor any significa que esa regla de acceso se aplica a cualquier dirección de esa red.

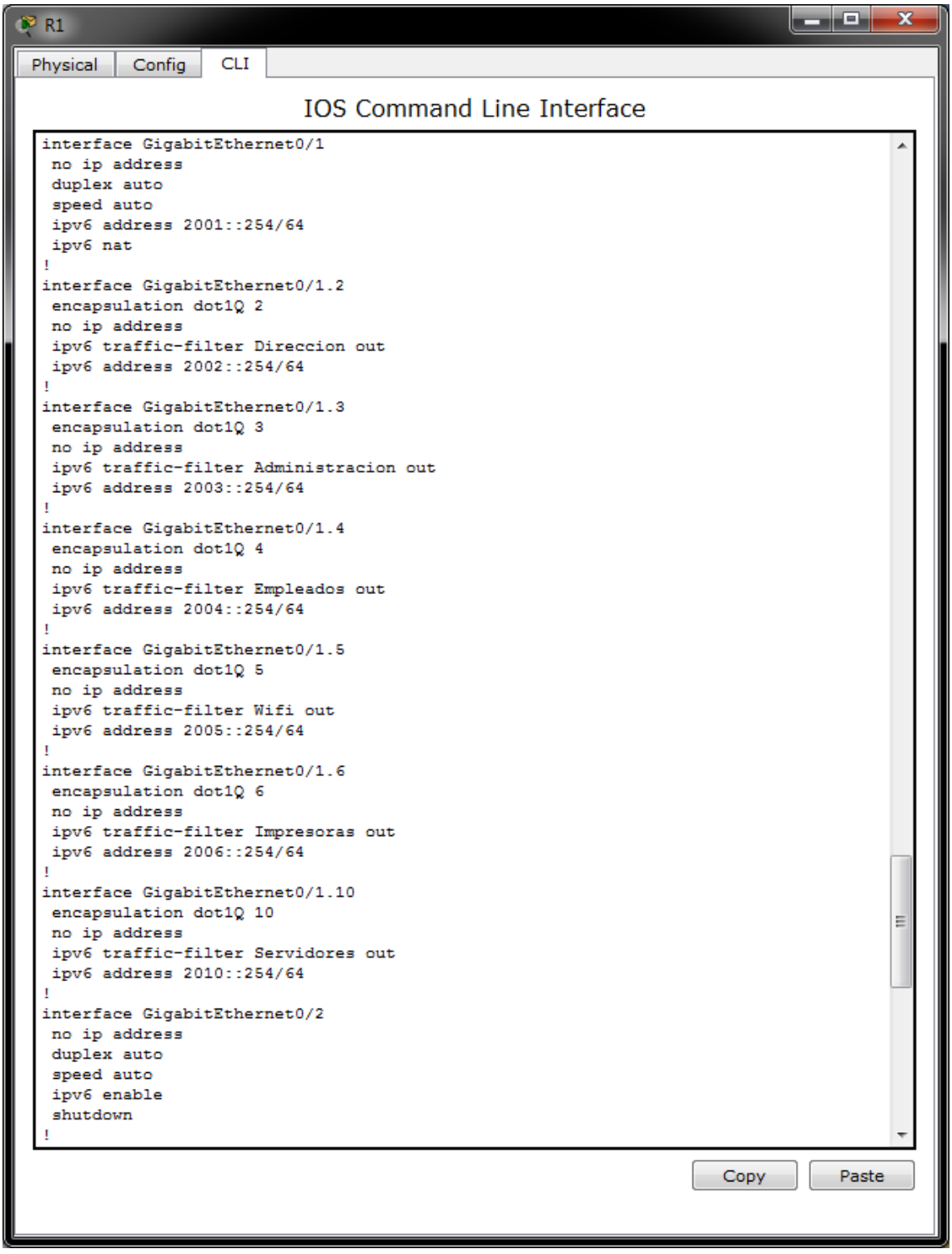


Figura 5.3.3. Configuración de las interfaces en IPv6.

En la figura 5.3.3 se configuran las interfaces para IPv6, usando para ello los comandos siguientes:

- Se selecciona interfaz virtual
  Router(config)#int g 0/1.2

- Se aplica encapsulación VLAN 802.1Q y se aplica el número o nombre de la VLAN en N.
  Router(config-subif)#enc dot1Q N

- Se indica que no posee dirección IPv4 esta interfaz, ya que se configura solamente con IPv6.
  Router(config-subif)#no ip address

- Se aplica la lista de acceso con el nombre que corresponda y se aplica la regla de entrada o salida de tráfico.
  Router(config-subif)#ipv6 traffic-filter Nombre in/out

- Por último, se asigna la dirección IPv6 que se desee aplicar.
  Router(config-subif)#ipv6 address IP

Como se puede observar, se ha realizado la configuración exactamente igual que en la solución de IPv4 pero con direcciones IPv6, teniendo mismos equipos y mismas opciones de acceso.

En resumen, ésta es una solución opcional ya que internamente no existe ninguna ventaja para tener configurados los equipos con IPv6. Además, si hay equipos antiguos es posible que no acepten este protocolo.

Por esto, se propone la que se ha considerado en este trabajo la mejor solución, tener red interna con IPv4 y poder salir a Internet tanto con dicho protocolo como con el nuevo protocolo IPv6. Esta solución se explica en el siguiente punto.

5.4. Solución de convivencia IPv4 – IPv6

Para finalizar este capítulo de soluciones a la red de una empresa se trata en este punto lo más importante: la adaptación de la red de una PyME para la convivencia entre el nuevo protocolo IPv6 e IPv4.

Las formas de tratar la convivencia se van a exponer a continuación, explicándolas y dando ejemplos con maquetas de cada situación.

- **Doble pila.**

  Esta primera solución consiste simplemente en configurar todos los equipos de la red con dos direcciones IP en cada interfaz, una IPv4 y otra IPv6, de esta forma todos los equipos saben direccionar con ambos protocolos.

  Es la solución más sencilla de implementar pero la que peores resultados proporciona, ya que genera demasiado tráfico redundante y provoca más carga en los equipos al tener doble direccionamiento.

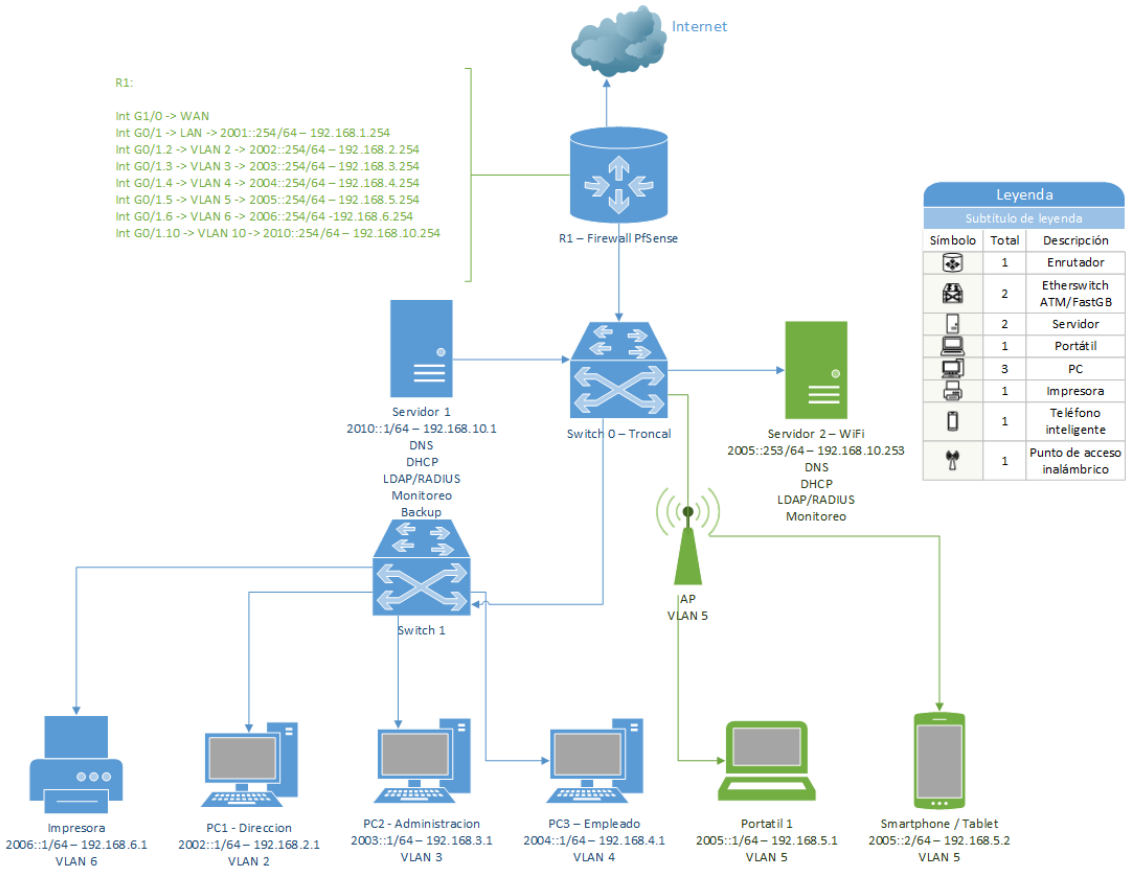


Figura 5.4.1. Maqueta configurada con IPv4 e IPv6

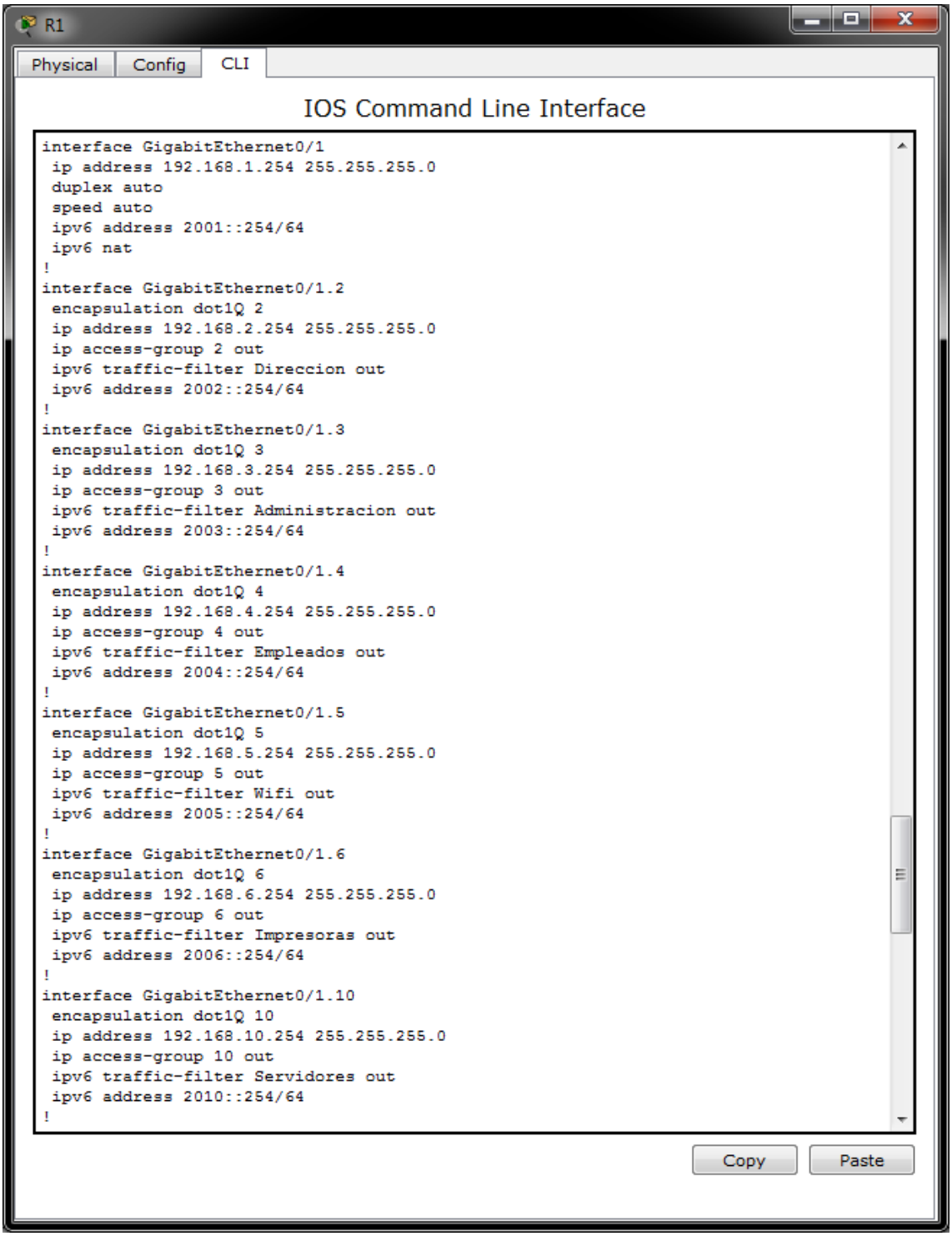


Figura 5.4.2. Configuración de las interfaces con IPv4 e IPv6

En la figura 5.4.2 se configuran las interfaces con direcciones de ambos protocolos, IPv4 e IPv6.

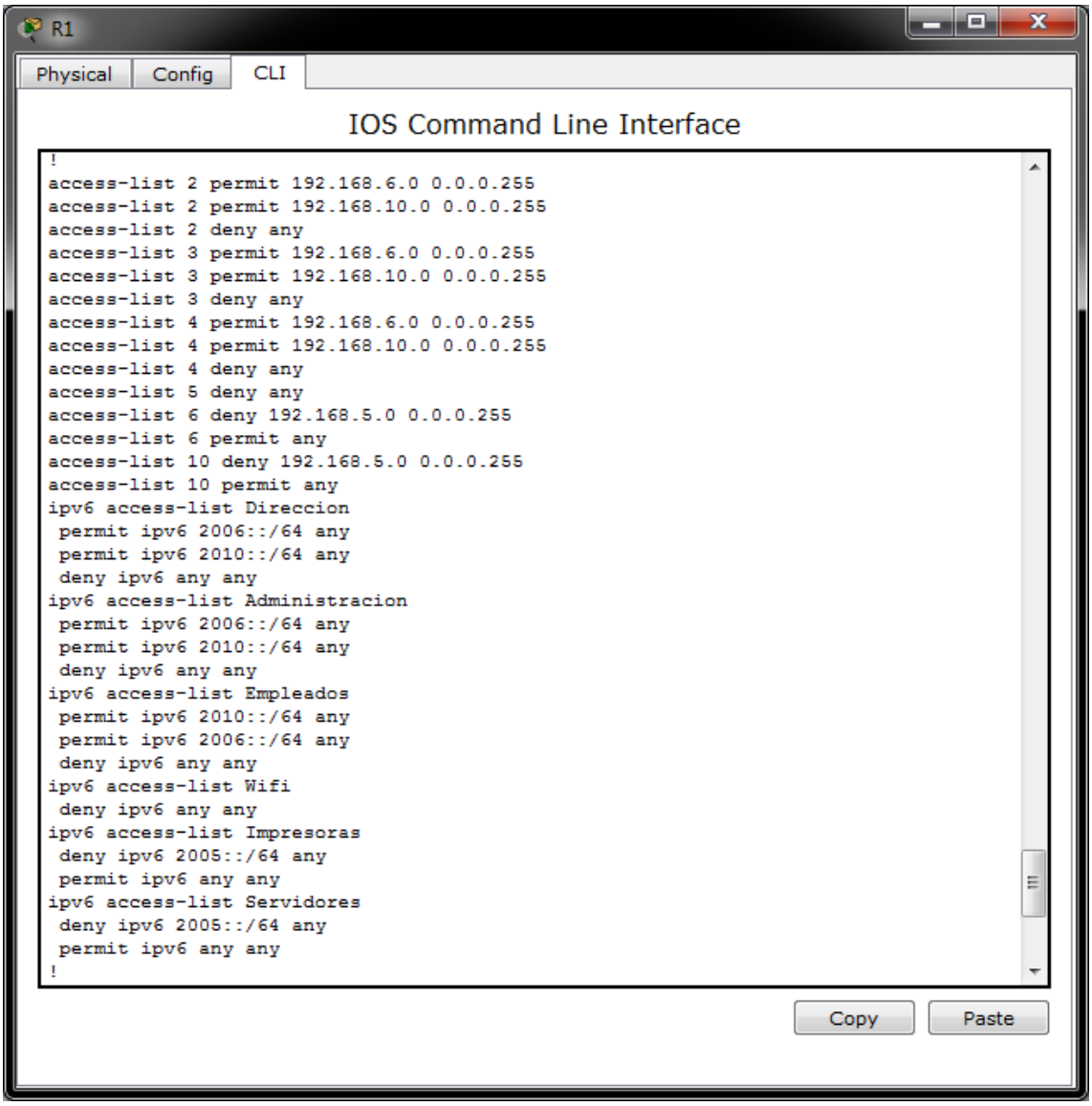


Figura 5.4.3. Configuración de listas de acceso para IPv4 e IPv6

Como se puede comprobar es una configuración tediosa pero muy simple, que conlleva tiempo de configuración y que además provoca cargas altas de CPU en los equipos, ya que por ejemplo, las listas de acceso son secuenciales. Por tanto, ésta es una mala solución.

- **Túneles**

  Otra solución viable es la configuración de túneles entre ambos protocolos, es decir, se crea un túnel que pase de la red configurada con IPv4 a IPv6 y viceversa, sería como un bridge.

  Un ejemplo para este caso sería una maqueta de red como la mostrada en la figura 5.4.4, en la que se tienen dos zonas con IPv6 conectadas mediante IPv4, teniendo que realizar el túnel 6to4 para comunicarlas.

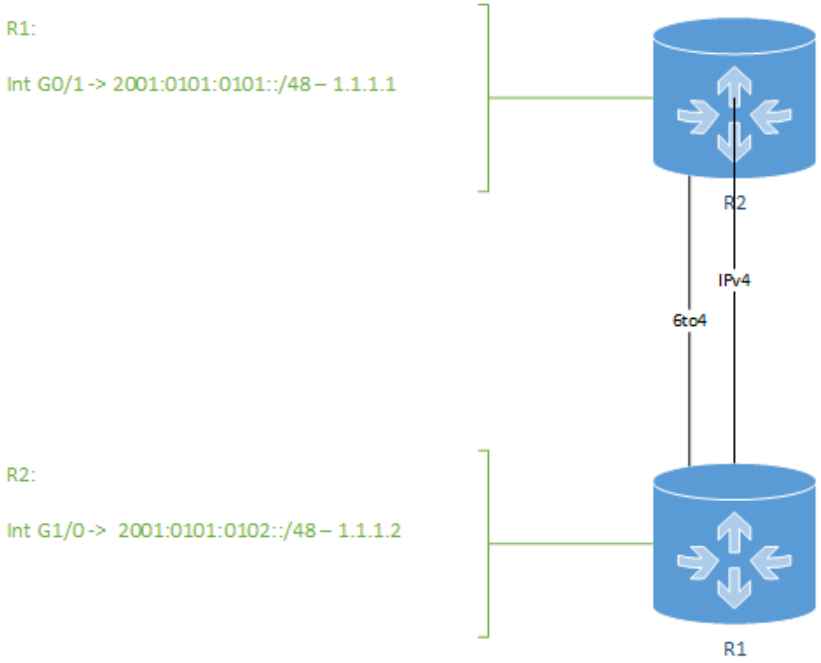


Figura 5.4.4. Maqueta de túneles.

Como se aprecia, se usa la dirección de destino IPv6 para la construcción de la dirección IPv4 del router, de esta manera los hosts con versión 6 se comunican con el router con dicha versión con normalidad.

Cuando el router consulta su tabla de enrutamiento ve que debe enrutar los paquetes por una interfaz túnel, además, esta interfaz es un túnel 6to4 por lo que examinando el paquete IPv6 es capaz de conocer la dirección IPv4 destino del paquete.

Por último, encapsula el paquete IPv6 en un paquete IPv4 que será capaz de llegar al router destino, que examinará, extraerá la cabecera IPv4 y lo reenviará por la red IPv6.

Se utilizan como redes origen y destino de IPv4 interfaces loopback, que ofrecen mayor estabilidad que una interfaz física. Las direcciones de estas interfaces se propagan por el protocolo de enrutamiento, ya que sin esto no se podría alcanzar el destino del túnel desde el origen.

La configuración del túnel en el router sería la siguiente:

Router(conf)#ipv6 unicast-routing

Router(conf)#interface Tunnel 0

Router(conf-if)#no ip address

Router(conf-if)#no ip redirects

Router(conf-if)#ipv6 enable

Router(conf-if)#tunnel source Loopback0

Router(conf-if)#tunnel mode ipv6ip 6to4

Router(conf)#ipv6 route 2001::/16 tunnel0

Cabe añadir que se accede al túnel mediante una única ruta estática.

En resumen, esta solución es escalable, ya que la configuración es siempre la misma y no depende del número de zonas IPv6 que se conecten, es sencilla de configurar, convierte automáticamente direcciones IPv6 en IPv4 y no requiere de rutas estáticas para cada destino.

- **Traducción**

  Por último, esta solución trata de configurar el router que da salida a Internet con un NAT que permita la conversión de la red interna. Esta es la mejor solución, ya que no nos importa la versión del protocolo que nos proporciona el operador ni la que tengamos configurada internamente. Además, es la solución de la que más formas se puede realizar la configuración y la que mejores resultados aporta.

  Normalmente se encontrará la red interna configurada con IPv4, ya que es lo que todas las empresas tendrán configurado actualmente y en un futuro será cuando los operadores ofrezcan directamente IPv6. Así que con esta solución tendremos la red interna con IPv4 y un NAT configurado en el router para poder salir tanto con IPv4 como con IPv6.

  CISCO da dos formas de realizar esta configuración en los routers, son las siguientes:

  - **NAT-PT**

    Con esta configuración hay que asignar al router frontera una IPv4 y una IPv6 en dos interfaces diferentes, además de activar NAT de versión 6 y crear un pool de direcciones tanto IPv4 como IPv6. Las direcciones del pool serán las que se usen a la hora de traducir en cualquiera de los dos sentidos (éste será el router del operador que estará conectado a la red interna con IPv4 por una interfaz que será la LAN y a la red externa con IPv6 por otra interfaz que será la WAN). Cabe añadir que esta configuración ésta en desuso (deprecated).

    Un ejemplo de este tipo de configuración es el que se puede contemplar en la figura 5.4.5, en el que se tiene una red con IPv4 que emula la red interna de la empresa y otra con IPv6 que se supone es la red del operador.

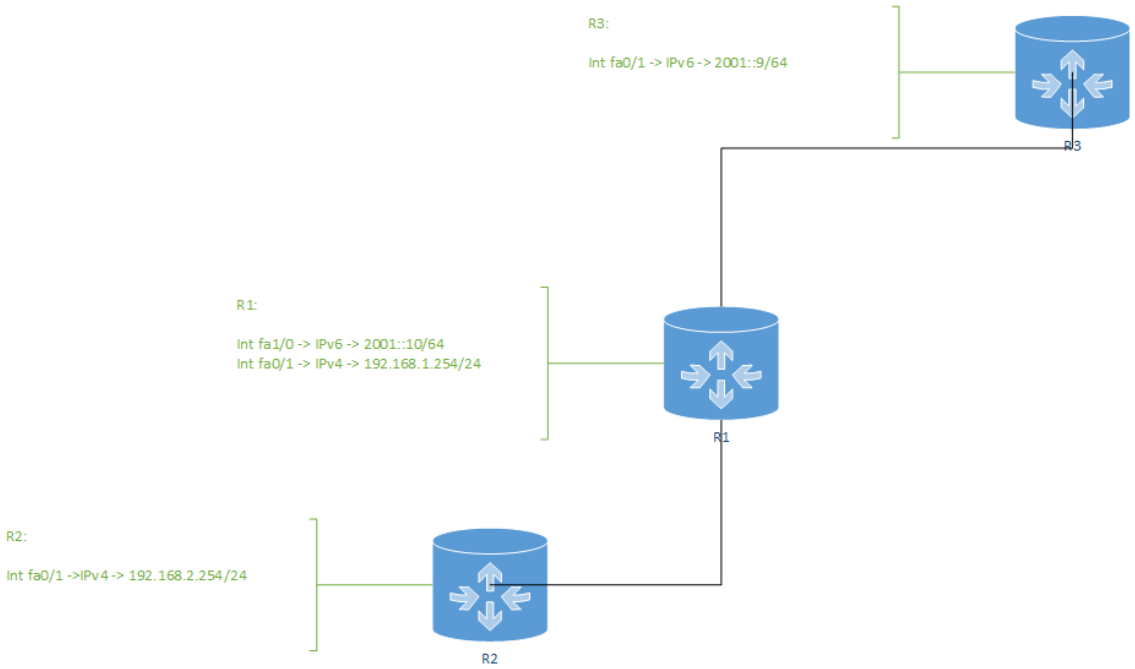


Figura 5.4.5. Maqueta de configuración NAT-PT.

ip cef

no ip domain lookup

ipv6 unicast-routing

!

interface FastEthernet0/1

ip address 192.168.1.254 255.255.255.0

ipv6 nat

!

interface FastEthernet1/0

no ip address

ipv6 address 2001::10/64

ipv6 enable

ipv6 nat

!

ipv6 route ::/0 2001::9

ipv6 nat v4v6 source 192.168.1.254 2000::202

ipv6 nat v6v4 source 3001::1 192.168.1.100

ipv6 nat prefix 2000::/96

Como se observa en el ejemplo, se configura una interfaz con IPv4 y otra con IPv6, activando el ruteo unicast de IPv6 y el NATv6. Por último, se crean las rutas de encaminamiento hacia cada red, se asigna un prefijo para la conversión y se dan IPs fijas (en este caso no se ha creado ningún pool de direcciones) a la hora de convertir tanto en un sentido como en otro.

- **NAT64**

Esta solución es la que usa CISCO actualmente, es muy similar a la anterior, lo único que cambia es que en lugar de usar el comando "ipv6 nat" se utiliza "nat64".

Cabe aclarar que esta solución no se pudo comprobar en el simulador Packet Tracer al no disponer de este comando los routers que lleva el programa.

Un ejemplo como el anterior pero con esta configuración es el que se muestra en la figura 5.4.6:

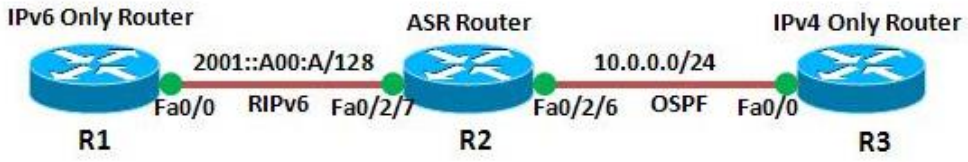


Figura 5.4.6. Maqueta de configuración NAT64.

R2(IPv4 e IPv6):

ipv6 unicast-routing
!
!
interface Loopback0
no ip address
ipv6 address BB10::1/128

```
!
interface Loopback1
ip address 2.2.2.2 255.255.255.255
!
!
interface FastEthernet0/2/6
ip address 10.0.0.2 255.255.255.0
negotiation auto
nat64 enable
!
interface FastEthernet0/2/7
no ip address
negotiation auto
ipv6 address 2001::A00:B/128
ipv6 rip RIP enable
ipv6 rip RIP default-information only
nat64 enable
!
!
router ospf 1
network 2.2.2.2 0.0.0.0 area 1
network 10.0.0.0 0.0.0.255 area 0
!
!
ipv6 router rip RIP
!
!
!
nat64 prefix stateful 3001::/96
nat64 v6v4 static 2001::A00:A 10.0.0.10
!
end
```

Esta solución de traducción mediante NAT con el enrutador PfSense es más sencilla, ya que por medio de la interfaz web se configura fácilmente. En la figura 5.4.7 se puede observar el menú de configuración para esta opción.

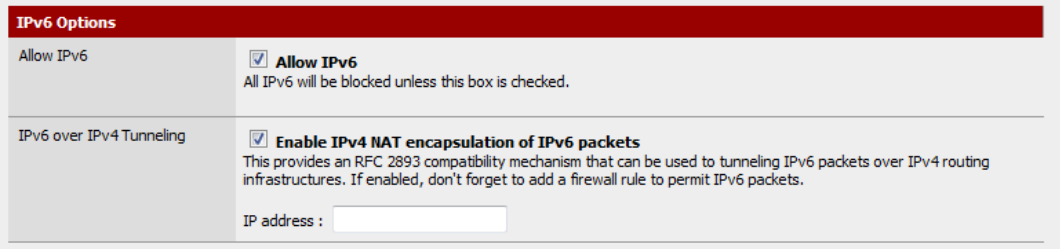


Figura 5.4.7. Configuración en PfSense de la traducción.

La configuración con NAT se puede realizar tanto si se tiene dentro IPv4 como IPv6, solo se configuran las direcciones origen y destino.

La solución más común sería la que cuenta con una red interna configurada con IPv4, y usar un NAT hacia Internet con IPv6, que será el ofrecido por el operador. Así hay que configurar solamente la traducción en el enrutador y no hay que cambiar nada en la red interna.

Capítulo 6

6. Conclusiones

En este trabajo se ha realizado una visión sobre el estado actual de la red de las PyMEs, analizando equipos y servicios, y se han dado soluciones finales para conseguir una red económica pero útil.

Se han estudiado y probado diferentes enrutadores. Como son la emulación de un router CISCO mediante imágenes distribuidas gratuitamente y la instalación de un software libre como es PfSense, resultando mejor opción éste último. Además, se han probado diferentes monitores de red, como son Cacti, OpenNMS y Nagios para el mantenimiento de la red y ayudar al control de errores y fallos de hardware y de seguridad.

Analizando los equipos que ofrecen los operadores a las empresas se ha podido detectar que no se proporcionan servicios ni equipos que aporten a las PyMEs la potencia que necesitan, ya que ofrecen los mismos equipos que para usuarios domésticos. Además, se ha comprobado que un enrutador como PfSense, que permite gran cantidad de opciones de configuración y es gratuito, aporta un añadido muy importante.

En ese mismo sentido, se observa que la virtualización ayuda a mejorar la red sin necesidad de grandes desembolsos por parte de la empresa, ya que con pocos equipos se pueden aplicar diversos servicios.

A la hora de probar configuraciones se ha utilizado CISCO Packet Tracer y los switches y equipos del laboratorio IT-5, pudiendo en este último caso realizar pruebas reales de configuración y comportamiento.

Por último, se han dado soluciones para la mejora de la red de una empresa y para adaptarla al uso del nuevo protocolo de Internet IPv6, viendo que la mejor solución es realizar una traducción (NAT) en el router de acceso, manteniendo la red interna

con la configuración que tuviese y haciendo posible la convivencia del nuevo protocolo con el anterior.

Líneas de desarrollo futuro

Se pueden investigar nuevas formas de realizar la traducción entre IPv4 e IPv6 además de comprobar si aparece nuevo software libre que se pueda utilizar, como por ejemplo usar un firewall más dedicado que PfSense, como puede ser IPFire o software de monitoreo más potente como Centreon.

Es posible realizar mayor número de maquetas y diferentes configuraciones en los equipos para probar nuevos protocolos o más casos en los que analizar el funcionamiento de las configuraciones que se realicen o de las que se han realizado durante el desarrollo de este trabajo.

Lógicamente queda pendiente siempre prestar atención a nuevas versiones del software libre y de la electrónica de red para aprovechar al máximo el desembolso realizado.

Además de que los equipos informáticos siempre son ampliables y se deben ir renovando los componentes para no tener que cambiarlos completamente en años, solo comprando los componentes necesarios, así la inversión se rentabiliza al máximo.

Bibliografía

[1] CCSP Self-Study: CISCO Secure PIX Firewall Advanced (CSPFA) Second Edition. Behzad Behtash. CISCOpress.com

[2] Administering CISCO QoS in IP Networks. Michael E. Flannagan, Benoit Durand, Jerry Sommerville, Mark BUchmann, Ron Fuller. Calisma.

[3] Sitio Web: http://es.wikipedia.org/wiki/Direcci%C3%B3n_IPv6

[4] Sitio Web: http://es.wikipedia.org/wiki/IPv6#Paquete_IPv6

[5] Sitio Web: http://es.wikipedia.org/wiki/IPv6

[6] Sitio Web: https://www.pfsense.org/

[7] Sitio Web: http://www.gns3.net/dynamips/

[8] Sitio Web: http://www.cacti.net/

[9] Sitio Web: http://www.opennms.org/

[10] Sitio Web: http://www.wireshark.org/

[11] Sitio Web: http://www.nagios.org/

[12] Manual de usuario switch D-Link DES-3200.

[13] Manual de usuario switch D-Link DGS-3200.

[14] Documentación de Ethertype:

http://standards.ieee.org/develop/regauth/ethertype/eth.txt

Anexos

Manual de instalación de PfSense

PfSense es un proyecto libre de código abierto especialmente diseñada como firewall y router totalmente personalizable a través de interfaz web. Derivada de m0n0wall, creado en 2004.

Dispone de una gran lista de características y paquetes adicionales para expandir su funcionalidad, llegando a ser muy popular y obteniendo más de 1 millón de descargas desde su aparición.

Si se intenta instalar PfSense sobre un disco duro sin virtualizar ocupara todo el espacio del disco, así que la mejor opción es instalarlo sobre un máquina virtual basada en Linux, así aprovechamos los beneficios de la virtualización que es lo que se pretende en este trabajo.

A continuación se explica la instalación de PfSense sobre Debian:

Instalación de Debian en máquina virtual VirtualBox:

Agregar estos repositorios en el fichero /etc/apt/sources.list

 # deb cdrom:[Debian GNU/Linux 7.0.0 _Wheezy_ - Official amd64 CD Binary-1 20130504-14:44]/ wheezy main

 # deb cdrom:[Debian GNU/Linux 7.0.0 _Wheezy_ - Official amd64 CD Binary-1 20130504-14:44]/ wheezy main

deb http://ftp.es.debian.org/debian/ wheezy main

deb-src http://ftp.es.debian.org/debian/ wheezy main

deb http://security.debian.org/ wheezy/updates main

deb-src http://security.debian.org/ wheezy/updates main

 # wheezy-updates, previously known as 'volatile'

deb http://ftp.es.debian.org/debian/ wheezy-updates main

deb-src http://ftp.es.debian.org/debian/ wheezy-updates main

#===

Modificaciones extra

#===

Debian

deb http://ftp.us.debian.org/debian wheezy main contrib non-free

Webmin

deb http://download.webmin.com/download/repository sarge contrib

deb http://webmin.mirror.somersettechsolutions.co.uk/repository sarge contrib

VirtualBox

deb http://download.virtualbox.org/virtualbox/debian wheezy contrib

#

Guardamos y salimos.

A continuación, en consulta, añadimos estos enlaces para que funcionen los repositorios correctamente:

wget http://www.webmin.com/jcameron-key.asc

apt-key add jcameron-key.asc

wget -q http://download.virtualbox.org/virtualbox/debian/oracle_vbox.asc -O- | sudo apt-key add -

Si va todo bien, nos saldrá OK en cada uno de ellos.

Después, podemos hacer:

aptitude install virtualbox-4.2

aptitude install unrar-free

aptitude install rar unrar p7zip

aptitude install webmin

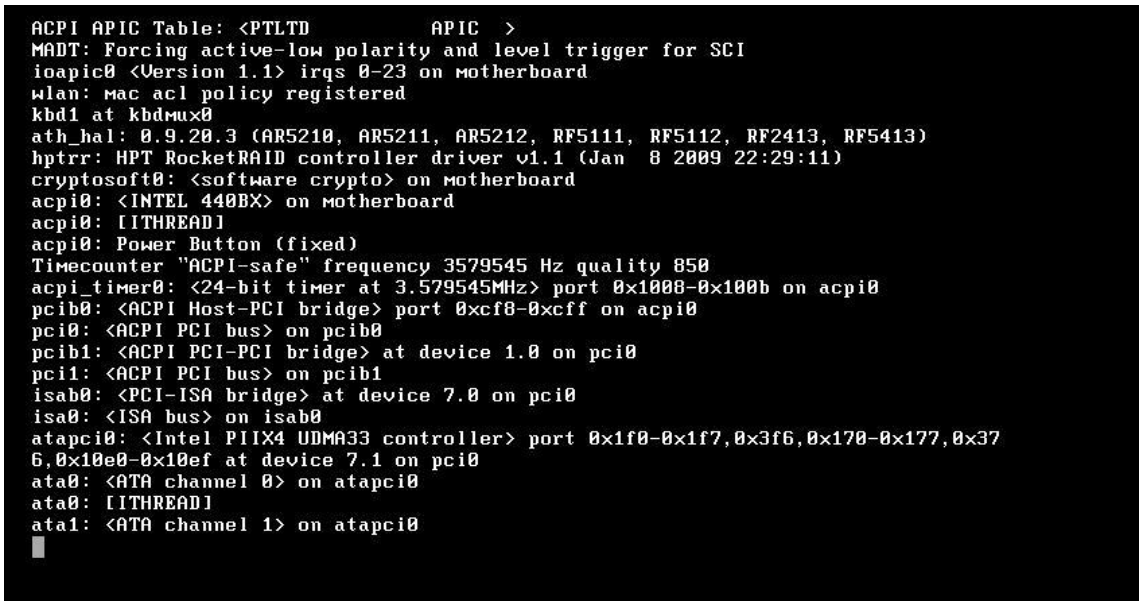
aptitude install build-essential linux-headers-`uname -r` gcc make libstdc++6 fakeroot

Instalación de PfSense:

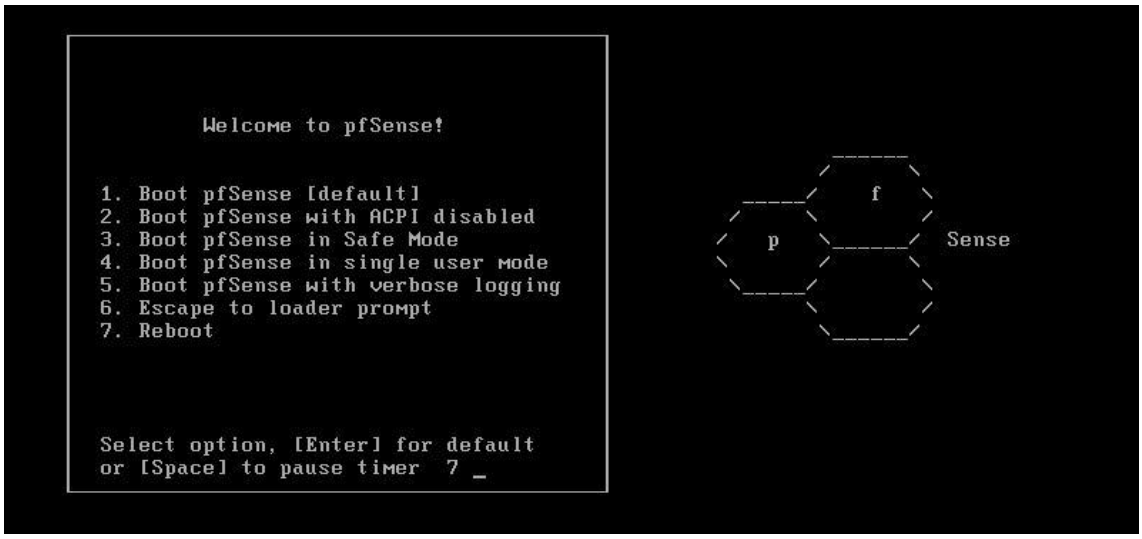
Descargamos PfSense y lo grabamos en un CD.

https://www.pfsense.org/download/index.html?section=downloads

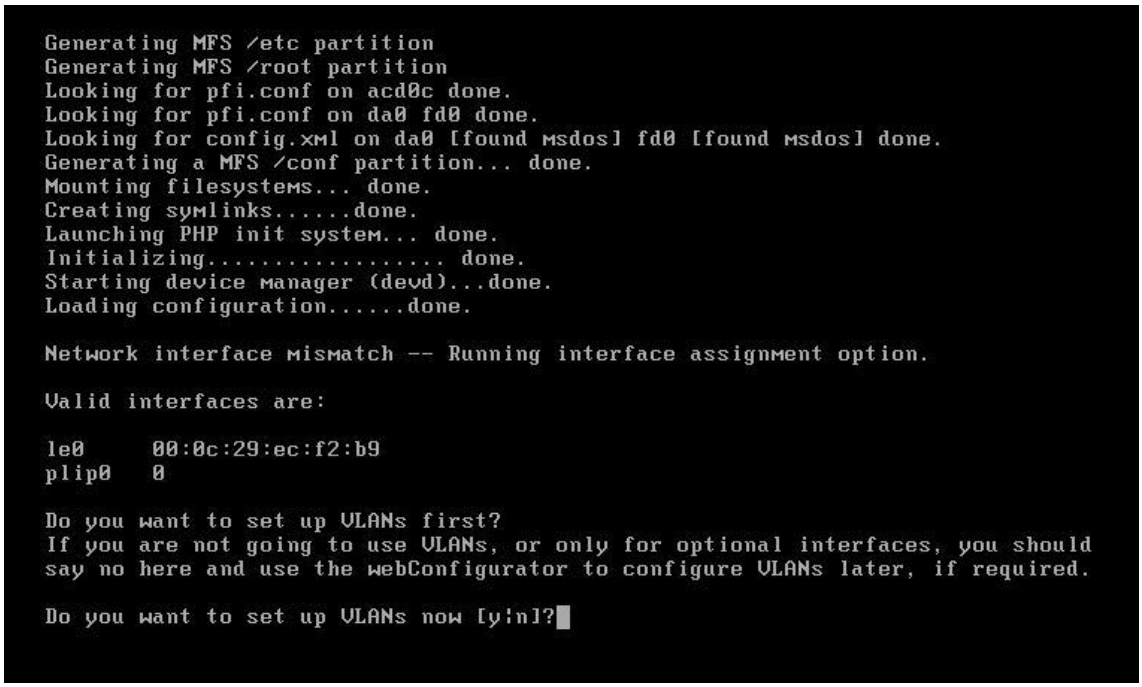
Durante la instalación vemos:



Al finalizar la instalación vemos la pantalla de bienvenida siguiente y pulsamos 1:



Después nos preguntará si queremos crear VLAN, en principio decimos que no (N):



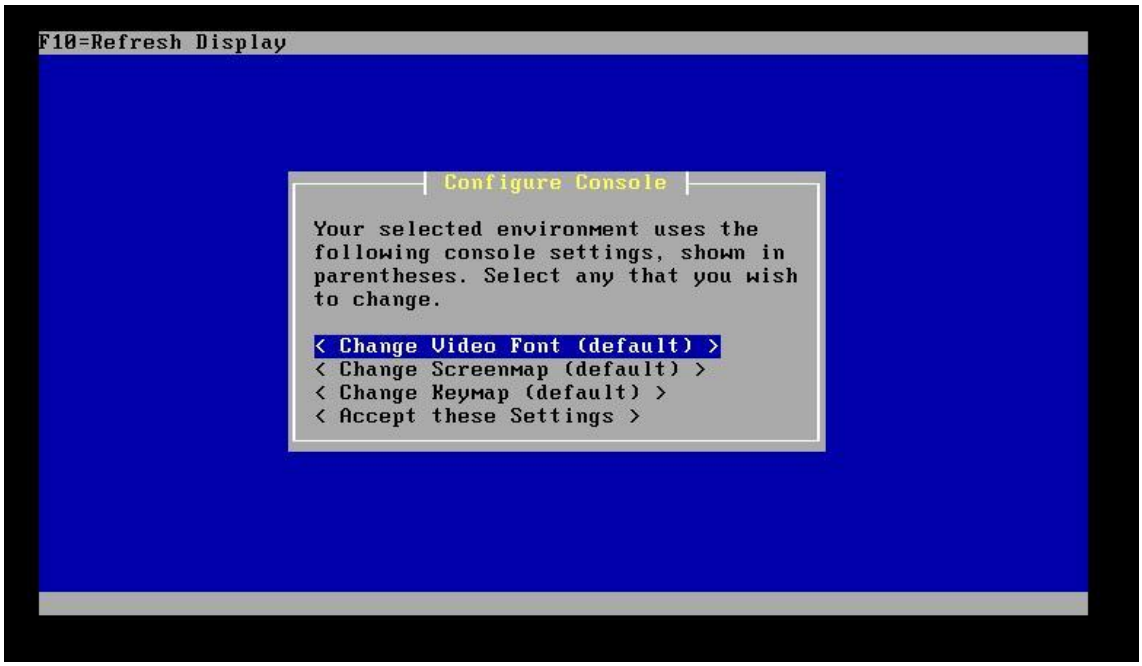
En el siguiente paso se eligen la interfaz WAN y LAN, elegimos las dos interfaces que queramos de nuestro PC (permite la auto detección, pero mejor elegirlas manualmente para saber posteriormente cual hemos elegido):

```
le0     00:0c:29:ec:f2:b9
le1     00:0c:29:ec:f2:c3
plip0   0

Do you want to set up VLANs first?
If you are not going to use VLANs, or only for optional interfaces, you should
say no here and use the webConfigurator to configure VLANs later, if required.

Do you want to set up VLANs now [y|n]?n

*NOTE*  pfSense requires *AT LEAST* 2 assigned interfaces to function.
        If you do not have two interfaces you CANNOT continue.

        If you do not have at least two *REAL* network interface cards
        or one interface with multiple VLANs then pfSense *WILL NOT*
        function correctly.

If you do not know the names of your interfaces, you may choose to use
auto-detection. In that case, disconnect all interfaces now before
hitting 'a' to initiate auto detection.

Enter the LAN interface name or 'a' for auto-detection: le1

Enter the WAN interface name or 'a' for auto-detection:
```

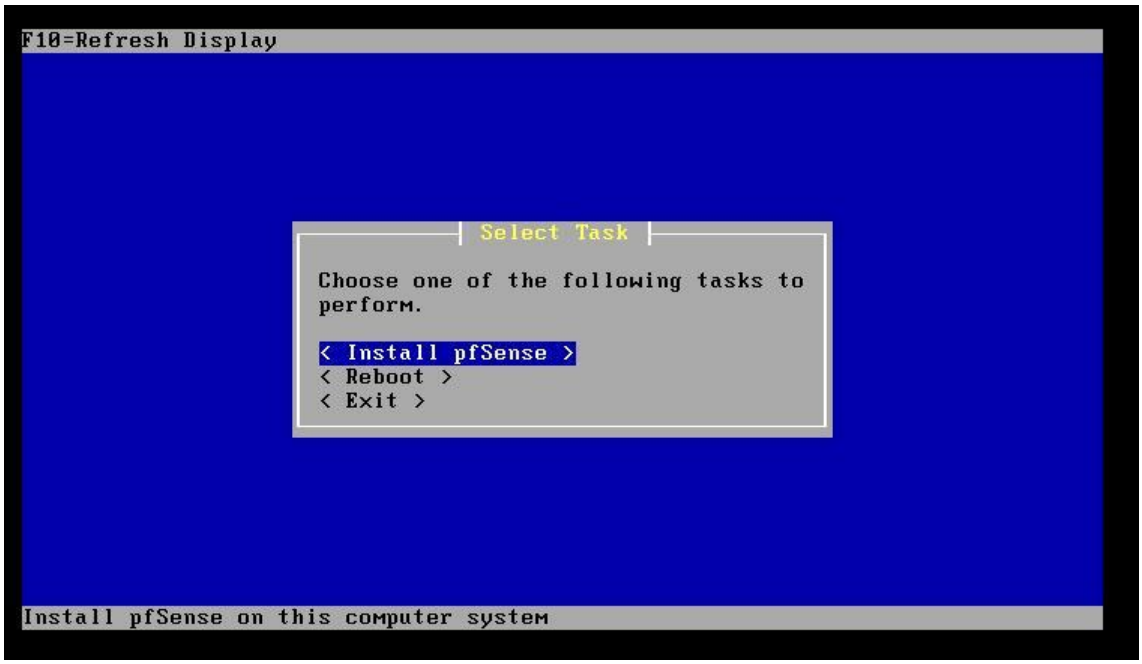
Al finalizar la creación de las interfaces presionamos ENTER y nos lleva a la siguiente pantalla donde elegiremos la opción 99 para empezar la instalación en disco.

```
  WAN*                  ->   le0     ->      192.168.1.66(DHCP)
  LAN*                  ->   le1     ->      192.168.1.1

 pfSense console setup
************************
 0)  Logout (SSH only)
 1)  Assign Interfaces
 2)  Set LAN IP address
 3)  Reset webConfigurator password
 4)  Reset to factory defaults
 5)  Reboot system
 6)  Halt system
 7)  Ping host
 8)  Shell
 9)  PFtop
10)  Filter Logs
11)  Restart webConfigurator
12)  pfSense PHP shell
13)  Upgrade from console
14)  Enable Secure Shell (sshd)
98)  Move configuration file to removable device
99)  Install pfSense to a hard drive/memory drive, etc.


Enter an option:
```

En la primera pantalla de instalación seleccionamos la opción por defecto.

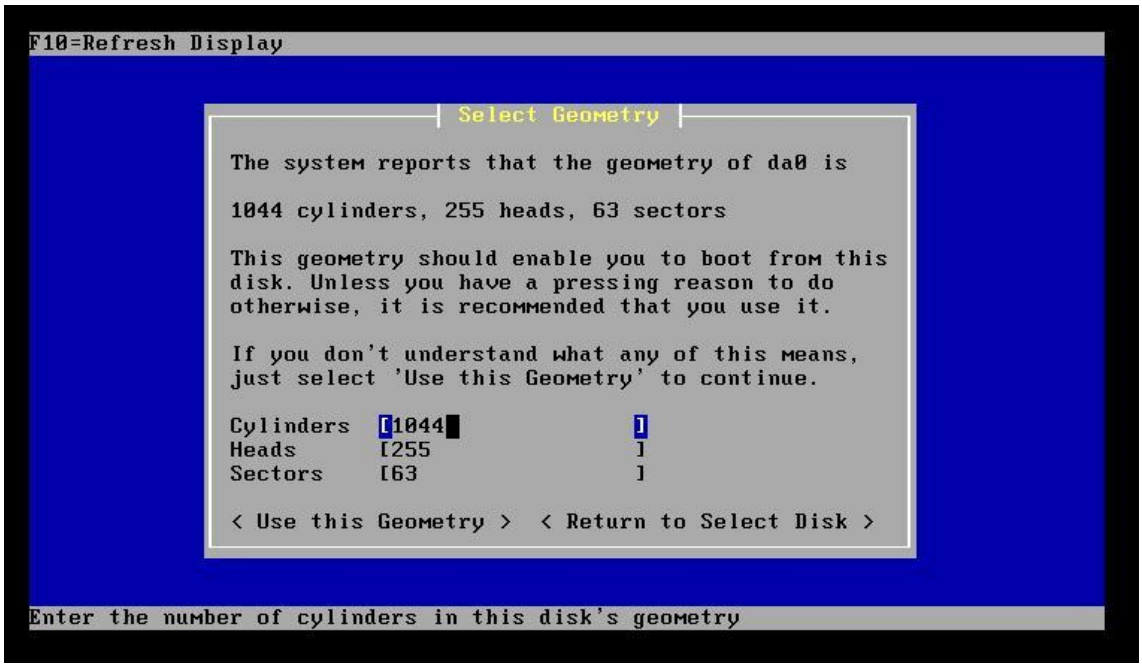


En el siguiente paso se comienza la instalación.

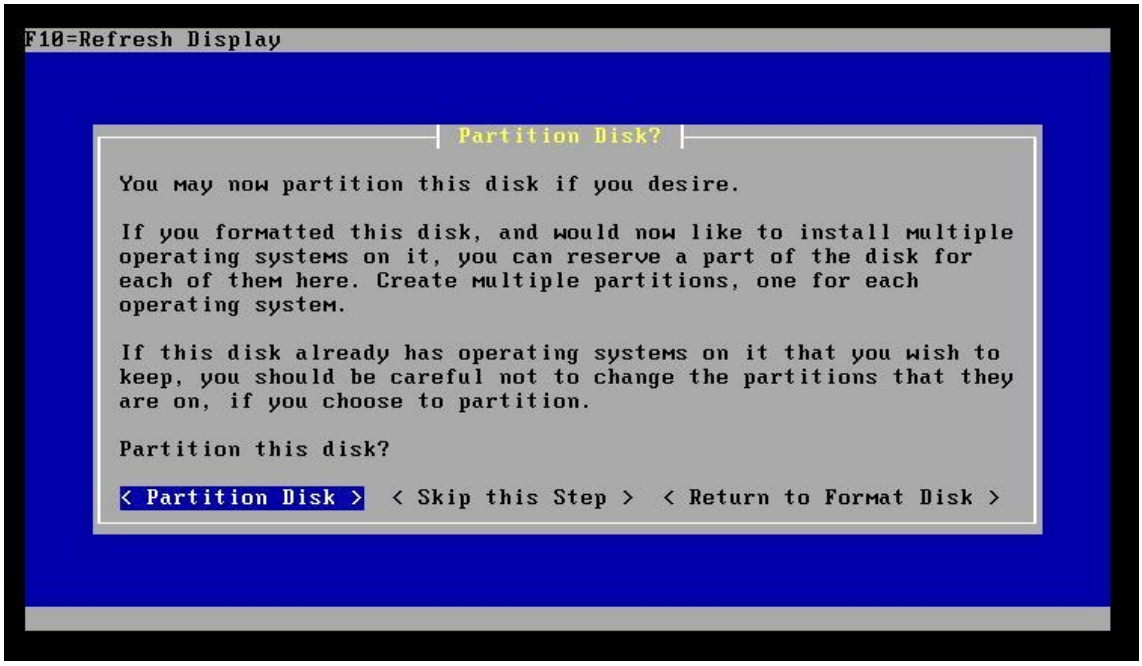


Ahora nos pide que formateemos el disco. La ventaja de hacerlo en máquina virtual es que no se perderá nada, ya que solo instalara en la partición que hayamos dado a nuestra máquina virtual (dar 12 GB a la máquina virtual, 2 GB para swap y 10 para la instalación de PfSense).

A continuación se le da el tamaño que queremos según el tamaño de disco que tengamos asignado (daremos todo, ya que estamos trabajando con una máquina virtual).

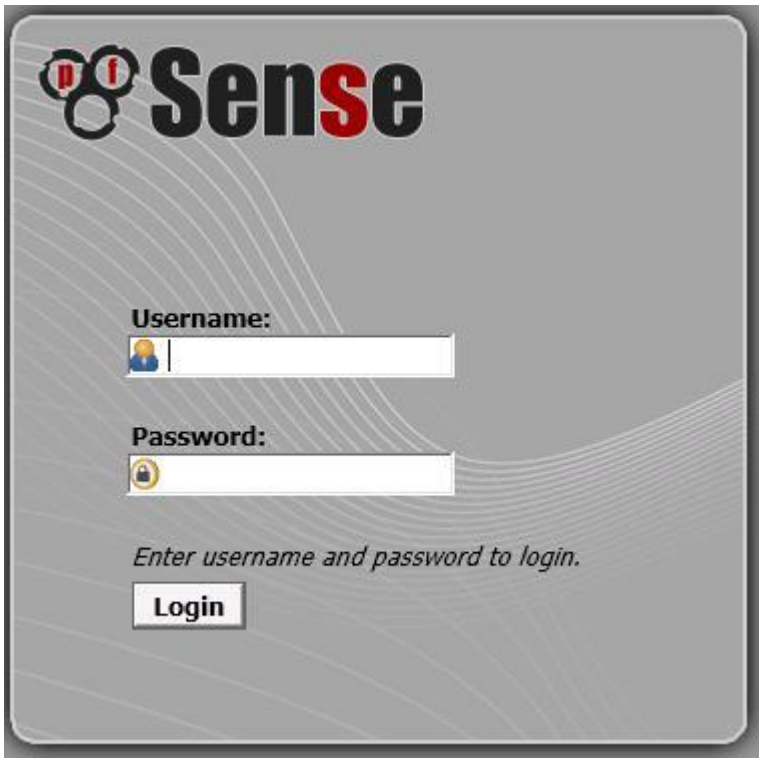


Tras formatear, nos pide particionar el disco para instalar el sistema operativo de PfSense. Seleccionamos FreeBSD, que es la opción por defecto, y lo instalamos en la partición anterior.



Cuando finalice el proceso de instalación reiniciamos.

Una vez reiniciado podemos abrir un navegador y a través de la IP dada (192.168.1.1) podemos acceder a la interfaz web para configurar el enrutador.



La pantalla que vemos es la anterior, y los datos de acceso por defecto son:

User: admin

Password: pfsense.

Manual de emulación de un router con IOS CISCO

Proceso para instalar y emular un router CISCO con la IOS que se prefiera en Windows XP / 7. Los pasos son los siguientes:

1. Instalar WinPcap. http://www.winpcap.org/install/default.htm
2. Instalar Dynagen. http://sourceforge.net/projects/dyna-gen/files/
3. Ejecutar Network Device List que estará en el escritorio. De ahí sacamos el NIO_gen_eth de las tarjetas que usamos como WAN y como LAN del router emulado.
4. En *C:\Archivos de programa\Dynampis\images* metemos las IOS de CISCO que queramos emular.
5. En *C:\Archivos de programa\Dynamips\sample_labs\simple1*, dónde simple1 será la carpeta que contendrá el fichero de texto donde indiquemos las interfaces. Hacemos click derecho sobre el archivo Simple1 y lo abrimos como bloc de notas.
    a. Añadimos o modificamos la ruta de image para poner la ruta de la IOS que queremos usar.
    Por ejemplo:
    image = C:\Archivos de programa\Dynamips\images\c7200-p-mz.122-2.T4.bin
    b. Añadimos la línea del directorio de trabajo, que será por ejemplo:
    workingdir=C:\Archivosdeprograma\Dynamips\sample_labs\simple1
    c. Añadimos un router, le damos un número de consola para configurarlo y asignamos las interfaces. Quedará como el ejemplo:
    [[ROUTER R1]]
    console = 2001
    f0/0 = NIO_gen_eth:\Device\...
    f0/1 = NIO_gen_eth:\Device\...

6. Si no tenemos telnet activado en Windows lo activamos yendo a Panel de control\Programas\Activar o desactivar características de Windows y marcamos Cliente Telnet.
    a. En Windows 7 de 64 bits hay que copiar el ejecutable de Telnet en C:\ y en la carpeta C:\Windows.

Ejecución:

7. Abrimos el archivo Dynamips Server que está en el escritorio.
8. Abrimos (abrir con dg-local) el Simple1 o el fichero donde hayamos configurado nuestro router.
9. En la ventana de consola Dynagen escribimos: =>start R1, donde R1 será el nombre que hayamos puesto a nuestro router en el archivo de configuración (Simple1).
10. Después, escribimos en la misma venta: =>console R1. Haciendo que se conecte virtualmente por telnet al router que creamos anteriormente
11. Esperamos que arranque el router CISCO y escribimos no a la pregunta sobre la configuración inicial.
12. En la ventana de Dynagen escribimos *idlepc get R1* y al finalizar elegimos la configuración con idlepc más baja marcada con '*'.
13. Ya podemos ejecutar en la ventana de consola Telnet los comandos CLI de CISCO.

Manual de instalación de Nagwin

Nagios es un potente sistema de monitorización que permite identificar y resolver problemas en infraestructuras de red antes de que afecten críticamente al proceso productivo. Monitoriza la red completa para asegurar que el sistema, las aplicaciones, los servicios y los procesos funcionan correctamente. En un evento de fallo, Nagios alerta al personal técnico del problema, permitiendo que reparen la incidencia antes de que sea más grave.

En este trabajo se va a utilizar una versión gratuita que solamente cuenta con el Core de Nagios, teniendo que instalar a parte del cliente la herramienta RRDTool (herramienta para captura de datos y su posterior representación en graficas) y Net-SNMP (aplicación que permite capturar los paquete SNMP que contienen la información de monitorización para que los trate el software gestor).

A continuación se explica la instalación y configuración de Nagwin, cliente para Windows XP y 7 con el Core de Nagios.

1. Descargar Nagwin: https://www.itefix.no/i2/nagwin
2. Instalar Nagwin.
3. Arrancar todos los servicios con Nagwin
    a. Inicio/Panel de control/Herramientas administrativas/Servicios
    b. Iniciar todos los servicios Nagwin
4. Una vez arrancados abrir navegador e ir a localhost
    a. Usuario: *nagiosadmin*
    b. Contraseña: *nagios*

5. Configurar Nagwin:
   a. Modificar/crear en la carpeta *C:\Archivos de programa\ICW\etc\nagios\nagwin el archivo hosts.cfg*
   b. Añadir los hosts usando la plantilla:

      # Define a host for the local machine

      define host{

      use windows-server,host-pnp

      host_name fileserver

      alias fileserver

      address 10.1.1.10

      }
   c. Reiniciar los procesos.

Instalación de RRDTool:

1. Descargar RRDTool: http://oss.oetiker.ch/rrdtool/
2. Instalar RRDTool.

Instalación de Net-SNMP:

1. Descargar Net-SNMP: http://www.net-snmp.org/download.html
2. Instalar Net-SNMP.

Manual de instalación de OpenNMS

Debido a que el sistema monitor y gestor comentado en el punto anterior está más limitado al tener partes de pago, y ya que buscamos abaratar costes se presenta OpenNMS. OpenNMS es un sistema monitor y gestor de base de datos muy potente.

En este apartado se explica la instalación y configuración de este sistema con todos los componentes necesarios para su funcionamiento.

1. Descargar un gestor de base de datos, en este caso usamos PostGre, que es el recomendado por OpenNMS. Se necesita porque aquí será donde se almacenen los usuarios y contraseñas del sistema gestor y los títulos y variables de las gráficas.
   http://www.postgresql.org.es/descargas
2. Descargar Java JDK.
3. Descargar OpenNMS:

http://sourceforge.net/projects/opennms/files/latest/download?source=files

4. Instalar PostGre.
   a. Recordar la contraseña que pongamos.
   b. Desactivar la última casilla, Stack Builder.
5. Instalar JDK.
6. Instalar OpenNMS.
   a. Instalar todos los paquetes.
   b. Datos a introducir:
      i. DataBase host: localhost
      ii. PostgreSql Database Name: opennms
      iii. Database username (administrator): postgres
      iv. Database Password (administrator): ********** (la contraseña a recordar de antes).
      v. Database username (user): opennms
      vi. Database Password (user): opennms

7. Arrancar Opennms.
    a. Ejecutar cmd.
        i. Ir a cd .../bin de la carpeta de opennms.
        ii. Ejecutar: opennms start.
        iii. En el navegador ir a: http://localhost:8980
        iv. En el primer acceso:
            a. Usuario: admin.
            b. Contraseña: admin.

Manual de instalación de Cacti

Cacti es también, como Nagios (Nagwin) y OpenNMS, un sistema de gestión y monitorización de red.

Al igual que OpenNMS necesita una base de datos, RRDTool y SNMP, además necesita PHP. Se pueden instalar todos los componentes por separado como se explica en el manual de OpenNMS, pero en los foros oficiales de Cacti hay una versión para Windows Vista/7/2008/2012 con todos los componentes necesarios.

Esta versión completa contiene:

-Cacti 0.8.8b

-Spine 0.8.8a (x86)

-Apache 2.4.9 VC11 (x86/x64)

-MySQL 5.6.17.0 (x86/x64)

-PHP 5.5.12 VC11 (x86/x64)

-Net-SNMP 5.7.0 (x86/x64)

-RRDTool 1.4.5 VC10 (x86)

Se puede descargar de la URL: http://forums.cacti.net/viewtopic.php?t=14946

Por último, para la instalación de Cacti con los componentes por separado es necesario instalar XAMPP, que será el servidor para poder acceder por interfaz web a Cacti.

Manual de configuración de IPv6 en Windows XP/Debian

- **Windows XP**

Como los PCs del laboratorio tienen Windows XP lo instalo de la siguiente forma (en Windows 7 ya va por defecto):

1. Abrir conexiones de red
2. Haz clic en cualquier conexión de área local y, a continuación, haz clic en Propiedades.
3. Haz clic en Instalar.
4. En el cuadro Seleccione el tipo de componente de red, haz clic en Protocolo y, a continuación, haz clic en Agregar.
5. En el cuadro de diálogo Selecciona Protocolo de Red, haz clic en Microsoft TCP / IP versión 6, a continuación, haz clic en Aceptar.
6. Haz clic en Cerrar para guardar los cambios en la conexión de red.

O bien en CMD escribir:

netsh int ipv6 install

- **Debian**

Primeramente hay que comprobar si el módulo IPv6 está activo. Esta comprobación se realiza con el comando *lsmod.*

En caso de que no esté disponible, se activa con el comando *insmod ipv6*.

Para configurar el direccionamiento IPv6 en Debian se realiza de la siguiente manera:

1. Asignar una dirección IPv6.

ip addr add direccion_ipv6 dev nombre_interfaz

2. Agregar la ruta por defecto y el gateway

ip route add direccion_ipv6/prefijo dev nombre_interfaz
ip route add ::0/0 via direcion_ipv6

Para realizar un túnel con IPv6 en Debian:

ip tunnel add sit1 mode sit remote direccion_ipv4
ip link set sit1 up
ip addr add direccion_ipv6/126 dev sit1
ip route add ::0/0 via direccion_ipv6

Otros comandos de interés que pueden resultar útiles al trabajar con IPv6 son:

netstat -Ainet6 -rn (muestra la tabla de ruteo IPv6)

ping6 (ping)

traceroute6 (traza)

dig -6 (DNS)

Glosario de términos.

DNS	Domain Name System (Sistema de Nombres de Dominio).
DHCP	Dynamic Host Configuration Protocol (Protocolo de Configuración Dinámica de Host).
LDAP	Lightweight Directory Access Protocol (Protocolo Ligero de Acceso a Directorios).
RADIUS	Remote Authentication Dial-In User Service (Servicio de Autenticación de Usuario).
STP	Spanning Tree Protocol.
VLAN	Virtual Local Area Network (Red de Área Local Virtual).
QoS	Quality of Service (Calidad de Servicio).
IPv4	Internet Protocol versión 4.
IPv6	Internet Protocol versión 6.
PyME	Pequeña y Mediana Empresa.
ACL	Access Control List (Lista de Control de Acceso).
ISP	Internet Service Provider (Proveedor de Servicios de Internet).
TTL	Time to Live (Tiempo de Vida).
ARP	Address Resolution Protocol (Protocolo de Resolución de Direcciones).
ADSL	Asymmetric Digital Subscriber Line (Línea Digital Asimétrica de Suscriptor).
VPN	Virtual Private Network (Red Privada Virtual).
MPLS	Multiprotocol Label Switching.
FTTH	Fiber To The Home (Fibra Hasta la Casa).
DMZ	Demilitarized Zone (Zona Desmilitarizada).

HTTP Hypertext Transfer Protocol (Protocolo de Transferencia de Hipertexto).

SMTP Simple Mail Transfer Protocol (Protocolo para la Transferencia Simple de Correo Electrónico).

MAC Media Access Control (Control de Acceso al Medio).

SSID Service Set IDentifier.

AP Access Point (Punto de Acceso).

IOS Internetwork Operating System.

NAT Network Address Translation (Traduccion de Dirección de Red).

VoIP Voice over Internet Protocol (Voz sobre Protocolo de Internet).

SNMP Simple Network Management Protocol (Protocolo Simple de Administración de Red).

LACP Link Aggregation Control Protocol (Protocolo de Control de Agregación de Enlace).

ERPS Ethernet Ring Protection Switching. (Protección de Anillos en Conmutación Ethernet).

LLDP Link Layer Discovery Protocol (Protocolo de Descubrimiento a Nivel de Enlace).

BW Bandwidth (Ancho de Banda).

ICMP Internet Control Message Protocol (Protocolo de Mensajes de Control de Internet).

DSCP Differentiated Services Code Point.

RTP Real-time Transport Protocol (Protocolo de Transporte en Tiempo Real).

RTSP Real Time Streaming Protocol (Protocolo de Streaming en Tiempo Real).

RTCP Real Time Control Protocol (Protocolo de Control en Tiempo Real).

PCI Peripheral Component Interconnect (Interconexión de Componentes Periféricos).

LAN Local Area Network (Red de Área Local).

WAN Wide Area Network (Red de Área Amplia).

CPU Central Processing Unit (Unicdad Central de Procesado).

NAT-PT Network Address Translation/Protocol Translation.