SIMULACIÓN MIGRACIÓN DE CORE DE RED DE OPERADOR

Treball Fi de Grau

Tutor: Antoni Morell Pérez
Integració de xarxes telemàtiques

Autor: Miguel Ángel Martín Sánchez

ÍNDICE

Índice de Figuras

Índice de tablas

1. DESCRIPCIÓN DEL PROYECTO

El proyecto fin de grado pretende demostrar la utilidad de la simulación de entornos y laboratorios antes de aplicar configuraciones de protocolos o nuevas tecnologías en una red en producción. La adquisición de equipos para montar redes de preproducción tiene un coste elevado ya que se deben de comprar equipos con similares características a los de producción.

En este proyecto vamos a simular un entorno de preproducción con elementos virtuales, de tal manera que no sea necesaria la adquisición de equipamiento y que por ejemplo en un ordenador portátil se puedan montar un entorno de preproducción de red sin costes para la empresa.

En el proyecto se describe como simular la aplicación de mejoras en la red de un operador/proveedor local de servicios (internet y televisión) con una red multi-fabricante aprovechando un sistema de preproducción virtual.

La posibilidad de crear entornos de simulación de equipos para preparar la configuración y emular el resultado de nuevos protocolos puede ser una ventaja a la hora de desplegar nuevos proyectos.

Se ha intentado tomar como referencia las distintas tecnologías y entornos estudiados en diversas asignaturas. Por tanto se plantea un supuesto de red de operadora local en una isla conectada mediante cable submarino al proveedor de servicios de la península.

La parte práctica del proyecto consiste en la creación de las configuraciones iniciales para el sistema que utilicen los equipos del proyecto y las configuraciones con las mejoras y nuevos protocolos. Estas configuraciones serán simuladas mediante un entorno virtual donde se pretenden probar los resultados de las mejoras propuestas.

2. OBJETIVOS

El objetivo del proyecto es comprobar si un entorno de laboratorio con equipos virtuales puede ayudar a preparar la configuración de un escenario real.

Con el montaje de un laboratorio con *routers* y *switches* virtuales se va a desplegar una supuesta configuración inicial, desde este punto se van a proponer mejoras e implementarlas en entorno de preproducción. Se pretende demostrar que se pueden realizar configuraciones y realizar pruebas en los equipos virtuales para luego implementarlo en equipos en producción.

Otro punto a destacar es que las redes normalmente no están formadas por equipos de un único fabricante, por eso se hace el esfuerzo por utilizar un entorno con equipos de diversos fabricantes.

Si este proyecto se extrapolase a una empresa, ayudaría a desplegar nuevos servicios o mejoras haciendo pruebas en un entorno de laboratorio muy económico y luego aplicarlo a la red en producción sabiendo que los resultados serán satisfactorios y teniendo el mínimo impacto en su red.

Por tanto el objetivo principal del proyecto fin de grado es intentar comprobar si la simulación de redes tiene utilidad a la hora de planificar la configuración de mejoras en una red real.

3. PLANIFICACIÓN

Se adjunta las capturas de la panificación en Microsoft Project.

Nombre de tarea	Duración	Comienzo	Fin
Simulación Migración de Core de Red de Operador	**86 días**	**sáb 26/09/15**	**vie 22/01/16**
PEC 1: Entrega de la planificación del trabajo	**4 días**	**sáb 26/09/15**	**mié 30/09/15**
Investigación del diseño de redes de proveedor de servicios	1 día	sáb 26/09/15	sáb 26/09/15
Elección del tipo de red para el proyecto	1 día	lun 28/09/15	lun 28/09/15
Comunicación al consultor: titulo, objetivos y resumen	1 día	mar 29/09/15	mar 29/09/15
Creación documento base del proyecto	1 día	mié 30/09/15	mié 30/09/15
PAC 2 : Primera entrega del proyecto	**35 días**	**jue 01/10/15**	**mié 18/11/15**
Recopilación de requisitos de configuración inicial	5 días	jue 01/10/15	mié 07/10/15
Identificación de elementos necesarios	2 días	jue 08/10/15	vie 09/10/15
Investigación de tecnologías a emplear	10 días	lun 12/10/15	vie 23/10/15
Identificar propuestas de mejora	5 días	lun 26/10/15	vie 30/10/15
Boceto de diseño	8 días	lun 02/11/15	mié 11/11/15
Documentación Primera entrega	5 días	jue 12/11/15	mié 18/11/15
PAC 3 : Segunda entrega del proyecto	**20 días**	**jue 19/11/15**	**mié 16/12/15**
Montaje entorno simulación GNS3	5 días	jue 19/11/15	mié 25/11/15
Creación configuraciones entorno inicial y final	2 días	jue 26/11/15	vie 27/11/15
Pruebas en entorno de simulación	5 días	lun 30/11/15	vie 04/12/15
Evaluación de mejoras propuestas	3 días	lun 07/12/15	mié 09/12/15
Maquetación documentación	5 días	jue 10/12/15	mié 16/12/15
Entrega de la memoria final	**18 días**	**jue 17/12/15**	**dom 10/01/16**
Revisión documentación	8 días	jue 17/12/15	lun 28/12/15
Conclusiones	4 días	mar 29/12/15	vie 01/01/16
Memoria final	5 días	lun 04/01/16	vie 08/01/16
Presentación Final	**10 días**	**lun 11/01/16**	**vie 22/01/16**
Creación Presentación	5 días	lun 11/01/16	vie 15/01/16
Tribunal	5 días	lun 18/01/16	vie 22/01/16

Tabla 1 Planificación del proyecto

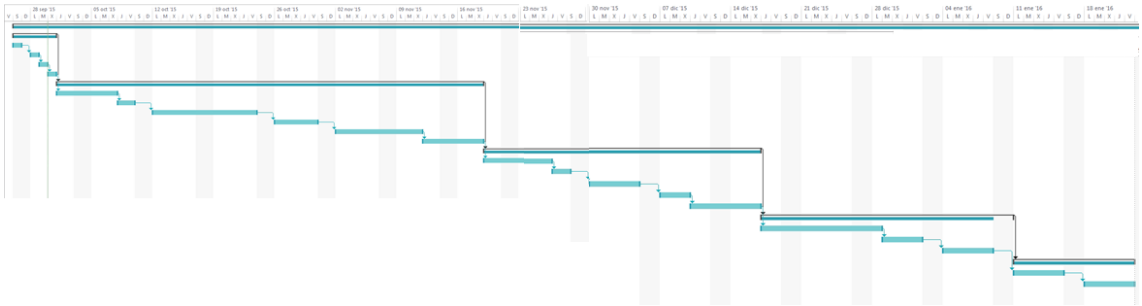

Figura 1: Diagrama de la planificación del proyecto

4. SIGLAS USADAS EN EL PROYECTO

Se recogen las siglas usadas en el proyecto:

CPD: Centro de Procesamiento de Datos

IP: *Internet Protocol*

OSI: *Open System Interconnection*

SONET: *Synchronous Optical Network*

SDH: *Synchronous Digital Hierarchy*

POTS: *Plain Old Telephone Service*

RDSI: Red Digital de Servicios Integrados

BGP: *Border Gateway Protocol*

ISP: *Internet service provider*

EGP: *Exterior Gateway Protocol*

IGP: *Interior Gateway Protocol*

RIP: *Routing Information Protocol*

OSPF: *Open Shortest Path First*

EIGRP: *Enhanced Interior Gateway Routing Protocol*

UDP: *User Datagram Protocol*

RTP: *Real-time Transport Protocol*

IGMP: *Internet Group Management Protocol*

PIM: *Protocol Independent Multicast*

VLAN: *Virtual Local Area Network*

CCITT: Comité Consultivo Internacional Telegráfico y Telefónico

UIT-T: Sector de Normalización de las Telecomunicaciones de la Unión Internacional de Telecomunicaciones

PDH: *Plesiochronous Digital Hierarchy*

STM: *Synchronous Transport Module*

SLTE: *Submarine Line Terminal Equipment*

DWDM: *Dense Wavelength Division Multiplexing*

NPE: *Network Protection Equipment*

WAN: *Wide Area Network*

CPE: *Customer Premises Equipment*

MIC: *Modular Interface Cards*

VRP: *Versatile Routing Platform*

MAC: *Media Access Control*

HSRP: *Hot Standby Router Protocol*

ICMP: *Internet Control Message Protocol*

5. ARQUITECTURA DE RED

La red propuesta para el proyecto es la de un operador local de televisión e internet. Este tipo de operador normalmente no se conecta directamente a un nodo central de Internet como por ejemplo ESpanix (nodo neutro de Internet donde se conectan las operadoras) sino que necesita de otra operadora para proveer de los servicios a sus abonados.

En este caso se ha decidido por una operadora situada en el entorno singular de una isla. Esto hace que para conectarse a la red de su proveedor haga uso del cable submarino o interoceánico. Este tipo de cable y conexión es común en todo el mundo y hace que tanto islas como continentes estén conectados.

La singularidad de esta red obliga a tener dos Centros de Procesamiento de Datos (CPD) donde instalar su equipamiento principal, uno de ellos en la península para realizar la conexión con su proveedor de servicios y al menos otro en la isla para la interconexión con la península y albergar el resto de equipos principales de su red.

Nos vamos a centrar en elementos principales o centrales de la red que proporcionan la conectividad con el proveedor de servicios y no en los que intercomunican el operador con sus clientes. A continuación aparece el esquema general de la red propuesta:

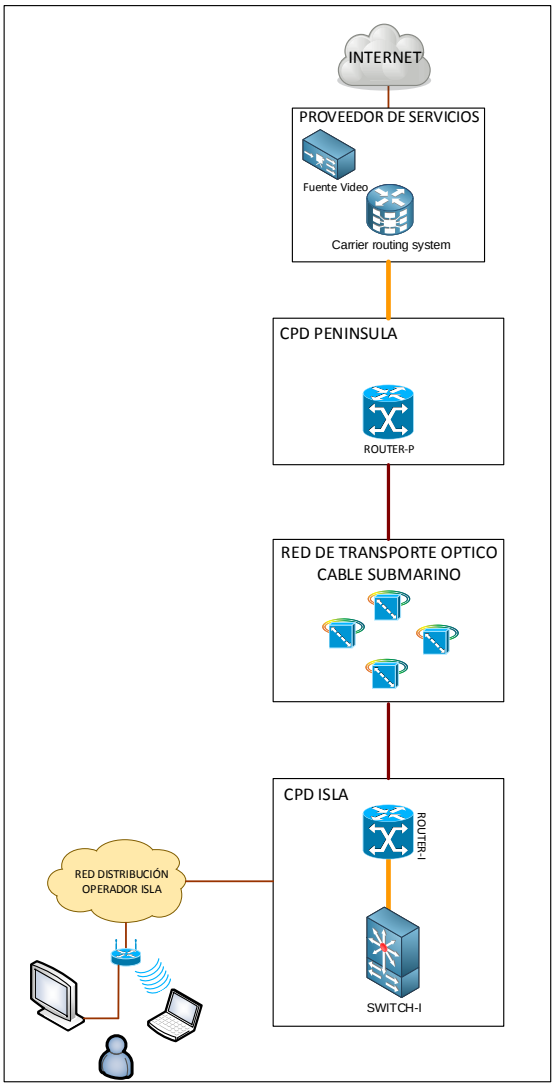

Figura 2: Esquema general de la red

6. SERVICIOS

Como se comenta, una operadora local normalmente no dispone de conexión directa a nodos centrales de Internet sino que lo hace mediante operadores principales que hacen de proveedores de servicios para estas. Es decir, una operadora local debe de hacer uso de la infraestructura de la operadora nacional para recibir los servicios y proporcionárselo a sus clientes finales.

En este proyecto se abordan dos servicios como ejemplo: Internet y televisión.

Para la conexión de la red del operador local y el proveedor de servicios se hace uso de elementos que sean capaces de encaminar el tráfico entre una red y otra; estos elementos son los denominados *routers*.

Estos routers además deben utilizar los protocolos que usan las operadoras para la conexión con los nodos de Internet y en este caso además los protocolos para el transporte de video por red.

Además se debe contar con una red de conmutadores de paquetes o *switches* para el transporte local de los servicios antes de transmitirlos a los clientes finales.

A continuación se hace una descripción de los protocolos que se deberían usar para cada servicio.

6.1. Internet

Para la conexión con los nodos de Internet se suele usar el protocolo *Border Gateway Protocol* (BGP).

BGP es un protocolo mediante el cual se intercambia información de entre sistemas autónomos, en nuestro proyecto un sistema autónomo sería la red del operador local y el otro a unir sería la red del proveedor de servicios.

Entre los sistemas autónomos de los proveedores de servicios de Internet (en inglés ISP) se intercambian sus tablas de rutas a través del protocolo BGP. Este intercambio de información de encaminamiento se hace entre los *routers* externos de cada sistema autónomo, los cuales deben soportar BGP.

La forma de configurar y delimitar la información que contiene e intercambia el protocolo BGP es creando lo que se conoce como sistema autónomo. Cada sistema autónomo (AS) tendrá conexiones o, mejor dicho, sesiones internas (internalBGP) y además sesiones externas (externalBGP).

BGP es un ejemplo de protocolo de *Gateway* exterior (EGP). Lo que hace este protocolo es intercambiar información de encaminamiento entre sistemas autónomos a la vez que garantiza una elección de rutas libres de bucles (un bucle de red hace que el tráfico circule de un *router* a otro de forma cíclica sin encontrar su destino).

BGP Es el protocolo principal de publicación de rutas utilizado por las compañías más importantes de ISP en Internet. A diferencia de los protocolos de *Gateway* internos (IGP), como RIP, OSPF y EIGRP, no usa métricas como número de saltos, ancho de banda, o retardo. BGP toma decisiones de encaminamiento basándose en políticas de la red o reglas que utilizan varios atributos de ruta BGP.

Las relaciones que existen entre distintos sistemas autónomos son principalmente de *peering* (emparejamiento) y de tránsito. Básicamente una relación de tránsito es la que existe entre el proveedor de servicios y el operador local, de modo que el operador pague por los recursos de Internet que le puede suministrar su proveedor. Las relaciones de *peering* proveedores de servicios no suelen ser pagadas y consisten en un enlace para comunicar dos sistemas autónomos con el fin de reducir costes, latencia, pérdida de paquetes y obtener caminos redundantes. Se suele hacer *peering* con sistemas autónomos potencialmente similares, es decir, no se hace *peering* con un cliente potencial ya que saldría uno de los dos sistemas autónomos beneficiado.

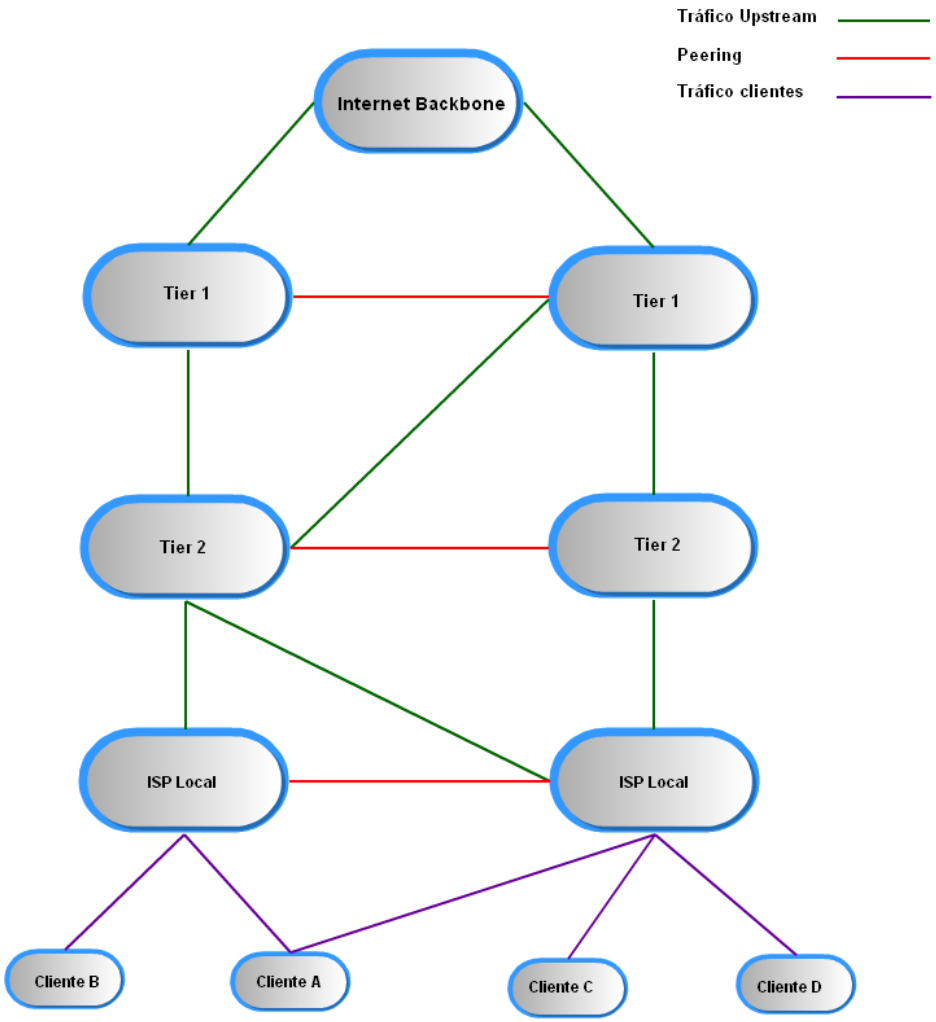

Figura 3: Esquema ejemplo BGP

En la figura se muestra una topología de red con diferentes tipos de relaciones. Los proveedores llamados *Tier* 1 (nivel 1) son los que por definición no pagan a otros proveedores y ofrecen servicio y conectividad a muy larga distancia. Los demás proveedores mostrados pagan al menos el tránsito con un *Tier* 1. Los clientes pagarán a los proveedores con los que tengan un enlace de tránsito.

BGP además permite la agregación de rutas de modo que las rutas manejadas por un *router* en concreto sean las menores posibles.

En nuestro proyecto el *router* del CPD de la península establecería una sesión BGP con el *router* del proveedor de servicios.

6.2. Televisión

Pare proveer de los servicios de televisión por IP se establecerá una comunicación de multidifusión o (*multicast*).

Multidifusión es el envío de la información en múltiples redes a múltiples destinos simultáneamente. En nuestro caso sería la transmisión de los canales de televisión del proveedor desde su *router*, pasando por el resto de *routers* y *switches* de la red, hasta llegar al equipo del cliente final.

Antes del envío de la información, deben establecerse una serie de parámetros. Para poder recibirla, es necesario establecer lo que se denomina "grupo *multicast*". Ese grupo *multicast* tiene asociado una dirección IP. La versión actual del protocolo de internet, conocida como IPv4, reserva las direcciones de tipo D para la multidifusión. Las direcciones IP tienen 32 bits, y las de tipo D son aquellas en las cuales los 4 bits más significativos en binario son '1110' (224.0.0.0 a 239.255.255.255)

Para el escenario propuesto además habrá que usar protocolos para distribuir y encaminar el tráfico IP *Multicast*.

Dado que las transmisiones *multicast* y *unicast* (un único origen a un único destino) son diferentes, sólo los protocolos diseñados para *multicast* pueden ser usados para transmitir los canales desde una fuente de video a múltiples receptores.

La mayoría de los protocolos de aplicaciones existentes que usan *multicast* lo hacen sobre UDP. En el caso del proyecto como lo que se quiere es transmitir contenidos multimedia de televisión, se hace usando el protocolo RTP.

La distribución la red del operador en la isla estará controlada por el protocolo IGMP. Para las comunicaciones entre la isla y la península, así como con el proveedor de servicios se usa el protocolo PIM.

Para encaminar los paquetes entre las diferentes redes utilizaremos Protocol Independent Multicast (PIM), es un Protocolo de encaminamiento que crea una estructura de árbol de distribución entre los clientes *multicast* formando dominios.

Más concretamente el protocolo a usar para el encaminamiento sería PIM *Sparse Mode* ya que viendo los diferentes protocolos, este es eficiente para grupos de *multicast* (un grupo por canal de televisión a transmitir), es eficiente y construye un esquema tipo árbol de cada emisor a receptor en el grupo *multicast*. Utilizando Sparse Mode se ahorra ancho de banda entre la península y la isla al no propagarse los canales de televisión si ningún usuario lo está viendo.

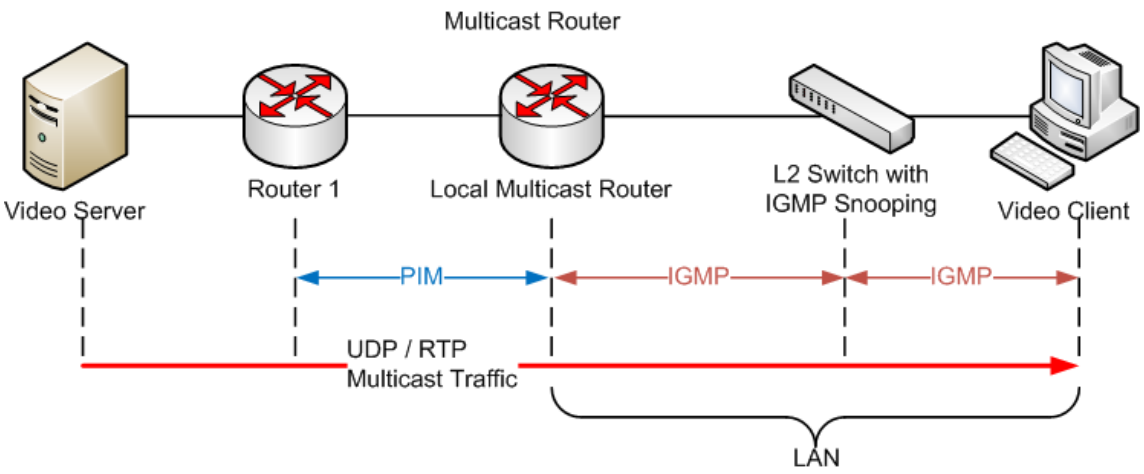

Figura 4: Esquema encaminamiento televisión

En el esquema podemos ver como el tráfico *multicast* RTP pasa desde la fuente de video al cliente final utilizando PIM entre los *routers* del proveedor de servicios y el operador local; para posteriormente usar IGMP en la red del operador local hasta sus clientes.

6.3. Transporte local

Aunque el transporte local no es un servicio en si se ha de tener en cuenta a la hora de transmitir el resto de servicios. La red de transporte en la isla estará compuesta por conmutadores de paquetes o *switches*.

La conmutación de paquetes es un método de envío de datos en una red local sin la intervención de *routers*. La conmutación de paquetes utiliza la capa 2 del Modelo OSI para realizar la distribución de los paquetes a los puertos de los *switches* utilizando las direcciones físicas de los dispositivos.

Un paquete es un grupo de información que consta de dos partes: los datos propiamente dichos y la información de control, que indica la ruta a seguir a lo largo de la red hasta el destino del paquete. Existe un límite superior para el tamaño de los paquetes; si se excede, es necesario dividir el paquete en otros más pequeños. En nuestro caso utilizaremos Ethernet que usa tramas de 1500bytes.

Para el transporte local del operador hay que tener en cuenta:

- Los paquetes forman una cola y se transmiten lo más rápido posible.
- Permiten la conversión en la velocidad de los datos.
- La red puede seguir aceptando datos aunque la transmisión sea lenta.
- Existe la posibilidad de manejar prioridades (si un grupo de información es más importante que los otros, será transmitido antes que dichos otros).

En entornos donde existe una gran cantidad de usuarios/clientes o se quiere dividir el tráfico dentro de un mismo entorno de *switches* se requiere el uso y creación de redes virtuales independientes (VLAN) para contener el tráfico.

En el proyecto propuesto se hace uso de VLAN para dividir el tráfico para los diferentes servicios. A continuación un ejemplo del uso de VLAN:

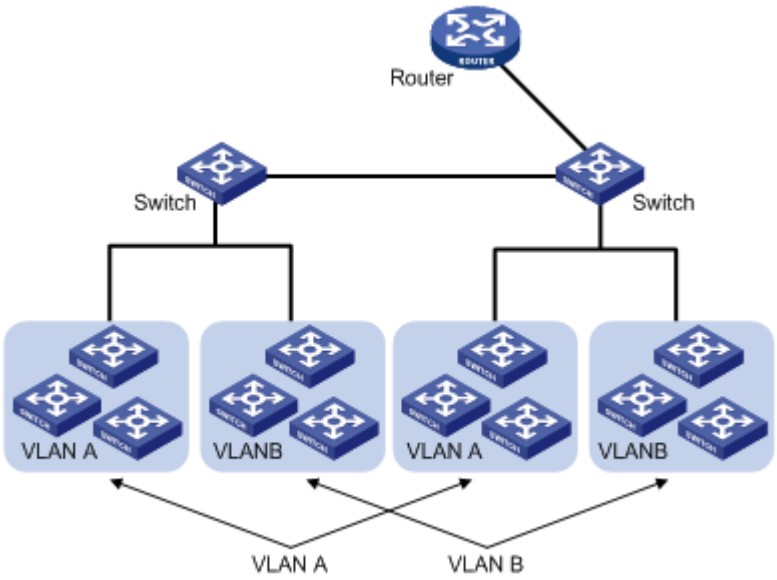

Figura 5: Entorno donde se usa la VLAN

7. CONEXIÓN CABLE SUBMARINO

Al realizar la conexión entre una isla y la península es necesario el uso de alguna técnica poco convencional, para este caso se propone el uso del cable submarino.

Un cable submarino o Interoceánico es aquel cable de cobre o fibra óptica instalado sobre el lecho marino y destinado fundamentalmente a servicios de telecomunicación.

En lo relativo al servicio de telecomunicación los primeros cables, destinados al servicio telegráfico, estaban formados por hilos de cobre recubiertos de un material aislante denominado gutapercha, sistema desarrollado en 1847 por el alemán Werner von Siemens. Con este sistema se logró tender, en 1852, el primer cable submarino que unía el Reino Unido y Francia a través del Canal de la Mancha.

En 1855 se aprobó el proyecto para tender el primer cable trasatlántico que quedó fuera de servicio en poco tiempo. En 1865 se puso en marcha el segundo proyecto, empleándose para ello el mayor barco existente en ese entonces, el Great Eastern. Este cable no llegaría a funcionar hasta el año 1866 y unía Irlanda y Terranova.

Las dificultades de tendido fueron considerables, así como las de explotación, debido a las elevadas atenuaciones que sufrían las señales como consecuencia de la capacitancia entre el conductor activo y tierra, así como por los problemas de aislamiento. Muchos de estos problemas eran ocasionados por los accionistas de las compañías marítimas, introduciendo clavos y perforando así, la capa aislante del cable, se tuvieron que emplear muchos hombres y un trabajo minucioso y a conciencia para poder repararlos. El progreso de éste, era perjudicial económicamente para las compañías navieras.

El descubrimiento de aislantes plásticos posibilitó la construcción de cables submarinos para telefonía, dotados de repetidores amplificadores sumergidos, con suministro de energía a través de los propios conductores por los que se transmitía la conversación.

Posteriormente, en la década de los 60, se instalaron cables submarinos formados por pares coaxiales, que permitían un elevado número de canales telefónicos analógicos, del orden de 120 a 1800, lo que para la época era mucho. Finalmente, los cables submarinos de fibra óptica han posibilitado la transmisión de señales digitales portadoras de voz, datos, televisión, etc. con velocidades de transmisión de hasta 2,5 Gbit/s, lo que equivale a más de 30 000 canales telefónicos de 64 kbit/s.

Figura 6: Componentes del cable submarino

Aunque los satélites de comunicaciones cubren una parte de la demanda de transmisión, especialmente para televisión e Internet, los cables submarinos de fibra óptica siguen siendo la base de la red mundial de telecomunicaciones. Por tanto vemos conveniente el uso de cable submarino para el tipo de red propuesta.

A continuación se puede ver un mapa de Europa y sus cables submarinos.

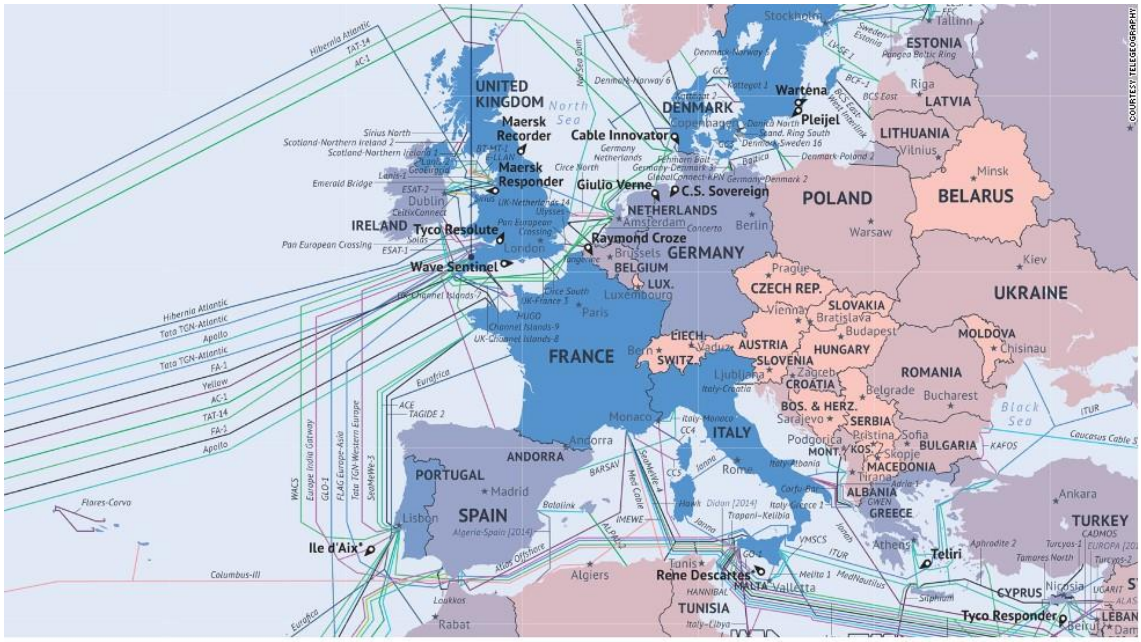

Figura 7: Cable submarino en Europa

7.1. Tecnologias de transmisión por cable submarino

Después de revisar diferentes fuentes sobre la transmisión sobre fibra óptica vemos que uno de los métodos de transmisión usados en el cable submarino es la jerarquía digital síncrona (SDH), por tanto será el empleado en el proyecto propuesto.

SDH es un conjunto de protocolos de transmisión de datos empleados en la comunicación sobre cable submarino. Se puede considerar como la revolución de los sistemas de transmisión, como consecuencia de la utilización de la fibra óptica como medio de transporte de datos, así como de la necesidad de sistemas más flexibles y que soporten anchos de banda elevados. La jerarquía SDH se desarrolló en EE.UU. bajo el nombre de SONET y posteriormente el CCITT (actualmente UIT-T) en 1989 publicó una serie de recomendaciones donde quedaba definida con el nombre de SDH.

Uno de los objetivos de esta jerarquía estaba en el proceso de adaptación del sistema PDH (*Plesiochronous Digital Hierarchy*), ya que el nuevo sistema jerárquico se implantaría paulatinamente y debía convivir con la jerarquía plesiócrona instalada. Ésta es la razón por la que la UIT-T normalizó el proceso de transportar las antiguas tramas en la nueva. La trama básica de SDH es el STM-1 (*Synchronous Transport Module level* 1), con una velocidad de 155 Mbit/s.

Figura 8: Estructura STM-1

Cada trama va encapsulada en un tipo especial de estructura denominado contenedor. Una vez encapsulados se añaden cabeceras de control que identifican el contenido de la estructura (el contenedor) y el conjunto, después de un proceso de multiplexación, se integra dentro de la estructura STM-1. Los niveles superiores se forman a partir de multiplexar a nivel de byte varias estructuras STM-1, dando lugar a los niveles STM-4, STM-16, STM-64 y STM-256.

En nuestro proyecto el supuesto ancho de banda a manejar entre la isla y la península nos hace pensar que un STM-1 no llegaría al mínimo deseable por lo que se propone emplear STM-4.

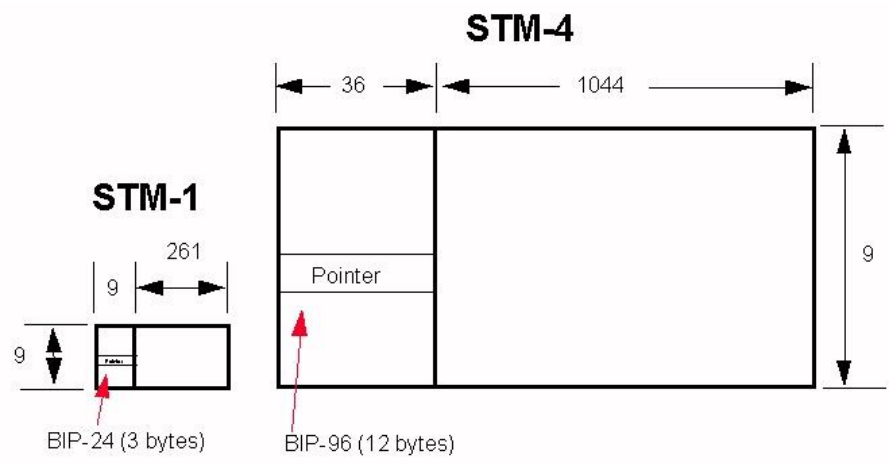

Figura 9: Comparación STM-1 y STM-4

Por tanto si la trama mínima es STM-1 con 155 Mbit/s, al multiplicarlo por cuatro usaremos enlaces de 622 Mbit/s.

8. EQUIPAMIENTO – ROUTERS

Abstrayéndonos del plano de transmisión donde los operadores tienen sus equipos de red ópticos y que ya se han mencionado en otros apartados, lo que interconecta los diferentes entornos son *routers*.

Un *router* es un equipo capaz de encaminar los paquetes de una red de protocolo Internet (IP), estos equipos permiten interconectar los diferentes entornos de nivel 3/red (según modelo OSI). No se entra a comentar protocolos o el propio modelo OSI al no ser la finalidad del proyecto.

Por tanto los *routers* proporcionan la conectividad entre los diferentes CPDs, el proveedor de servicios y los clientes finales.

Existen muchos modelos de *routers* para entornos empresariales, según su función o tipología. Se deben tener en cuenta:

- El volumen de tráfico que tiene que ser capaces de encaminar.
- El número de fuentes de alimentación para proporcionar la suficiente potencia y redundancia en caso de fallo.
- El tipo de interfaces de red que debe soportar
- Los protocolos de red a utilizar

Después de analizar la información sobre el tipo de *router* que tendría que emplearse, parece que el más apropiado sería un *router* con chasis para insertar las tarjetas de línea necesarias, estas tarjetas proporcionan el tipo de puerto necesario para cada tipo de conexión.

8.1. Elección tipo de router

Router con arquitectura de chasis. Un chasis es una estructura donde son ensamblados los componentes de circuitería de los *routers* que proporciona energía y un *backplane* de alta velocidad. Esta estructura de chasis hace que la circuitería quede libre de polvo, humedad y sea más difícil manipular o dañar componentes internos.

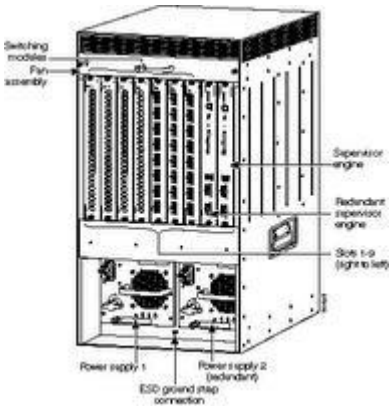

Figura 10: *Router* tipo chasis

El formato chasis permite que este sea un recipiente de distintos componentes, permitiendo configurar el equipo según necesidades, eligiendo número de fuentes de alimentación, tarjetas de línea, etc.

Como se comentaba uno de los componentes más importantes del chasis es el *backplane*, este es una placa de circuitos con los zócalos que permite a las tarjetas supervisoras/procesadoras o módulos que se insertan en estos zócalos y conectarlos entre sí.

Los módulos o tarjetas de línea ofrecen diferentes tipos de interfaces, pero el procesamiento de paquetes se hace generalmente en las tarjetas supervisoras. Así el *backplane* es el medio para el flujo de datos entre los módulos de interfaces y las supervisoras.

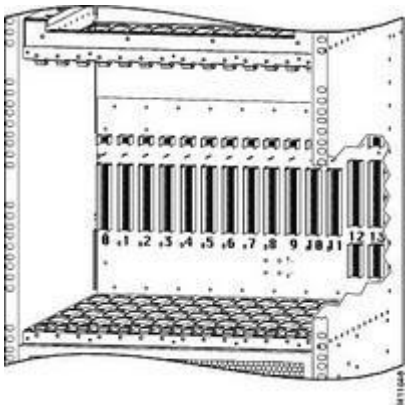

Figura 11: *Router backplane*

Una tarjeta de línea puede proveer diferentes interfaces para dar servicio, por ejemplo SONET/SDH o Ethernet. Algunas tarjetas de línea son capaces de dar más de un tipo de servicio.

La red del proyecto estará compuesta por 2 routers con procesadoras y tarjetería que pueda interconectar mediantes tecnologías de cable submarino la isla con la península. Existen múltiples fabricantes y equipos que cumplen con estos requisitos, nombrar alguno y centrarnos en los que tienen capacidad de emulación con el software GNS3.

8.2. Elección Interfaces interconexión routers

En la elección de los elementos de red hay que tener en cuenta que para la interconexión por cable submarino se usan tecnologías de transmisión por fibra.

En general, el equipo de transmisión utilizado para los sistemas ópticos submarinos de cable está compuesto por SLTE (*Submarine Line Terminal Equipment*) basado en la tecnología DWDM (*Dense Wavelength Division Multiplexing*) y NPE (*Network Protection Equipment*) con protección de línea y funciones de conmutación.

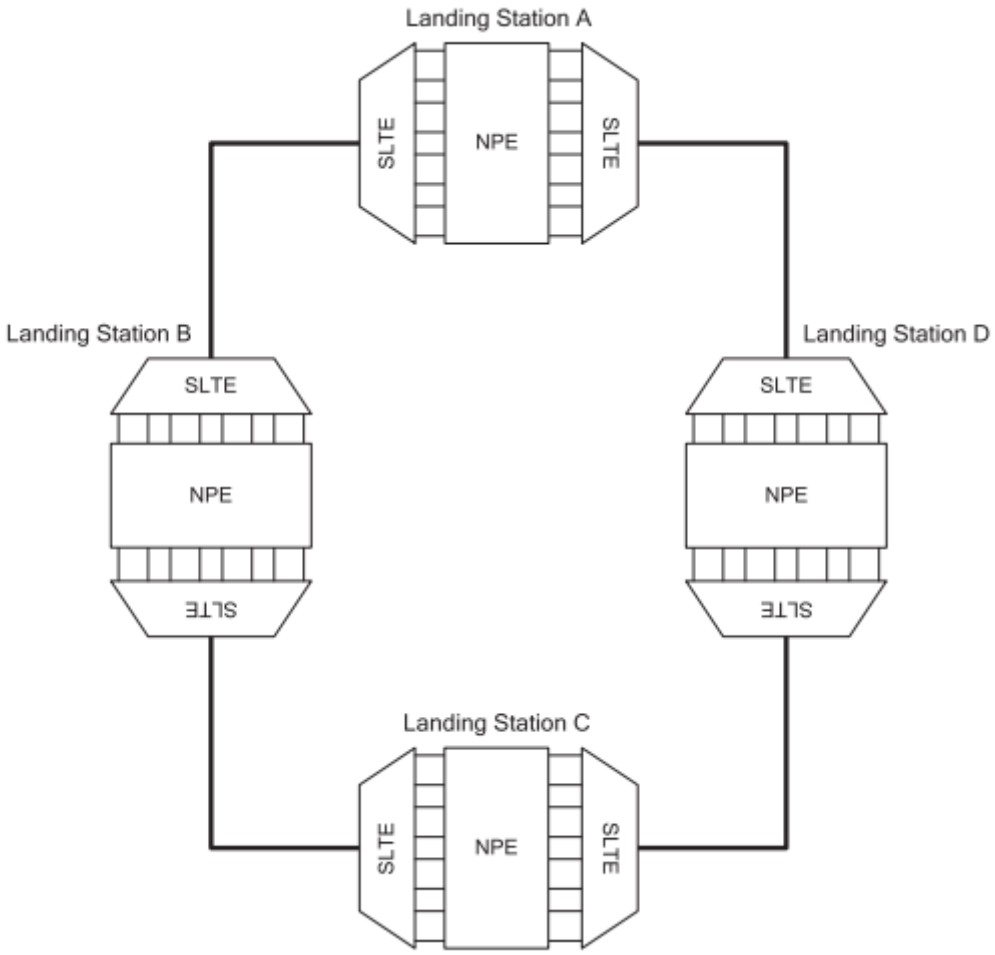

Figura 12: Conexión transmisión

NPE emplea SONET/SDH (Synchronous Optical Network/Synchronous Digital Hierarchy) como tecnología de protección de línea y funciones de conmutación. Estas funciones están contribuyendo en gran medida a la mejora de la disponibilidad y fiabilidad de un sistema de cable óptico submarino. Cuando una línea de transmisión se desconecta debido a un fallo en SLTE o una fibra, la función de conmutación línea de NPE cambia automáticamente la línea de transmisión a una línea de protección preparada. La tecnología SONET/SDH permite ejecutar dicha conmutación de línea en muy poco tiempo (50 a 200 ms), minimizando así los efectos de las interrupciones del tráfico.

Basándonos en estas tecnologías vemos que se ofrecen conexiones STM desde las cabeceras de cable submarino, por tanto los equipos elegidos deben disponer de estas interfaces para comunicar la península con la isla.

El proyecto solo se centra en la red Ethernet, la red de transmisión óptica es un servicio contratado a terceros, por tanto los equipos se conectarán mediante enlaces STM-N/SDH.

8.3. Elección fabricante de *router*

Dentro de las diferentes gamas empresariales de *routers* se analizan las más importantes para la elección del equipamiento que cumplan con las condiciones anteriores:

- Cisco Systems
- Juniper Networks
- Huawei Technologies

8.3.1. Cisco Systems

Cisco Systems es una empresa global con sede en San José, (California, Estados Unidos), principalmente dedicada a la fabricación, venta, mantenimiento y consultoría de equipos de telecomunicaciones. Entre los equipos que fabrica se destacan:

- Dispositivos de conexión para redes informáticas: routers y switches.
- Dispositivos de seguridad como Cortafuegos y Concentradores para VPN.
- Productos de telefonía IP como teléfonos y centralitas VoIP.
- Software de gestión de red.
- Equipos para redes de área de almacenamiento.

Analizando la información obtenida en Internet vemos que es el más extendido y del que más información se dispone, es usado por muchas operadoras en el mundo y tiene equipos que se pueden adaptar a las necesidades del proyecto.

Uno de los equipos que se puede emular para las pruebas sería el Cisco 7200.

El Cisco 7200 VXR Series *Router* ofrece un buen rendimiento/precio, modularidad y escalabilidad en un en un chasis reducido con una amplia gama de opciones de implementación.

Figura 13: Cisco *router*

Es capaz de procesar hasta 2 millones de paquetes por segundo y puede albergar puertos para dar servicio Gigabit Ethernet y SONET/SDH. Es ideal para la agregación servicios WAN/MAN, interconexión de CPDs y para proveedores de servicios que quieran desplegar cualquiera de las siguientes soluciones:

- Conexiones WAN con calidad de servicio.
- Banda Ancha con agregación de 16.000 sesiones por chasis.
- Voz/video/datos
- Gateway
- Seguridad IP de red privada virtual con 5.000 túneles por chasis.
- Uso como Customer Premises Equipment (CPE) para servicios WAN

El Cisco 7200 soporta los requisitos del proyecto mediante:

- Interfaces LAN y WAN
- Interfaces SONET (SDH)
- Interfaces Ethernet

Figura 14: Cisco SDH interface

Como el proyecto dispone de una parte de pruebas de laboratorio virtual la elección está marcada por la compatibilidad con la aplicación GNS3, en este caso se soporta la serie Cisco router 7200. Concretamente soporta el modelo 7206 que dispone de 6 bahías Port Adapters (PA).

Este será el equipo elegido para emular la parte del proveedor de servicios, proporcionando un interface para sus servicios y otro para dar conectividad al operador local.

8.3.2. Juniper Networks

Juniper Networks es una multinacional dedicada a sistemas de redes y seguridad fundada en 1996. Su sede principal está Sunnyvale, California. Es actualmente junto con Extreme Networks, la competencia más directa de Cisco, sobre todo en Europa.

Sus gamas de producto están divididas por tipo de dispositivo:

- Routers:
    - Serie BX (Gateways multiacceso)
    - Serie CTP (Plataforma circuito a paquete)
    - Serie J (Routers de servicio)
    - Serie E (Routers de servicio)
    - Serie LN (Routers de seguridad movil)
    - Serie M (Routers de multiservicio)
    - Serie T (Routers de core)

Posee, al igual que Cisco, un sistema operativo propio para sus routers, denominado JunOS. Este sistema se utiliza en los routers, los switches y los dispositivos de seguridad que ofrece Juniper. Lo que hace que se reduzca el tiempo necesario para implementar nuevos servicios y los costes de operación.

Los routers serie M son una plataforma modular, altamente redundante y con todas las funcionalidades necesaria para una empresa proveedora de servicios. Está diseñado para proporcionar la agregación, servicios móviles, alta capacidad para empresas y servicios de

acceso residenciales, así como para ofrecer servicios de vanguardia para los proveedores de servicios.

Por ejemplo la plataforma MX104 ofrece 80 Gbps de capacidad con cuatro puertos de 10 GbE fijos y cuatro bahías para tarjetas de línea (MIC). Está optimizado para el despliegue de conectividad entre CPDs, apoya un plano de control redundante para alta disponibilidad con dos procesadoras, y su chasis es de altas capacidades para todo tipo de entornos.

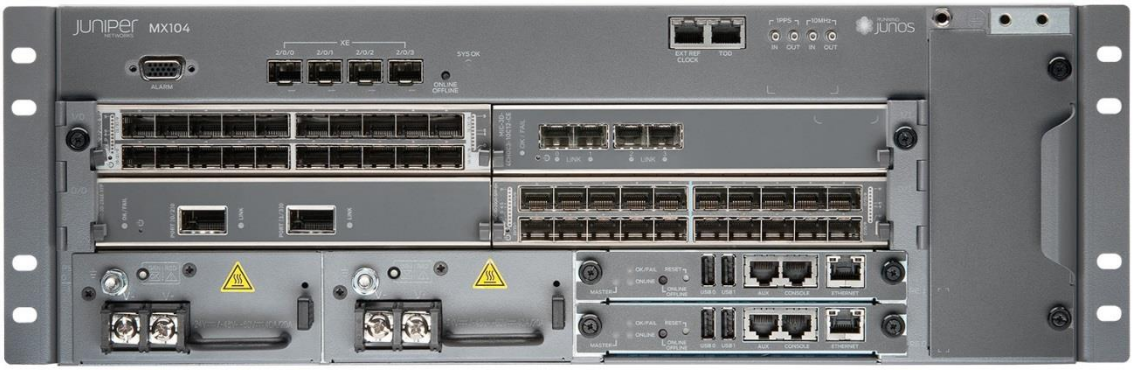

Figura 15: *Router* Juniper

Los *router* de Juniper soportan interfaces SONET/SDH, por ejemplo se puede utilizar una tarjeta de línea de 4 puertos: 4 OC3 / STM1 o puertos / STM4 OC12

Cada puerto se puede configurar con los estándares STM-1, STM-4 o STM-16.

Figura 16: Juniper SDH interface

Con respecto a la emulación de GNS3, los *router* Juniper usan el sistema operativo JunOS que está basado en FreeBSD, este es un sistema UNIX que puede ser ejecutado en cualquier PC. Las versiones de JunOS para la familia Juniper M están oficialmente soportadas por GNS3.

8.3.3. Huawei

Huawei Technologies Co. Ltd. es una empresa privada multinacional china de alta tecnología que se especializa en investigación y desarrollo (I+D), producción y marketing de equipamiento de comunicaciones y provee soluciones de redes personalizadas para operadores de la industria de telecomunicaciones.

De sus diversos productos para el proyecto la línea de *routers* AT cumple con los requisitos propuestos. El router de la serie AR es el router de gama alta para las redes de comunicación de

datos de telecomunicaciones. Puede ser desplegado como un router en el núcleo IP y redes metro. Proporciona a los operadores servicios para el aumento de ancho de banda de la red.

Por sus características podría usarse el router AR3200; son *routers* de clase empresarial de próxima generación basados la plataforma de encaminamiento desarrollada por Huawei (VRP), muy potentes y útiles en este tipo de entorno. Su chasis modular permite a los clientes elegir entre dos tarjetas de control principales y nueve tarjetas de línea que proporcionan una amplia gama de opciones de servicio y rendimiento.

En el proyecto se descarta el uso de este fabricante al no disponer de un emulador compatible con GNS3, pero debido a la importancia en el mercado se hace mención del mismo.

9. EQUIPAMIENTO – SWITCH

La parte de la red local de la operadora en la isla estará compuesta por *switches*.

Un *switch* o conmutador es el dispositivo digital lógico de interconexión de equipos que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más segmentos de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red y eliminando la conexión una vez finalizada esta.

Los conmutadores se utilizan cuando se desea conectar múltiples tramos de una red, fusionándolos en una sola red. Funcionan como un filtro en la red y solo retransmiten la información hacia los tramos en los que hay el destinatario de la trama de red, mejoran el rendimiento y la seguridad de las redes de área local.

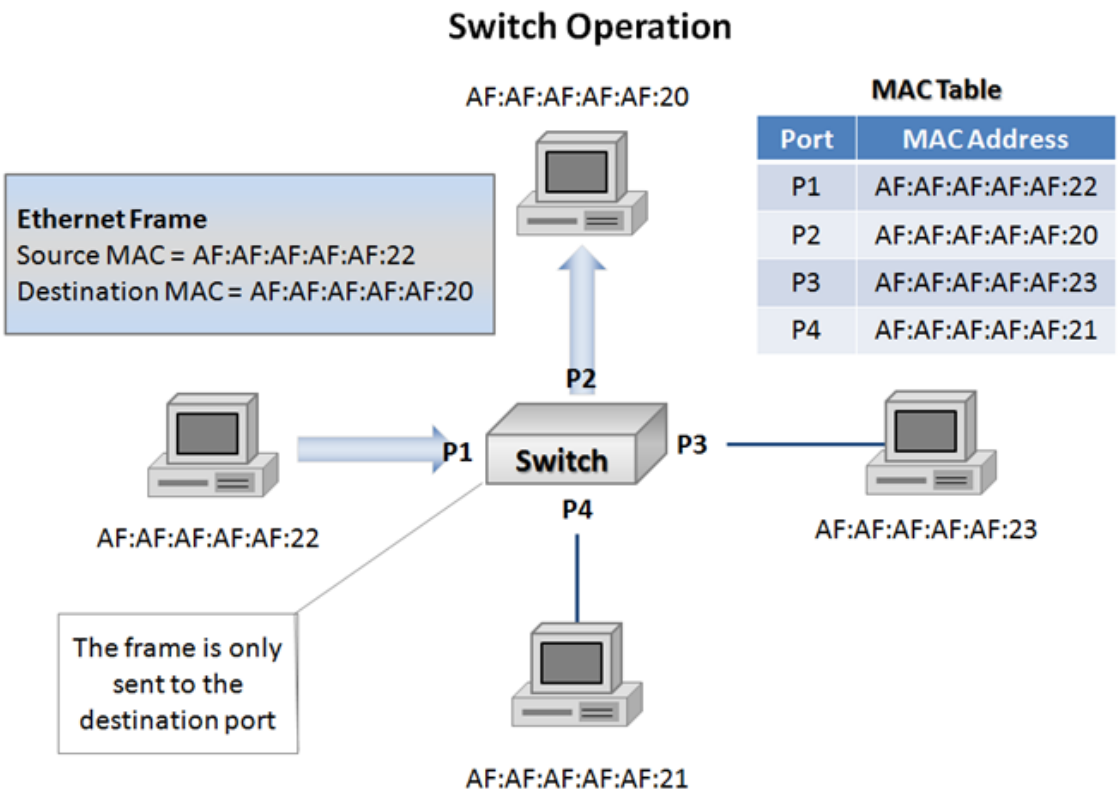

Figura 17: Funcionamiento switch

Dado que uno de los objetivos del proyecto es simular una red multi-fabricante y ya se emplean simulador de Cisco y Juniper se ha optado por la utilización de un *switch* del fabricante Exteme Netwoks.

9.1. Extreme Networks

Extreme Networks es una compañía de ingeniería de redes con sede en San José, California que fue fundada en 1996. Diseña, construye e instala productos para redes Ethernet de empresa u operadoras con una gama de productos muy variada.

Siguiendo los mismos criterios a la hora de elegir los routers de todos los productos de este fabricante, elegiríamos la serie BlackDiamond 8000.

Esta gama de equipos proporciona buena calidad para datos, video y alta densidad puertos Ethernet, Gigabit Ethernet y 10 Gigabit Ethernet según necesidad.

Figura 18: Switch Extreme Networks

Los BlackDiamond 8000 tienen una arquitectura muy simple, son chasis con tarjetas procesadoras y bahías para tarjetas de línea. Sirven como distribución de alto rendimiento para CPD centros de datos y encajan perfectamente con lo propuesto en el proyecto.

Dado que ya disponemos de equipos de otros fabricantes para los routers del proyecto, esta es la elección directa para el switch. Disponen de un sistema operativo basado en UNIX llamado EXOS que puede ser virtualizado y emulado en GNS3.

10. ARQUITECTURA INICIAL

Como arquitectura inicial partimos de una red compuesta por dos CPDs, uno en la península y otro en la isla.

El CPD de la península se conecta al proveedor de servicios y a la red de transporte que incluye el cable submarino, contará con un único router.

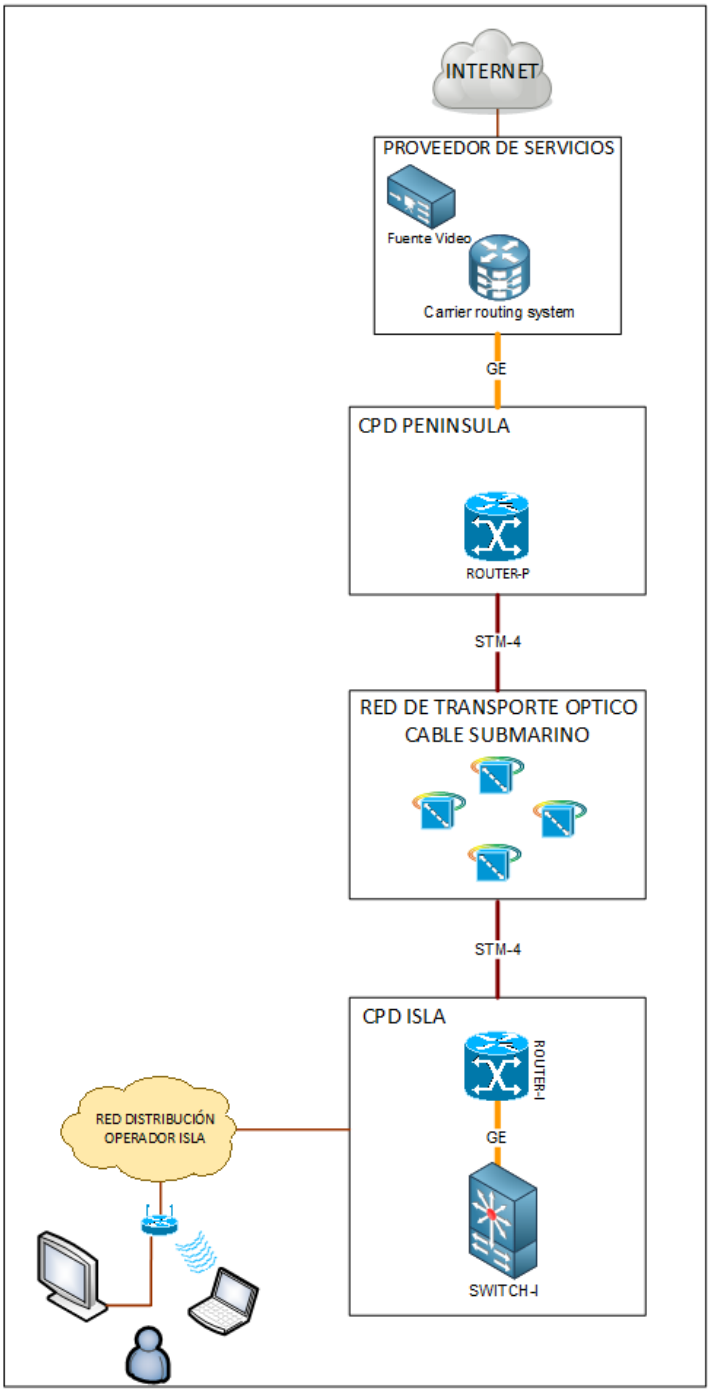

Figura 19: Diagrama inicial de red

El CPD de la isla estará comunicado por un enlace STM-4 a la península mediante los equipos de transmisión óptica del cable submarino. Además en la isla habrá un elemento de conmutación o switch para repartir el tráfico a los diferentes elementos.

Además de los equipos del operador local también prepararemos la configuración de los equipos del proveedor de servicios.

Se usa direccionamiento IPv4 privado, para todas las interconexiones y redes de servicio. Para las redes con posibilidad de múltiples equipos se ha elegido rangos de 254 direcciones, para las redes de interconexión donde solo intervienen las interfaces de los *routers*, se han elegido redes con dos direcciones (enlaces punto a punto).

10.1. Direccionamiento IP

El direccionamiento usado en cada caso será el siguiente:

RED	DIRECCIONAMIENTO	MASCARA	DIRECCIONES
Red Servicios	10.0.0.0	255.255.255.0	254
Interconexión Proveedor	10.1.1.0	255.255.255.252	2
Interconexión Sedes	10.2.2.0	255.255.255.252	2
Sede insular	10.4.4.4.0	255.255.255.252	2
Equipos Clientes	10.5.5.0	255.255.255.0	254
TV Clientes	10.6.6.0	255.255.255.0	254

Tabla 2 Direccionamiento inicial

En una red real existirían mayor número de redes para la escalabilidad de clientes, pero como en el proyecto solo se pretende simular el entorno no es necesario la creación de más redes.

La asignación de direccionamiento en los equipos de red es la siguiente:

EQUIPO	DIRECCIONAMIENTO	Nº INTERFACE	USO
Proveedor de Servicios –R1	10.0.0.1/24	Ethernet 0	Servicios
Proveedor de Servicios –R1	10.1.1.1/30	Ethernet 1	Interconexión Servicios
Router Península – R2	10.1.1.2/30	Ethernet 0	Interconexión Servicios
Router Península – R2	10.2.2.1/30	STM-4 1	Interconexión Isla
Router Isla – R3	10.2.2.2/30	STM-4 1	Interconexión Península
Router Isla – R3	10.4.4.1/30	Ethernet 0	Interconexión red local
Switch Isla – R4-SW	10.4.4.2/30	VLAN 4	Interconexión red local
Switch Isla – R4-SW	10.5.5.1/24	VLAN 5	Red Clientes Internet
Switch Isla – R4-SW	10.6.6.2/24	VLAN 6	Red Clientes Televisión

Tabla 3 Asignación direccionamiento inicial

10.2. Rutas

Al no ser objetivo de este proyecto la configuración de protocolos de encaminamiento se ha optado por simplificar las rutas entre las diferentes redes creando encaminamiento estático.

Estas son las rutas configuradas en los equipos para que exista comunicación entre las diferentes redes:

EQUIPO	DESTINO	VIA
Proveedor de Servicios –R1	10.5.5.0/24	10.1.1.2
Proveedor de Servicios –R1	10.6.6.0/24	10.1.1.2
Router Península – R2	10.0.0.0/24	10.1.1.1
Router Península – R2	10.5.5.0/24	10.2.2.2
Router Península – R2	10.6.6.0/24	10.2.2.2

Router Isla – R3	10.0.0.0/24	10.2.2.1
Router Isla – R3	10.5.5.0/24	10.4.4.2
Router Isla – R3	10.6.6.0/24	10.4.4.2
Switch Isla – R4-SW	Todos	10.4.4.1

Tabla 4 Rutas en los equipos de red

10.3. Configuración Inicial

Con la arquitectura elegida, los equipos de red seleccionada y los diferentes lenguajes de cada sistema se han elaborado las configuraciones de los equipos de red. Cada fabricante usa un sistema operativo diferente por lo que la configuración no es homogénea.

10.3.1. Configuracion Inicial Router Proveedor R1 - Cisco Systems

```
hostname Cisco_R1
!
interface Ethernet0/0
 description RED_SERVICIOS
 ip address 10.0.0.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 description INTERCONEXION_OPERADOR-ISLA
 ip address 10.1.1.1 255.255.255.252
 duplex auto
 speed auto
!
ip classless
ip route 10.5.5.0 255.255.255.0 10.1.1.2
ip route 10.6.6.0 255.255.255.0 10.1.1.2
```

10.3.2. Configuracion Inicial Router Sede Peninsula – Juniper

```
system {
    host-name Juniper_R2;
}
interfaces {
    em0 {
        description INTERCONEXION_PROVEEDOR;
        unit 0 {
            family inet {
                address 10.1.1.2/30;
            }
        }
    }
    em1 {
        description STM-4_1;
        unit 0 {
            family inet {
                address 10.2.2.1/30;
            }
        }
    }
    }
routing-options {
    static {
        route 10.0.0.0/24 next-hop 10.1.1.1;
        route 10.5.5.0/24 next-hop 10.2.2.2;
        route 10.6.6.0/24 next-hop 10.2.2.2;
    }
}
```

10.3.3. Configuracion Inicial Router Sede Isla – Juniper

```
system {
   host-name Juniper_R3;
      }
   interfaces {
   em0 {
      description INTERCONEXION_SWITCH;
      unit 0 {
         family inet {
            address 10.4.4.1/30;
         }
      }
   }
   em1 {
      description STM-4_1;
      unit 0 {
         family inet {
            address 10.2.2.2/30;
         }
      }
   }
   routing-options {
   static {
      route 10.0.0.0/24 next-hop 10.2.2.1;
      route 10.5.5.0/24 next-hop 10.4.4.2;
      route 10.6.6.0/24 next-hop 10.4.4.2;
   }
}
```

10.3.4. Configuracion Inicial Switch Sede Isla – Extreme

```
configure vlan default delete ports all
configure vlan default delete ports 1-3
create vlan "CONEXION_R3"
configure vlan CONEXION_R3 tag 4
create vlan "CLIENTES_TV"
configure vlan CLIENTES_TV tag 6
create vlan "CLIENTES_INTERNET"
configure vlan CLIENTES_INTERNET tag 5
configure vlan CONEXION_R3 add ports 1 untagged
configure vlan CLIENTES_TV add ports 3 untagged
configure vlan CLIENTES_INTERNET add ports 2 untagged
configure vlan CONEXION_R3 ipaddress 10.4.4.2 255.255.255.252
enable ipforwarding vlan CONEXION_R3
configure vlan CLIENTES_INTERNET ipaddress 10.5.5.1 255.255.255.0
enable ipforwarding vlan CLIENTES_INTERNET
configure vlan CLIENTES_TV ipaddress 10.6.6.1 255.255.255.0
enable ipforwarding vlan CLIENTES_TV
#
configure iproute add default 10.4.4.1
#
# Module stp configuration.
#
configure stpd s0 delete vlan default ports all
disable stpd s0 auto-bind vlan default
enable stpd s0 auto-bind vlan Default
configure stpd s0 add vlan CONEXION_R3 ports 1 dot1d
configure stpd s0 add vlan CLIENTES_INTERNET ports 2 dot1d
configure stpd s0 add vlan CLIENTES_TV ports 3 dot1d
```

11. PROPUESTAS DE MEJORA

Después de analizar la arquitectura inicial se detectan puntos de mejoras en la infraestructura.

Si el enlace por cable submarino (STM-4) falla, se pierden todos los servicios. Es recomendable que se contrate un segundo enlace. Para esto además de configurar un segundo interface habría que añadir una segunda ruta y configurar balanceo entre los dos enlaces. De esta manera se dispondría del doble ancho de banda y un enlace secundario en caso de fallo.

Si el router del proveedor de servicios falla, afecta a todo el servicio, por tanto se solicitaría al proveedor que instalase un segundo router de respaldo. Para esto además de configura el segundo router, habría que configurar un protocolo que permitiese balancear la dirección IP del router entre los dos equipos.

11.1. Nuevo Direccionamiento IP

Se amplía la máscara de red de interconexión con el proveedor al aparecer un segundo router y necesitar direccionamiento del mismo rango de red.

Al aparecer una nueva conexión punto a punto entre las dos sedes por medio de cable submarino.

El direccionamiento adicional será el siguiente:

RED	DIRECCIONAMIENTO	MASCARA	DIRECCIONES
Interconexión Proveedor	10.1.1.0	255.255.255.248	6
Interconexión Secundaria Sedes	10.7.7.0	255.255.255.252	2

Tabla 5 Direccionamiento mejoras

Además de los nuevos interfaces STM-4 hay que asignar direccionamiento al nuevo router del proveedor de servicios:

EQUIPO	DIRECCIONAMIENTO	Nº INTERFACE	USO
Proveedor de Servicios –R1	10.0.0.1/24	Virtual	Servicios
Proveedor de Servicios –R1	10.0.0.2/24	Ethernet 0	Servicios
Proveedor de Servicios –R1	10.1.1.1/29	Virtual	Interconexión Servicios
Proveedor de Servicios –R1	10.1.1.3/29	Ethernet 1	Interconexión Servicios
Proveedor de Servicios –R5	10.0.0.1/24	Virtual Respaldo	Servicios
Proveedor de Servicios –R5	10.0.0.3/24	Ethernet 0	Servicios
Proveedor de Servicios –R5	10.1.1.1/29	Virtual Respaldo	Interconexión Servicios
Proveedor de Servicios –R5	10.1.1.4/29	Ethernet 1	Interconexión Servicios
Router Península – R2	10.1.1.2/29	Ethernet 0	Interconexión Servicios
Router Península – R2	10.7.7.1/30	STM-4 2	Interconexión Isla
Router Isla – R3	10.7.7.2/30	STM-4 2	Interconexión Península

Tabla 6 Asignación direccionamiento mejoras

11.2. Rutas

Solo habría que añadir las rutas referentes a los nuevos enlaces STM-4:

EQUIPO	DESTINO	VIA
Router Península – R2	10.5.5.0/24	10.7.7.2
Router Península – R2	10.6.6.0/24	10.7.7.2
Router Isla – R3	10.0.0.0/24	10.7.7.1

Tabla 7 Rutas en los equipos de red

11.3. Configuración Final

Con las mejoras propuestas la creación de la configuración para cada equipo difiere de la inicial. Los cambios más significativos es la aparición de un nuevo router de proveedor junto con un protocolo para la compartición de la IP de la interconexión y el balanceo de encaminamiento entre los dos enlaces STM.

Para la parte de compartición de la IP de interconexión al ser tecnología Cisco se ha configurado el protocolo HSRP.

Para la parte de balanceo de las rutas en los Juniper por los STM se ha elegido el balanceo por paquetes, de esta forma se reparte la carga equitativamente entre los dos enlaces.

En las configuraciones aparecerán en "azul énfasis" lo que se haya modificado.

11.3.1. Configuracion Router Proveedor R1 - Cisco Systems

```
hostname Cisco_R1
!
interface Ethernet0/0
 description RED_SERVICIOS
 ip address 10.0.0.2 255.255.255.0
 duplex auto
 speed auto
standby 10 ip 10.0.0.1
 standby 10 priority 120
 standby 10 preempt
!
```

```
interface FastEthernet0/1
 description INTERCONEXION_OPERADOR-ISLA
 ip address 10.1.1.3 255.255.255.252
 duplex auto
 speed auto
standby 1 ip 10.1.1.1
 standby 1 priority 120
 standby 1 preempt
!
ip classless
ip route 10.5.5.0 255.255.255.0 10.1.1.2
ip route 10.6.6.0 255.255.255.0 10.1.1.2
```

11.3.2. Configuracion Router Proveedor R5 - Cisco Systems

Nuevo equipo del proveedor de servicios.

```
hostname Cisco_R5
!
interface Ethernet0/0
 description RED_SERVICIOS
 ip address 10.0.0.2 255.255.255.0
 duplex auto
 speed auto
standby 10 ip 10.0.0.1
!
interface FastEthernet0/1
 description INTERCONEXION_OPERADOR-ISLA
 ip address 10.1.1.4 255.255.255.252
 duplex auto
 speed auto
standby 10 ip 10.1.1.1
 !
ip classless
ip route 10.5.5.0 255.255.255.0 10.1.1.2
ip route 10.6.6.0 255.255.255.0 10.1.1.2
```

11.3.3. Configuracion Router Sede Peninsula – Juniper

```
system {
   host-name Juniper_R2;
}
interfaces {
   em0 {
      description INTERCONEXION_PROVEEDOR;
      unit 0 {
         family inet {
            address 10.1.1.2/30;
         }
      }
   }
   em1 {
      description STM-4_1;
      unit 0 {
         family inet {
            address 10.2.2.1/30;
         }
      }
   }
em2 {
      description STM-4_2;
      unit 0 {
         family inet {
            address 10.7.7.1/30;
         }
      }
   }
   }
```

```
routing-options {
   static {
      route 10.0.0.0/24 next-hop 10.1.1.1;
      route 10.5.5.0/24 next-hop 10.2.2.2;
      route 10.6.6.0/24 next-hop 10.2.2.2;
      route 10.5.5.0/24 next-hop 10.7.7.2;
      route 10.6.6.0/24 next-hop 10.7.7.2;
   }
   forwarding-table {
      export POLITICA-BALANCEO;
   }
}
policy-options {
   policy-statement POLITICA-BALANCEO {
      then {
         load-balance per-packet;
      }
   }
}
```

11.3.4. Configuracion Router Sede Isla – Juniper

```
system {
   host-name Juniper_R3;
      }
   interfaces {
   em0 {
      description INTERCONEXION_SWITCH;
      unit 0 {
         family inet {
            address 10.4.4.1/30;
         }
      }
   }
   em1 {
      description STM-4_1;
      unit 0 {
         family inet {
            address 10.2.2.2/30;
         }
      }
   }
em2 {
      description STM-4_2;
      unit 0 {
         family inet {
            address 10.7.7.2/30;
         }
      }
   }
```

```
routing-options {
   static {
      route 10.0.0.0/24 next-hop 10.2.2.1;
      route 10.0.0.0/24 next-hop 10.7.7.1
      route 10.5.5.0/24 next-hop 10.4.4.2;
      route 10.6.6.0/24 next-hop 10.4.4.2;
   }
   forwarding-table {
      export POLITICA-BALANCEO;
   }
}
policy-options {
   policy-statement POLITICA-BALANCEO {
      then {
         load-balance per-packet;
      }
   }
}
```

11.3.5. Configuracion Switch Sede Isla – Extreme

```
configure vlan default delete ports all
configure vlan default delete ports 1-3
create vlan "CONEXION_R3"
configure vlan CONEXION_R3 tag 4
create vlan "CLIENTES_TV"
configure vlan CLIENTES_TV tag 6
create vlan "CLIENTES_INTERNET"
configure vlan CLIENTES_INTERNET tag 5
configure vlan CONEXION_R3 add ports 1 untagged
configure vlan CLIENTES_TV add ports 3 untagged
configure vlan CLIENTES_INTERNET add ports 2 untagged
configure vlan CONEXION_R3 ipaddress 10.4.4.2 255.255.255.252
enable ipforwarding vlan CONEXION_R3
configure vlan CLIENTES_INTERNET ipaddress 10.5.5.1 255.255.255.0
enable ipforwarding vlan CLIENTES_INTERNET
configure vlan CLIENTES_TV ipaddress 10.6.6.1 255.255.255.0
enable ipforwarding vlan CLIENTES_TV
#
configure iproute add default 10.4.4.1
#
# Module stp configuration.
#
configure stpd s0 delete vlan default ports all
disable stpd s0 auto-bind vlan default
enable stpd s0 auto-bind vlan Default
configure stpd s0 add vlan CONEXION_R3 ports 1 dot1d
configure stpd s0 add vlan CLIENTES_INTERNET ports 2 dot1d
configure stpd s0 add vlan CLIENTES_TV ports 3 dot1d
```

12. ARQUITECTURA FINAL

La arquitectura final propuesta permite que el servicio no se vea afectado ante la caída de uno de los routers del proveedor o ante el fallo de uno de los enlaces STM entre la isla y la península.

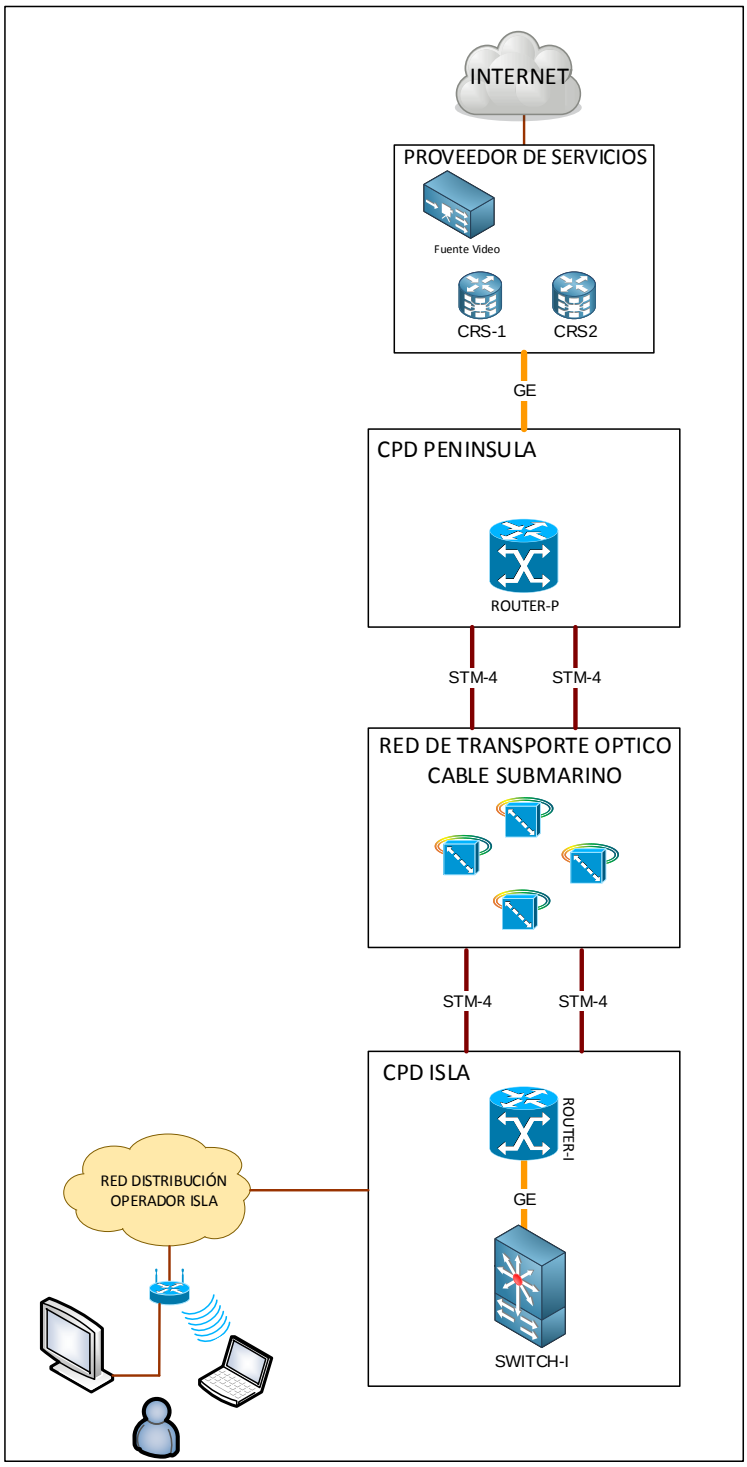

Figura 20: Diagrama final de red

13. MONTAJE LABORATORIO GNS3

GNS3 es un simulador gráfico de red gratuito que te permite diseñar topologías de red complejas y poner en marcha simulaciones sobre ellos.

Para permitir completar simulaciones, GNS3 está estrechamente vinculada con:

- Dynamips, un emulador de IOS que permite a los usuarios ejecutar binarios imágenes IOS de Cisco Systems.
- VirtualBox, para permitir utilizar máquinas virtuales donde corren los sistemas de Juniper o Extreme.

Estas características hacen que sea una herramienta muy potente a la hora de simular redes y concretamente redes multifabricante. En el ANEXO I aparecen los enlaces para su instalación y los requisitos necesarios de GNS3.

Como se comenta también es necesario el uso de VirtualBox para la emulación de sistemas. Para más información consultar ANEXO II.

No es posible simular todos los dispositivos del mercado, como tampoco es posible todos los modelos de hardware de los fabricantes que se pueden simular, por ello se ha elegido equipos que su sistema se puede virtualizar y donde se pueden probar las configuraciones de la propuesta del proyecto. A continuación se muestran los equipos simulados:

Equipo Físico	Función	Equipo virtual	Virtualización
	Servicios	RED_SERVICIOS	Host GNS3
Router Cisco 7200	Proveedor	Cisco_R1 – 3700 12.4(3)	Dynamips IOS
Router Cisco 7200	Proveedor	Cisco_R5 – 3700 12.4(3)	Dynamips IOS
	Servicios	SW1	Ethernet SW GNS3
Router Juniper MX104	Operador	Juniper_R2 – Olive 12.1R1.9	FreeBSD Olive + VirtualBox
Router Juniper MX104	Operador	Juniper_R2 – Olive 12.1R1.9	FreeBSD Olive + VirtualBox
Switch Extreme BD8000	Distribución	ExN_R4-SW - Summit-PC 15.3.1.4	Summit-PC + VirtualBox
	Clientes	RED_CLIENTES	Host GNS3
	Clientes	TV	Host GNS3

Tabla 8 Equipos virtuales

13.1. Pruebas en laboratorio

Se han utilizado las configuraciones propuestas con anterioridad en el sistema GNS3 en los diferentes escenarios propuestos.

Para comprobar que la comunicación es correcta entre las redes de cliente y la red de servicio se usa el protocolo ICMP. Más concretamente la herramienta *ping*, con ella se envían paquetes ICMP de solicitud (ICMP *Echo Request*) y si la otra dirección tiene conectividad, envía de respuesta (ICMP *Echo Reply*). Esta herramienta está disponible en todos los equipos del laboratorio.

Para las conexiones a los equipos con la instalación completa de GNS3 se instala las herramientas de acceso terminal PuTTY y SuperPuTTY. Desde estas herramientas se hace uso de comandos de cada uno de los sistemas para comprobar, rutas, estados y resultados.

13.1.1. Laboratorio Inicial

La siguiente captura muestra el escenario inicial, todos los enlaces activos, con conectividad entre los servicios y las redes de acceso del operador:

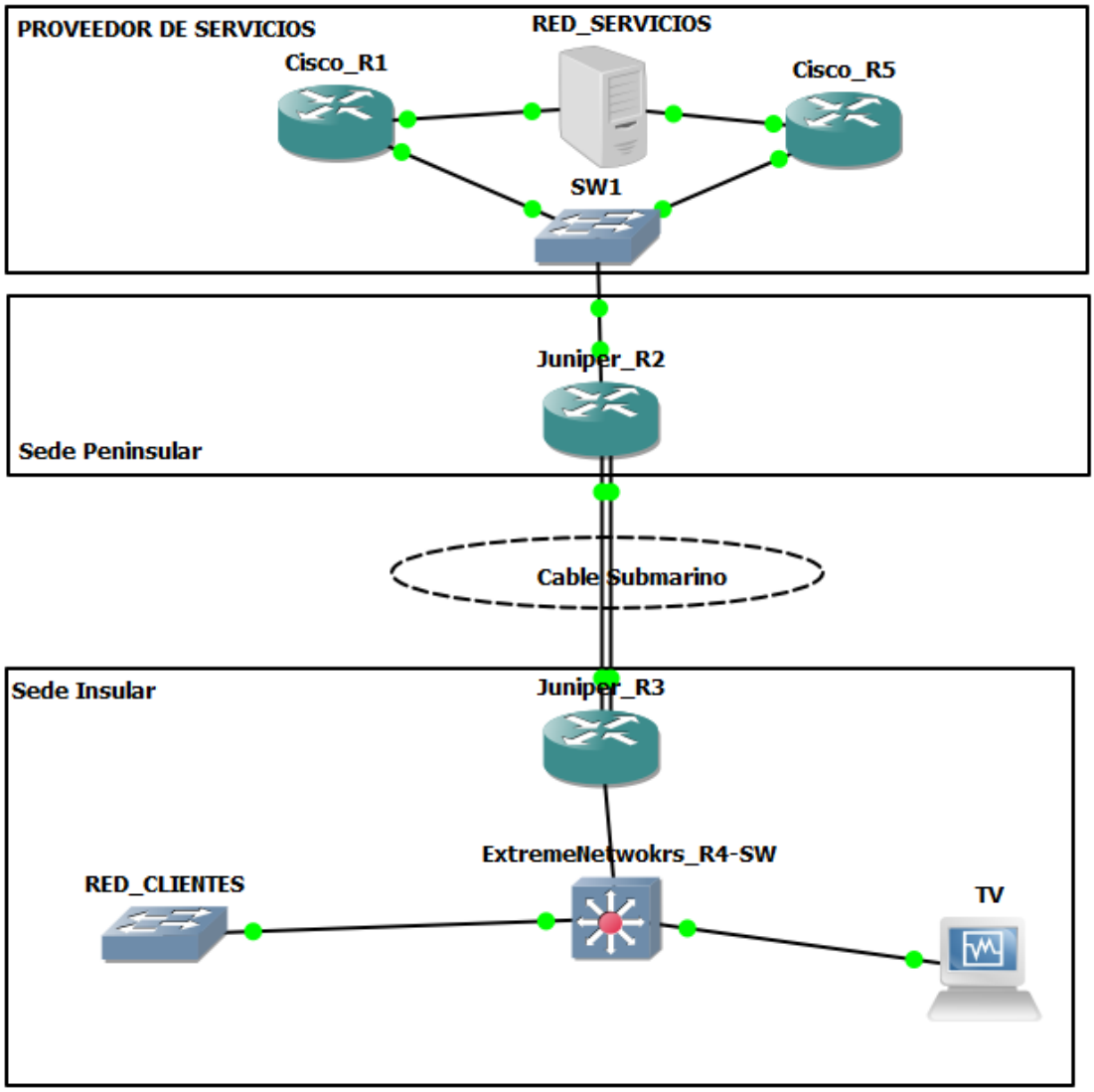

Figura 21: Escenario inicial GNS3

A continuación se muestran las pruebas de conectividad entre todos los segmentos de red.

1. Desde la red de servicios hasta los clientes de Internet:

```
Cisco_R1#ping 10.5.5.1 source 10.0.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.5.5.1, timeout is 2 seconds:
Packet sent with a source address of 10.0.0.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/67/92 ms
Cisco_R1#
```

Figura 22: Ping desde red de servicios a clientes Internet

2. Desde la red de servicios hasta los clientes de TV:

```
Cisco_R1#ping 10.6.6.1 source 10.0.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.6.6.1, timeout is 2 seconds:
Packet sent with a source address of 10.0.0.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/55/68 ms
Cisco_R1#
```

Figura 23: Ping desde red de servicios a clientes TV

3. Desde la red de clientes de Internet a los servicios:

```
ExN_R4-SW.5 # ping 10.0.0.1 from 10.5.5.1
Ping(ICMP) 10.0.0.1: 4 packets, 8 data bytes, interval 1 second(s).
16 bytes from 10.0.0.1: icmp_seq=0 ttl=253 time=10 ms
16 bytes from 10.0.0.1: icmp_seq=1 ttl=253 time=10 ms
16 bytes from 10.0.0.1: icmp_seq=2 ttl=253 time=0.000 ms
16 bytes from 10.0.0.1: icmp_seq=3 ttl=253 time=10 ms

--- 10.0.0.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% loss
round-trip min/avg/max = 0/7/10 ms
ExN_R4-SW.6 #
```

Figura 24: Ping desde red de clientes de Internet a Proveedor de Servicios

4. Desde la red de clientes de TV a los servicios:

```
ExN_R4-SW.6 # ping 10.0.0.1 from 10.6.6.1
Ping(ICMP) 10.0.0.1: 4 packets, 8 data bytes, interval 1 second(s).
16 bytes from 10.0.0.1: icmp_seq=0 ttl=253 time=10 ms
16 bytes from 10.0.0.1: icmp_seq=1 ttl=253 time=10 ms
16 bytes from 10.0.0.1: icmp_seq=2 ttl=253 time=0.000 ms
16 bytes from 10.0.0.1: icmp_seq=3 ttl=253 time=10 ms

--- 10.0.0.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% loss
round-trip min/avg/max = 0/7/10 ms
ExN_R4-SW.7 #
```

Figura 25: Ping desde red de clientes de TV a Proveedor de Servicios

A continuación se muestran los pasos del tráfico por los diferentes routers de la red:

5. Desde la red de servicios hasta los clientes de Internet y TV, pasando por los equipos que simulan estar conectados por el cable submarino, Juniper_R2 y Juniper_R3:

```
Cisco_R1#traceroute 10.5.5.1 source 10.0.0.1

Type escape sequence to abort.
Tracing the route to 10.5.5.1

  1 10.1.1.2 60 msec 32 msec 56 msec
  2 10.2.2.2 32 msec 60 msec 32 msec
  3 10.5.5.1 64 msec 64 msec 40 msec
Cisco_R1#traceroute 10.6.6.1 source 10.0.0.1

Type escape sequence to abort.
Tracing the route to 10.6.6.1

  1 10.1.1.2 28 msec 64 msec 32 msec
  2 10.2.2.2 64 msec 36 msec 64 msec
  3 10.6.6.1 68 msec 64 msec 52 msec
Cisco_R1#
```

Figura 26: Traza desde Proveedor de Servicios a los clientes de TV e Internet

6. Desde las redes de cliente a los servicios, pasando por los equipos que simulan estar conectados por el cable submarino, Juniper_R3 y Juniper_R2:

```
ExN_R4-SW.7 # traceroute 10.0.0.1 from 10.5.5.1
traceroute to 10.0.0.1, 30 hops max
 1  10.4.4.1                                    0 ms        0 ms        0 ms
 2  10.2.2.1                                   10 ms        0 ms        0 ms
 3  10.1.1.4                                   10 ms       10 ms       10 ms

--- Packet Response/Error Flags ---
 (*) No response, (!N) ICMP network unreachable, (!H) ICMP host unreachable,
 (!P) ICMP protocol unreachable, (!F) ICMP fragmentation needed,
 (!S) ICMP source route failed, (!u) Transmit error, network unreachable,
 (!f) Transmit error, fragmentation needed, (!t) General transmit error
ExN_R4-SW.8 # traceroute 10.0.0.1 from 10.6.6.1
traceroute to 10.0.0.1, 30 hops max
 1  10.4.4.1                                    0 ms        0 ms       10 ms
 2  10.2.2.1                                    0 ms       10 ms        0 ms
 3  10.1.1.4                                   10 ms       10 ms       10 ms

--- Packet Response/Error Flags ---
 (*) No response, (!N) ICMP network unreachable, (!H) ICMP host unreachable,
 (!P) ICMP protocol unreachable, (!F) ICMP fragmentation needed,
 (!S) ICMP source route failed, (!u) Transmit error, network unreachable,
 (!f) Transmit error, fragmentation needed, (!t) General transmit error
ExN_R4-SW.9 #
```

Figura 27: Traza desde los clientes de TV e Internet al Proveedor de servicios

13.1.2. Laboratorio Final

El siguiente escenario es el montado después de las propuestas de mejora, de igual forma se proporciona conectividad entre los servicios y las redes del operador en la isla. Además se emplean los protocolos de balanceo por paquetes entre los STM4 y HSRP entre los routers Cisco:

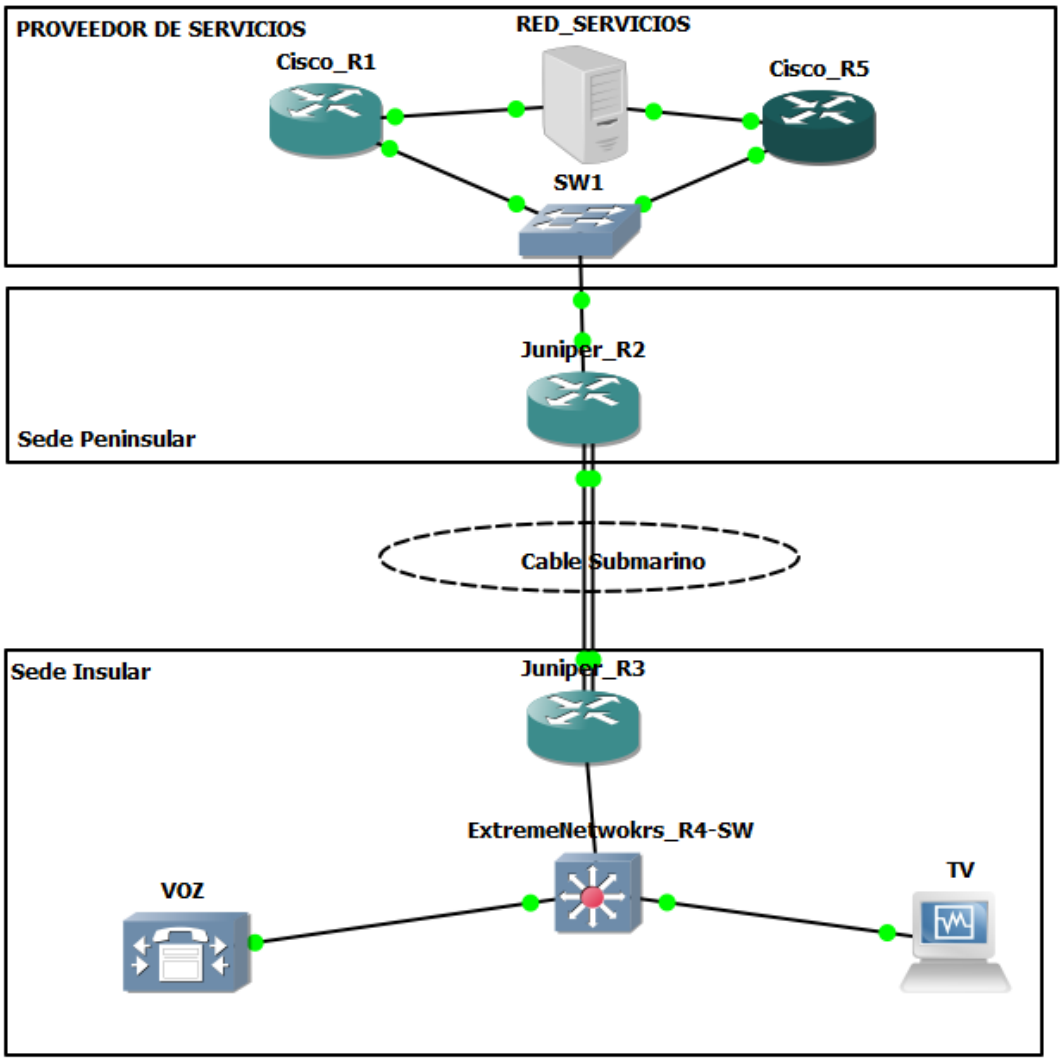

Figura 28: Escenario final GNS3

Una vez modificado el escenario y añadidas las configuraciones del apartado de propuestas de mejora se comprueba que la conectividad es la misma que el laboratorio inicial. Para comprobar las mejoras:

1. Dos conexiones por cable submarino con balanceo de tráfico por paquetes:

1.1. Ver estado de las rutas a los clientes de TV e Internet de R2 por las dos conexiones:

```
root@Juniper_R2> show route forwarding-table destination 10.5.5.0
Routing table: default.inet
Internet:
Destination        Type RtRef Next hop           Type Index NhRef Netif
10.5.5.0/24        user     0                    ulst 131070     3
                              10.2.2.2           ucst   549     3 em1.0
                              10.7.7.2           ucst   559     2 em2.0

Routing table: __master.anon__.inet
Internet:
Destination        Type RtRef Next hop           Type Index NhRef Netif
default            perm     0                    rjct   521     1

root@Juniper_R2> show route forwarding-table destination 10.6.6.0
Routing table: default.inet
Internet:
Destination        Type RtRef Next hop           Type Index NhRef Netif
10.6.6.0/24        user     0                    ulst 131070     3
                              10.2.2.2           ucst   549     3 em1.0
                              10.7.7.2           ucst   559     2 em2.0

Routing table: __master.anon__.inet
Internet:
Destination        Type RtRef Next hop           Type Index NhRef Netif
default            perm     0                    rjct   521     1
```

Figura 29: Estado de las rutas en router de la península del operador local

1.2. Ver estado de las rutas a los servicios de R3 por las dos conexiones:

```
root@Juniper_R3> show route forwarding-table destination 10.0.0.1
Routing table: default.inet
Internet:
Destination        Type RtRef Next hop           Type Index NhRef Netif
10.0.0.0/24        user     0                    ulst 131070     2
                              10.2.2.1           ucst   549     4 em1.0
                              10.7.7.1           ucst   557     2 em2.0

Routing table: __master.anon__.inet
Internet:
Destination        Type RtRef Next hop           Type Index NhRef Netif
default            perm     0                    rjct   525     1

root@Juniper_R3>
```

Figura 30: Estado de las rutas en router de la isla del operador local

1.3. Comprobar que el tráfico se cursa por los dos enlaces de forma balanceada en R3 después de lanzar varios paquetes ICMP desde los clientes finales:

```
root@Juniper_R3> show interfaces em2.0 statistics
  Logical interface em2.0 (Index 69) (SNMP ifIndex 117)
    Flags: SNMP-Traps Encapsulation: ENET2
    Input packets : 76
    Output packets: 71
    Protocol inet, MTU: 1500
      Flags: Sendbcast-pkt-to-re
      Addresses, Flags: Is-Preferred Is-Primary
        Destination: 10.7.7.0/30, Local: 10.7.7.2, Broadcast: 10.7.7.3

root@Juniper_R3> show interfaces em1.0 statistics
  Logical interface em1.0 (Index 68) (SNMP ifIndex 24)
    Flags: SNMP-Traps Encapsulation: ENET2
    Input packets : 71
    Output packets: 75
    Protocol inet, MTU: 1500
      Flags: Sendbcast-pkt-to-re
      Addresses, Flags: Is-Preferred Is-Primary
        Destination: 10.2.2.0/30, Local: 10.2.2.2, Broadcast: 10.2.2.3

root@Juniper_R3>
```

Figura 31: Tráfico balanceado en R3

1.4. Comprobar que el tráfico se cursa por los dos enlaces de forma balanceada en R2 después de lanzar varios paquetes ICMP desde los servicios:

```
root@Juniper_R2> show interfaces em1.0 statistics
  Logical interface em1.0 (Index 68) (SNMP ifIndex 24)
    Flags: SNMP-Traps Encapsulation: ENET2
    Input packets : 45
    Output packets: 42
    Protocol inet, MTU: 1500
      Flags: Sendbcast-pkt-to-re
      Addresses, Flags: Is-Preferred Is-Primary
        Destination: 10.2.2.0/30, Local: 10.2.2.1, Broadcast: 10.2.2.3

root@Juniper_R2> show interfaces em2.0 statistics
  Logical interface em2.0 (Index 69) (SNMP ifIndex 117)
    Flags: SNMP-Traps Encapsulation: ENET2
    Input packets : 43
    Output packets: 45
    Protocol inet, MTU: 1500
      Flags: Sendbcast-pkt-to-re
      Addresses, Flags: Is-Preferred Is-Primary
        Destination: 10.7.7.0/30, Local: 10.7.7.1, Broadcast: 10.7.7.3

root@Juniper_R2>
```

Figura 32: Tráfico balanceado en R2

2. Dos routers de operadora con el protocolo HSRP compartiendo el encaminamiento de forma virtual
   2.1. Si apagamos R1, tras un breve instante R5 toma el control de las direcciones de encaminamiento del proveedor de servicios y apenas se pierden unos paquetes:

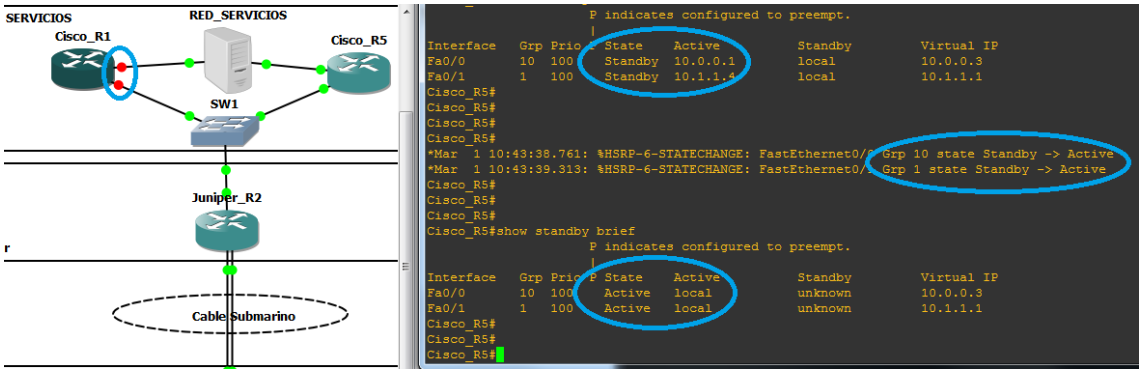

Figura 33: Funcionamiento HSRP en proveedor de servicios

14. DATOS DE SIMULACIÓN

Los datos obtenidos en la simulación demuestran que se cumple el objetivo del proyecto, se pueden utilizar entornos virtuales para probar protocolos, comandos o soluciones a implantar a futuro en una red en producción.

Si bien no es posible probar todas las gamas de producto de los fabricantes elegidos, si es posible realizar pruebas básicas que nos sirven para probar los cambios y adelantarnos a fallos en momentos de aplicación de configuración.

Se ha conseguido comunicar a nivel de red los diferentes elementos de los escenarios, se han podido aplicar los cambios. Se han visto como las mejoras propuestas tienen efecto. Estos datos demuestran que el entorno de simulación valido y se puede utilizar a nivel empresarial.

Si en el escenario final eliminamos uno de los enlaces simulados del cable submarino, no se pierde la comunicación entre el operador y el proveedor de servicios.

Si en el escenario final apagamos alguno de los routers del proveedor de servicios, no se pierde la comunicación entre el operador y el proveedor de servicios.

Con la simulación pude comprobar que los cambios propuestos aportaban las mejoras esperados:

En el caso de la interconexión entre los Juniper además de tener un enlace de respaldo ante fallos se duplicaba el ancho de banda:

Inicial	Ancho de banda	Final	Ancho de banda
1 Enlace STM-4	622 Mbit/s	2 Enlaces STM-4	1244 Mbit/s

Tabla 9 Conclusión Mejora Ancho de banda

Si un canal de TV en HD son 3000Kbps y se emiten 50 canales se reservan mediante mecanismos de calidad de servicio 146.5 Mbit/s.

Si un supuesto cliente medio consume 0.5Mbit/s de forma continua para Internet en la situación inicial se puede dar servicio a unos 950 usuarios (475Mbit/s). De esta forma al incrementar con un STM-4 se podría dar servicio a 2195 usuarios (1097Mbit/s).

En el caso del segundo router de proveedor de servicios según lo propuesto no se ganaría en ancho de banda o número de conexiones, únicamente ante el fallo del router principal tendríamos el otro de respaldo para dar el servicio.

Por tanto en el escenario virtual se han podido simular las propuestas de mejora de forma satisfactoria.

15. VIABILIDAD ECONOMICA

El proyecto tiene una viabilidad económica clara, por un lado la creación del laboratorio virtual no tienen ningún coste, únicamente es necesario un PC con los requisitos mínimos para poder llevar a cabo las pruebas. El software es gratuito (GNS3 y VirtualBox) y por tanto no requiere de ningún coste adicional. Por tanto cualquier empresa podría proporcionar a su departamento de comunicaciones este modelo para realizar pruebas muy reales fuera de la red de producción.

Otro de los aspectos económicos a destacar es la anticipación a futuros fallos, si conseguimos realizar las configuraciones en el entorno de laboratorio antes de llevarlas a producción, podemos detectar si hay algún fallo de configuración, de incompatibilidad, etc. De esta forma se ahorran los costes correspondientes a penalizaciones ante caídas de servicio, quejas de usuarios finales, etc.

Este entorno virtual se puede aprovechar para formar a futuros trabajadores, ahorrando los costes de la adquisición de equipos para formación.

Si se monta un escenario con equipos reales en lugar del laboratorio virtual tendría un coste de varios miles de euros, a este coste habría que sumarle el consumo eléctrico de la maqueta y el espacio necesario para albergarla. Como se quería demostrar la mayoría de pruebas se pueden realizar en un entorno virtual con apenas costes.

Estos aspectos hacen que sea un proyecto viable económicamente, resultando mínimos los gastos en inversión.

16. CONCLUSIONES

Se ha conseguido instalar un entorno de simulación de red con equipos de varios fabricantes. Este entorno es gratuito y permite realizar pruebas de configuraciones, protocolos o nuevos equipos sin alterar una red en producción.

La simulación ha sido muy real ya que se utilizan los sistemas operativos de la electrónica de los diferentes fabricantes en entornos virtuales, no se pueden realizar pruebas de hardware, pero sí de las diferentes características del software.

La interoperabilidad de los diferentes elementos mediante el GNS3 ha sido total, pudiendo interconectar equipos virtuales de diferentes fabricantes, esto resulta muy ventajoso a la hora de evaluar cambios, dispositivos o compatibilidad de equipos.

La limitación más grande es hardware, la herramienta no tiene capacidad para emular switches de Cisco, solo routers y no todos los modelos. Se ha visto que hay fabricantes como Huawei que no tiene modelos para GNS3.

La fiabilidad es muy buena, al ser el mismo software que en el entorno real se pueden probar los comandos, las funcionalidades, la compatibilidad de protocolos entre distintos fabricantes, etc. Incluso se pueden realizar capturas del tráfico para analizar los paquetes según pasan de un elemento a otro.

Lo que hay que tener presente es que no sería viable sustituir un router real por uno virtualizado en GNS3 para un entorno real.

Se puede concluir que al menos con los fabricantes de la propuesta se pueden realizar simulaciones en un entorno virtual, realizar configuraciones, aplicar cambios, simular fallos, etc; todo esto con un bajo coste y con resultados válidos para entornos reales.

17. ABSTRACT

Many large companies support their business over communication networks. Therefore, any network failure can potentially affect the business: production delays, lost transactions, dissatisfied customers, etc. This means that finding a system that anticipates failures or helps plan future deployments, becomes very necessary.

This paper argues that there are tools to help resolve this issue. On one hand, companies save money by not buying real equipment. On the other hand, it allows to make tests without affecting the equipment in service.

The aim is to provide a tool which is simple to install and easy to use that simulates network devices. Specifically, a tool that supports various manufacturers and device models. At the same time, it fulfils the largest companies' requirements while keeping a low cost of implementation.

To do this, a free tool was tested with a simulated enterprise network. GNS3 software - with Dynamips and VirtualBox- was used to make a simulated deployment in a virtual environment. Also, it is important to note that it was analyzed with the software of the most important networking technologies companies - Cisco Systems, Juniper Networks and Extreme Networks-.

As a result, the presented tool demonstrates that it is possible to install a free virtual lab in a simple computer with fully featured of real network devices. Furthermore, it can be extended with other device models and other network protocols that where not part of this paper.

18. REFERENCIAS Y BIBLIOGRAFÍA

ESpanix: http://www.espanix.net/ → volver

Backplane: https://es.wikipedia.org/wiki/Backplane → volver

Sistema Autónomo (BGP): https://es.wikipedia.org/wiki/Sistema_aut%C3%B3nomo → volver

ISP: https://es.wikipedia.org/wiki/Proveedor_de_servicios_de_Internet → volver

EGP: https://es.wikipedia.org/wiki/Exterior_Gateway_Protocol → volver

IGP: https://es.wikipedia.org/wiki/Interior_Gateway_Protocol → volver

IPv4: https://es.wikipedia.org/wiki/IPv4 → volver

UDP: https://es.wikipedia.org/wiki/User_Datagram_Protocol → volver

RTP: https://en.wikipedia.org/wiki/Real-time_Transport_Protocol → volver

IGMP: https://en.wikipedia.org/wiki/Internet_Group_Management_Protocol → volver

PIM: https://en.wikipedia.org/wiki/Protocol_Independent_Multicast→ volver

Modelo OSI: https://es.wikipedia.org/wiki/Modelo_OSI → volver

VLAN: https://es.wikipedia.org/wiki/VLAN→ volver

Tecnologías transmisión cable submarino: → volver

http://www.nec.com/en/global/techrep/journal/g10/n01/pdf/100109.pdf

http://www.mitsubishielectric.com/bu/communication/transmission/wdm/intro.html

http://www.alaskaunited.com/technology/

Dirección MAC: https://es.wikipedia.org/wiki/Direcci%C3%B3n_MAC → volver

Manuales para generar configuración: → volver

Cisco: http://www.cisco.com/c/en/us/td/docs/routers/access/1800/1841/software/configuration/guide/sw/b_cli.pdf

Juniper:

http://www.juniper.net/techpubs/en_US/junos12.1/information-products/topic-collections/swconfig-cli/swconfig-cli.pdf

Extreme Networks:

https://www.extremenetworks.com/wp-content/uploads/2014/01/EXOS_Command_Reference_Guide_15_4.pdf

Cisco HSRP: → volver
http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3560/software/release/12-2_52_se/configuration/guide/3560scg/swhsrp.html

Balanceo por paquetes Juniper: → volver
http://www.juniper.net/documentation/en_US/junos14.1/topics/task/configuration/per-packet-load-balancing-qfx-series.html

ICMP: https://es.wikipedia.org/wiki/Internet_Control_Message_Protocol → volver

PuTTY: https://es.wikipedia.org/wiki/PuTTY → volver

Enlaces a la información necesaria para la elavoracion del proyecto, que sin hacer referencia expresa se utiliza para estructurar o elaborar ideas:

http://ciscorouterswitch.over-blog.com/article-what-is-cisco-chassis-backplane-and-line-card-95760275.html

https://www.grupoice.com/wps/wcm/connect/1ce76680488ea50692409a051eb7cca6/Acceso_capacidades_cables_submarinos_backhaul.pdf?MOD=AJPERES

https://www.movistar.co/documents/10184/299459/OFERTA_COMERCIAL_ACCESO_CABECERAS_CABLES_24112011.pdf/9e5fda6a-983e-4420-b368-ee79e945e84d

http://www.cisco.com/c/en/us/solutions/service-provider/architecture.html

http://www.cisco.com/c/en/us/products/routers/7200-series-routers/index.html

http://www.cisco.com/c/en/us/products/collateral/routers/7200-series-routers/product_data_sheet0900aecd80221d3d.html

https://community.gns3.com/docs/DOC-1708

http://www.juniper.net/us/en/products-services/routing/

http://www.juniper.net/documentation/en_US/junos15.1/topics/concept/interfaces-sonet-sdh-interfaces-overview.html

http://networkengineer.me/2015/03/26/gns3-emulated-hardware-and-faqs/

http://www.juniper.net/techpubs/en_US/release-independent/junos/topics/reference/general/pic-m7i-sonet-oc12c-multirate-sfp.html

http://e.huawei.com/pl/related-page/products/enterprise-network/routers/ar-g3/ar3200/Router_AR3200

ANEXO I.

Como se comenta existen multitud de guías y foros donde se habla sobre la herramienta GNS3.

Estos son los enlaces que he utilizado para montar el laboratorio de simulación:

- Preguntas y respuestas: https://www.gns3.com/software/faq
- Instalación: https://www.gns3.com/support/docs/quick-start-guide-for-windows-us
- Añadir imágenes Cisco: https://www.gns3.com/support/docs/adding-ios-or-iou-qemu-virtual-2
- Como conectar máquinas virtuales de VirtualBox en GNS3: http://www.smartpctricks.com/2014/06/connect-gns3-to-virtualbox.html

Requisitos para la instalación:

Minimum Requirements	
OS	Windows 7 (64 bit) and later, Mavericks (10.9) and later, Any Linux Distro - Debian/Ubuntu are provided and supported
Processor	2 or more Logical cores - AMD-V / RVI Series or Intel VT-X / EPT - virtualization extensions present and enabled in the BIOS. More resources allows for larger simulation
Memory	4 GB RAM
Storage	1 GB available space (Windows Installation is < 200MB
Additional Notes	More storage is needed for OS and Device Images.

Figura 34: Requisitos mínimos GNS3

ANEXO II.

Oracle VM VirtualBox es un software de virtualización para arquitecturas x86/amd64, creado originalmente por la empresa alemana innotek GmbH. Actualmente es desarrollado por Oracle Corporation como parte de su familia de productos de virtualización. Por medio de esta aplicación es posible instalar sistemas operativos adicionales, conocidos como «sistemas invitados», dentro de otro sistema operativo «anfitrión», cada uno con su propio ambiente virtual.

Entre los sistemas operativos soportados (en modo anfitrión) se encuentran GNU/Linux, Mac OS X, OS/2 Warp , Microsoft Windows, y Solaris/OpenSolaris, y dentro de ellos es posible virtualizar los sistemas operativos FreeBSD, GNU/Linux, OpenBSD, OS/2 Warp, Windows, Solaris, MS-DOS y muchos otros.

La aplicación fue inicialmente ofrecida bajo una licencia de software privativo, pero en enero de 2007, después de años de desarrollo, surgió VirtualBox OSE (Open Source Edition) bajo la licencia GPL 2. Actualmente existe la versión privativa Oracle VM VirtualBox, que es gratuita únicamente bajo uso personal o de evaluación, y está sujeta a la licencia de "Uso Personal y de Evaluación VirtualBox" (VirtualBox Personal Use and Evaluation License o PUEL) y la versión Open Source, VirtualBox OSE, que es software libre, sujeta a la licencia GPL.

VirtualBox ofrece algunas funcionalidades interesantes, como la ejecución de máquinas virtuales de forma remota, por medio del Remote Desktop Protocol (RDP), soporte iSCSI, aunque estas opciones no están disponibles en la versión OSE.

En cuanto a la emulación de hardware, los discos duros de los sistemas invitados son almacenados en los sistemas anfitriones como archivos individuales en un contenedor llamado Virtual Disk Image, incompatible con los demás softwares de virtualización.

Otra de las funciones que presenta es la de montar imágenes ISO como unidades virtuales ópticas de CD o DVD, o como un disquete.

Tiene un paquete de controladores que permiten aceleración en 3D, pantalla completa, hasta 4 placas PCI Ethernet (8 si se utiliza la línea de comandos para configurarlas), integración con teclado y ratón.

La guía de instalación usada: https://www.virtualbox.org/manual/ch01.html