ESCUELA TÉCNICA SUPERIOR DE INGENIEROS
INDUSTRIALES Y DE TELECOMUNICACIÓN

UNIVERSIDAD DE CANTABRIA

Proyecto Fin de Carrera

DISEÑO DE UN LABORATORIO DE REDES SOBRE UNA RED TRONCAL ATM Y TECNOLOGÍA DE ACCESO DE USUARIO BASADA EN VLANS

(DESIGN OF A NETWORK LABORATORY OVER AN ATM BACKBONE AND USER ACCESS NETWORK BASED ON VLANS TECHNOLOGY)

Para acceder al Titulo de

INGENIERO DE TELECOMUNICACIÓN

Autor: Eugenio Sánchez Agüera

Julio - 2015

E.T.S. DE INGENIEROS INDUSTRIALES Y DE TELECOMUNICACION

INGENIERÍA DE TELECOMUNICACIÓN

CALIFICACIÓN DEL PROYECTO FIN DE CARRERA

Realizado por: Eugenio Sánchez Agüera
Director del PFC: José Ángel Irastorza Teja
Título: "Diseño de un laboratorio de redes sobre una red troncal ATM y tecnología de acceso de usuario basada en VLANs"
Title: "Design of a network laboratory over an ATM backbone and user access network based on VLANs technology"

Presentado a examen el día: 30 de Julio de 2015

para acceder al Título de

INGENIERO DE TELECOMUNICACIÓN

Composición del Tribunal:
Presidente (Apellidos, Nombre): Marta García Arranz
Secretario (Apellidos, Nombre): José Ángel Irastorza Teja
Vocal (Apellidos, Nombre): Alberto Eloy García Gutiérrez

Este Tribunal ha resuelto otorgar la calificación de: .....

Fdo.: El Presidente

Fdo.: El Secretario

Fdo.: El Vocal

Fdo.: El Director del PFC
(sólo si es distinto del Secretario)

Vº Bº del Subdirector

Proyecto Fin de Carrera Nº
(a asignar por Secretaría)

TÍTULO DEL PROYECTO:

DISEÑO DE UN LABORATORIO DE REDES SOBRE UNA RED TRONCAL ATM Y TECNOLOGÍA DE ACCESO DE USUARIO BASADA EN VLANS

TÉRMINOS CLAVE:

OmniSwitch Alcatel. Conmutación celdas. Conmutación de tramas. Tecnología ATM. VLAN Ethernet. Gestión de red. Simulación de redes.

RESUMEN:

Este proyecto tiene como objetivo el diseño y la implantación de una red dorsal basada en tecnología ATM y la creación de una práctica de laboratorio.

Para ello, se parte de la utilización de una serie de nodos que funcionan como conmutadores de altas prestaciones entre las tramas Ethernet generadas por los usuarios en la parte de acceso y las celdas ATM que viajan por la red dorsal de fibra óptica que interconecta los nodos.

Para comenzar se estudian las posibilidades que ofrecen los nodos Alcatel y se estudia la configuración que presentan al inicio de este proyecto.

A continuación, se estudia la integración de la red dentro del conjunto de redes existentes en el Laboratorio de Telemática y se realizan los cambios de configuración precisos para el correcto funcionamiento del sistema en su conjunto. Además, la red de acceso a usuario de los equipos que conforman el anillo se configura como una serie de VLAN independientes entre sí.

Una vez se finaliza el proceso de configuración de la red, se comprueba el funcionamiento de la misma mediante diferentes herramientas de comunicaciones (hardware y software), y por último, se elabora una práctica de laboratorio destinada para los alumnos de la asignatura de Redes Troncales.

TITLE OF THE PROJECT:

DESIGN OF A NETWORK LABORATORY OVER AN ATM BACKBONE AND USER ACCESS NETWORK BASED ON VLANS TECHNOLOGY

KEY TERMS:

OmniSwitch Alcatel. Cell Switching. Frame Switching. ATM technology. VLAN Ethernet. Network management. Network simulation.

SUMMARY:

The objective of this project is to design and implant a backbone network based on ATM technology and to create a laboratory practice.

For that, the project is based on the use of a group of nodes that works as high performance switches between Ethernet frames generated by users on the access network and ATM cells traveling through the fiber optic backbone network that interconnects the nodes.

The work begins with the study of the possibilities offered by Alcatel nodes and the configuration presented at the beginning of this project.

Coming up next, it follows with the integration of the network in the existing networks of the Telematics Laboratory and performs configuration changes required for the proper functioning of the system as a whole. In addition, the user-access network of devices that forms the physical ring is configured as a series of mutually independent VLAN.

Once the configuration of the network is finished, it is tested to see if it is working properly, using different communication tools (software and hardware) and finally a laboratory practice is elaborated for students of the subject “Redes Troncales”.

AGRADECIMIENTOS

Quiero aprovechar estas líneas para dar mi más sincero agradecimiento a todas las personas que me han apoyado y han estado conmigo a lo largo de estos años de carrera.

En primer lugar, quiero agradecer a mi familia su apoyo y cercanía, en especial a mis padres, sin ellos esto no hubiera sido posible. Quiero agradecerles la confianza que han depositado en mí, y la libertad y facilidades que me han dado para poder estudiar lo que yo quisiera.

Por supuesto, tengo que agradecer a todas las personas, tanto profesores como compañeros, que me han hecho crecer tanto en lo personal como en lo académico, destacando a Sergio, un compañero y amigo con el que he estado la mayor parte de la carrera. Agradecer de igual forma el compromiso y la dedicación (y la paciencia) que ha tenido en todo momento conmigo mi director de proyecto, José Ángel Irastorza.

Por último, pero no por ello menos importantes, agradecer a mis amigos todos los buenos momentos que me hacen pasar y los ratos en los que me ayudan a olvidarme de lo demás por un tiempo. Y a Lucía, que durante estos últimos años me ha animado e insistido para que hiciese un poco más y ha sido una parte fundamental para poder terminar este proyecto.

Muchas gracias a todos.

Índice de Contenidos

Índice de Figuras

Capítulo 1. Introducción

Este apartado introductorio expone las motivaciones y los objetivos perseguidos en la realización del proyecto y analiza la estructura de la memoria, explicando los aspectos fundamentales tratados en sus diferentes capítulos. A continuación, para finalizar este primer epígrafe, se describe la situación de la red sobre la que se trabajará a lo largo de todo el proyecto.

1.1 Motivación y objetivos del proyecto

La idea del proyecto surge de la necesidad de creación de una práctica de laboratorio debido a la detección de carencias de ámbito práctico acerca de determinados protocolos de comunicaciones impartidos de manera teórica durante la carrera. Por esto, con la realización de la práctica se pretende acercar a los alumnos a estas tecnologías y facilitar su aprendizaje.

El objetivo final de este proyecto se basa en la realización de esa práctica de laboratorio enfocada para alumnos de Redes Troncales, asignatura enmarcada en los estudios de Grado en Ingeniería de Tecnologías de Telecomunicación. Se desea que, mediante la utilización de una serie de dispositivos de red cedidos por el Servicio de Informática (ver Anexo I), los alumnos tengan la oportunidad de trabajar y familiarizarse con diversas tecnologías y protocolos de comunicaciones estudiados a lo largo de la carrera. Previamente será necesario configurar estos dispositivos de red, 5 nodos (o dispositivos) de comunicaciones fabricados por Alcatel, que integran las funciones de conmutación necesarias para dirigir el tráfico por la red, y realizar las pruebas de funcionamiento necesarias para comprobar que todo responde correctamente según lo esperado.

Los equipos que se emplean para el desarrollo práctico en el laboratorio formaron parte de la red corporativa universitaria y fueron sustituidos por otros de mejores prestaciones. Pero aunque se hayan quedado algo anticuados tecnológicamente hablando, son idóneos para explicar o aclarar el funcionamiento de diversos protocolos de comunicaciones.

Se pretende que al finalizar la práctica, los alumnos hayan adquirido las siguientes competencias:

- Conocimientos acerca del modo de configuración de la red del Laboratorio de Aplicaciones Telemáticas y su semejanza con la red que antiguamente enlazaba las distintas facultades de la Universidad.

- Entender los conceptos clave de las tecnologías y protocolos de red involucrados en la comunicación.

- Conocer y comprender los métodos de configuración necesarios para poner en funcionamiento la red.

- Manejo de herramientas de gestión de red en un entorno real.

- Manejo de distintas herramientas de comunicaciones (equipos, analizadores, simuladores…) para comprobar el buen funcionamiento de la red.

1.2 Estructura de la memoria

La presente memoria está estructurada en un total de 7 capítulos que engloban el desarrollo del proyecto y una serie de anexos que complementan la información expuesta a lo largo de todos ellos.

En este primer capítulo se aborda la introducción al proyecto, exponiendo su motivación y los objetivos que persigue y se realiza una breve descripción del entorno de trabajo. A continuación, en el segundo apartado, se describen los dispositivos de red con los que se trabaja, particularizando que módulos y funcionalidades incluye cada uno. En el tercero, se introducen los aspectos teóricos necesarios para facilitar la comprensión del documento, describiendo las tecnologías más relevantes que participan en la comunicación y aclarando conceptos necesarios para la comprensión de los apartados posteriores. En los capítulos cuarto y quinto, se exponen los contenidos prácticos desarrollados en el proyecto, es decir, el trabajo realizado en el laboratorio. Estos capítulos englobarán desde el estudio del conexionado y la configuración inicial y final de los nodos, hasta las pruebas de funcionamiento de la red. En el sexto capítulo se expone el guión de la práctica, enfocada para alumnos del laboratorio de telemática, así como los pasos a seguir para su resolución. El séptimo y último punto está pensado a modo de conclusión, y contiene una pequeña recapitulación del trabajo realizado a lo largo del proyecto, las conclusiones obtenidas durante su elaboración y una posible línea futura de trabajo.

Por su parte, los anexos contienen distinta documentación que, por motivos de extensión o relevancia, no es añadida directamente en los capítulos de la memoria, sino que se referencia su consulta a lo largo del presente documento.

1.3 Situación previa: Descripción de la red

En este apartado, se describen tanto la configuración de la red troncal de la Universidad de Cantabria tal y como operaba cuando los nodos estaban implantados en ella, como el esquema de la red global que se presenta en el entorno de los laboratorios de ingeniería telemática.

El emplazamiento principal de la Universidad de Cantabria es el Campus de las Llamas, situado en la Avenida de los Castros de Santander, lugar en el que se ubican el grueso de las facultades y las unidades administrativas de la universidad. Más allá de este campus, la Universidad de Cantabria dispone de diversos edificios y facultades repartidos por otras zonas de Santander, además de otro campus ubicado en Torrelavega. Para conectar todos los edificios y poder gestionar y controlar toda su arquitectura de red, se diseñó una red de comunicaciones que incluyese todos los emplazamientos de la universidad y que emplearía ATM como tecnología de comunicaciones.

En la figura 1.1 aparece una referencia que se hace en la página del Servicio de Informática (SdeI) a los equipos utilizados durante el proyecto, así como una breve descripción del servicio que prestaban [1].

Figura 1.1. Recorte página web Sdel

Según la documentación que el propio Servicio de Informática aporta acerca del conexionado físico de los equipos, la red troncal de la Universidad de Cantabria en Santander se diseñó para que estuviese conformada por una red de campus que, físicamente, constaba de un anillo de fibra óptica a 155 Mbps que enlazaba los edificios de [2]:

Servicio de Informática, Escuela de Náutica, Paraninfo, Escuela de Enfermería y Facultad de Medicina.

Además, contaba con un enlace punto a punto con otro nodo situado en la Facultad de Minas, Torrelavega, y con otro enlace punto a punto entre el Servicio de Informática y la Facultad de Ciencias. Estos dos enlaces no se incluyen en la maqueta que se implementa en este proyecto.

De este modo, trazando la red a utilizar sobre un plano resultaría el esquema que aparece en la figura 1.2.

Figura 1.2. Representación geográfica

En esta red, el Servicio de Informática de la Universidad de Cantabria opera como centro neurálgico de comunicaciones. Se encarga de tareas como instalar, mantener o gestionar la red de comunicaciones de la universidad. Es por este motivo que, a pesar de que la red sea físicamente un anillo, el nodo situado en esta ubicación actúa como nodo central de la red resultando una configuración lógica en forma de estrella.

Tras la actualización de la red UNICAN, los nodos de comunicaciones reemplazados se trasladaron a la Escuela Técnica Superior de Ingenieros Industriales y de Telecomunicación (ETSIIT), concretamente al Laboratorio de Aplicaciones Telemáticas, asignado como laboratorio docente para asignaturas de Ingeniería Telemática. En ese momento se tuvieron que tomar una serie de medidas para incorporar esta nueva red a las otras existentes hasta el momento. Tal como aparece en la figura 1.3, el Laboratorio de Telemática dispone de dos redes de área local (LAN) Ethernet conectadas mediante dos routers a una red de conmutación de paquetes con interfaz de acceso X.25. La red Ethernet 10Base2 utiliza un bus de coaxial fino al que están conectados los adaptadores de red de los PCs, del servidor y del router Cisco2500, constituyendo así un único dominio de colisión. Por otro lado, está la red Ethernet conmutada, basada en una topología de red en estrella que utiliza un cableado de par trenzado UDP (categoría 5) para conectar los adaptadores de red de los PCs, el servidor (Atlas) y el router Cisco2600 a un conmutador Ethernet de 24 puertos. Como el router Cisco 2600 del laboratorio de telemática disponía de una interfaz libre, se optó por conectar la red compuesta por el anillo que forman los nodos a dicha interfaz a través de la interfaz 5/1 del equipo correspondiente al Servicio de Informática. Se configuraron las interfaces para posibilitar la comunicación entre los laboratorios (red 192.168.0.20 /30) y se configuraron los dispositivos del Laboratorio de Telemática necesarios para dar salida a Internet al Laboratorio de Aplicaciones Telemáticas (Router Cisco2600 y Servidor Atlas).

Para ilustrar de forma visual el esquema físico de la red, se presenta la figura 1.3, en la que se ven claramente diferenciados los dos laboratorios telemáticos, el principal, aparece completamente dimensionado mientras que en el Laboratorio de Aplicaciones Telemáticas aparece únicamente su arquitectura física. Una vez finalizada la configuración de esta red, se completarán por tanto los datos que faltan en la figura 1.3, indicando la situación final de las redes que intervienen y el direccionamiento que presentan los dispositivos de red.

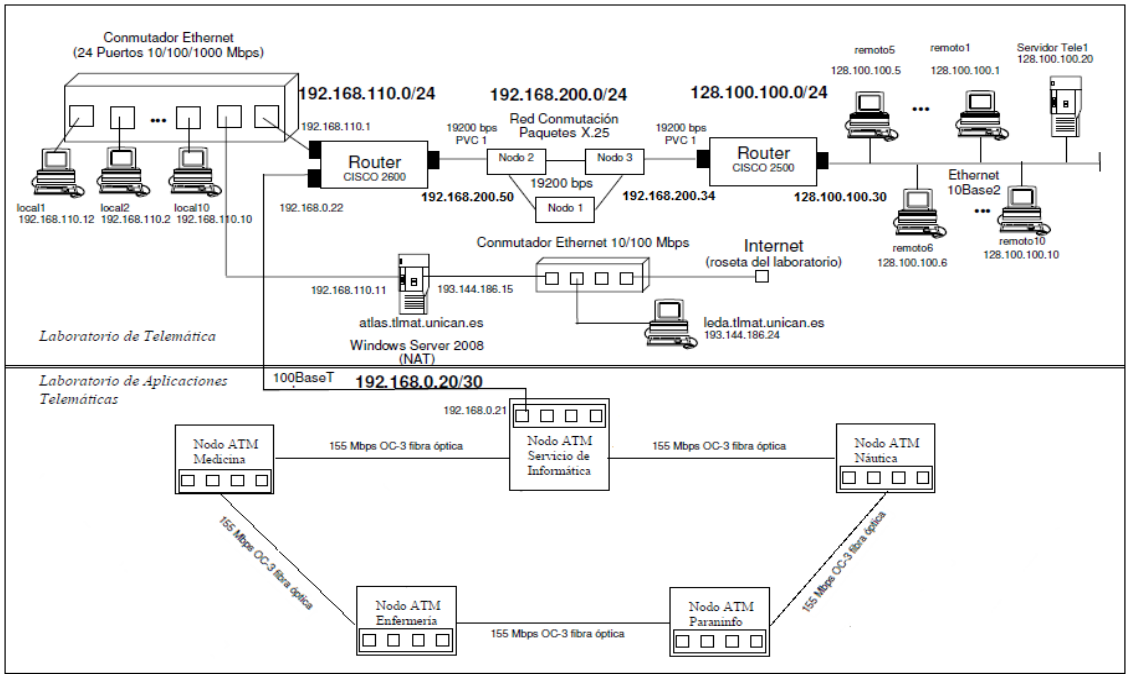


Figura 1.3. Red telemática inicio

Capítulo 2. Descripción de los nodos

En este capítulo se describen los nodos de comunicaciones del fabricante Alcatel, analizando cada uno de los componentes que los integran. La estructura de los nodos se basa en un chasis con slots. En primer lugar se estudia el chasis, comentando su funcionalidad y los modelos presentes. A continuación se analizan los módulos presentes en los slots, comentando en detalle únicamente aquellos que se utilizan. Finalmente, se hace referencia a las fuentes de alimentación que utilizan los nodos.

En el Anexo II pueden encontrarse las hojas de características de los componentes descritos.

2.1 El chasis

El chasis de los nodos alberga los diferentes slots con sus correspondientes módulos funcionales y las fuentes de alimentación. Además, cuenta con un backplane de alta capacidad. En el laboratorio existen dos versiones de chasis, el de la figura 2.1-B con capacidad para albergar 9 slots (Servicio de Informática y Paraninfo) y el de la figura 2.1-A con capacidad para 5 slots (Medicina, Enfermería y Náutica).

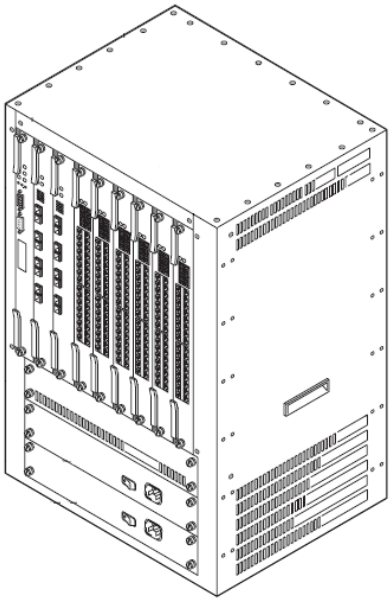


Figura 2.1-B. Chasis de 9 slots

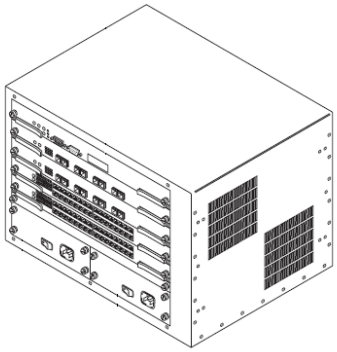


Figura 2.1-A. Chasis de 5 slots

El chasis capaz de alojar 9 módulos presenta un backplane con una capacidad de conmutación de hasta 22Gbps, mientras que el backplane presente en el chasis de 5 módulos posee una capacidad de hasta 12Gbps [3].

La primera ranura del chasis está reservada para el módulo de gestión y, en caso de que sea necesario un módulo de gestión redundante, deberá colocarse en la segunda ranura. El resto de ranuras se ocupan por los diferentes módulos de enrutado. Además, existen dos ranuras especiales para alojar las fuentes de alimentación, una necesaria para el funcionamiento del equipo y la otra, para alojar una fuente redundante en caso de ser precisa. Los equipos del laboratorio presentan una única fuente de alimentación.

2.2 Slots

En lo referente a las ranuras funcionales, por una parte se presentan los slots de gestión y, por otra, los de conmutación.

Para estos equipos, hay un módulo de gestión llamado MPM del que existen varias versiones, aunque sus funciones fundamentales son similares. De los módulos de enrutado existen múltiples ejemplares dependiendo de la tecnología de comunicaciones que se desee implementar. Existen módulos que ofrecen tecnología ATM, y por tanto son los que usan los nodos en nuestra configuración, y otros que soportan tecnologías como Ethernet, Token-Ring, Frame-Relay, FDDI, etc.

Los siguientes apartados se centrarán en describir los módulos utilizados durante el desarrollo del proyecto.

2.2.1 Módulo de gestión o MPM

En cada nodo ha de estar presente, al menos, un módulo de gestión situado en la primera ranura del nodo. Es posible encontrar un segundo slot de gestión si se trabaja con una configuración redundante, robusta ante posibles fallos de funcionamiento del módulo de gestión principal, pero en los equipos del laboratorio, está instalado un solo módulo de gestión. En caso de ser necesario, el módulo de gestión redundante se alojaría en la segunda ranura del chasis [3].

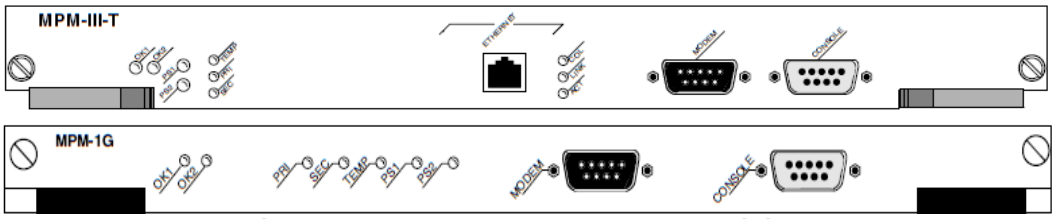


Figura 2.2. Management Processor Modules

Las funcionalidades propias del módulo de gestión son las siguientes:

- Albergar las configuraciones de los diversos módulos de conmutación.
- Realizar funciones básicas de bridging.
- Realizar funciones básicas de routing.
- Albergar el agente SNMP de gestión.
- Proporcionar acceso a la interfaz de configuración de usuario.

Como se puede apreciar en la figura 2.2, los equipos tienen instalados distintos módulos de gestión. El primero, MPM-III-T únicamente aparece en el nodo del SdeI, mientras que el módulo MPM-1G lo incorporan el resto de equipos que forman el anillo.

En la figura 2.2, también se puede ver que el módulo de gestión cuenta con una serie de LED que informan del estado del sistema según el color que presenten [3]:

- OK1: Este LED informa del estado del hardware. De este modo, brilla en color verde cuando el proceso de arranque y diagnóstico ha resultado satisfactorio y

no presenta problemas de funcionamiento. Sin embargo, si se produce un error en la etapa de arranque y diagnóstico, el LED luce en color ámbar. Además, este LED parpadea alternando en color verde y ámbar cuando se lleva a cabo una compresión del sistema de archivos.

- OK2: Este LED informa acerca del estado del Software. A lo largo del proceso de arranque, este LED parpadea en color ámbar para indicar que se está llevando a cabo la carga de software. Si la carga de software se ha realizado satisfactoriamente, brilla en color verde. Si este LED permanece en ámbar durante un periodo prolongado de tiempo se deberá reiniciar el equipo.

- PRI: Este LED luce en verde cuando el slot de gestión al que pertenece realiza las funciones de módulo de gestión primario o bien es el único módulo de gestión instalado.

- SEC: Este LED brilla en verde cuando el módulo de gestión al que pertenece opera como módulo redundante y se encuentra en modo stand-by.

- TEMP: Este LED es el indicador de temperatura del sistema. Luce en ámbar cuando la temperatura se aproxima a los niveles límites de temperatura de operación.

- PS1: Este LED luce en verde cuando el sistema está recibiendo una alimentación adecuada procedente de la fuente de alimentación 1. Si luce en ámbar indica que la fuente de alimentación 1 está conectada pero no suministra la alimentación adecuada. Este LED permanece apagado si la fuente de alimentación 1 está desconectada.

- PS2: Indica lo mismo que el LED PS1, pero referido a la fuente de alimentación número 2.

El puerto Ethernet, el puerto serie o la conexión módem se utilizan para acceder a la interfaz de usuario. Es en esta interfaz de usuario donde se procede a ejecutar los comandos que permiten, tanto visualizar las configuraciones como modificarlas. Además, es posible tanto cargar software de configuración, como descargar los ficheros alojados en la memoria de los equipos utilizando estas interfaces.

2.2.2 Módulo FCSM

Este módulo se encarga de transformar tramas Ethernet en celdas ATM y viceversa mediante conmutación interna tal y como aparece en la figura 2.3.

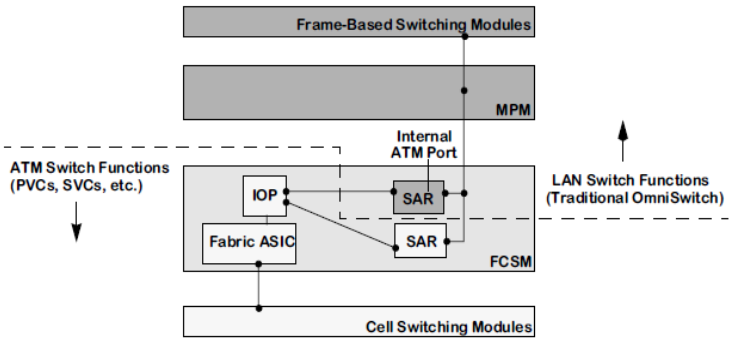


Figura 2.3. Detalle de la conmutación celdas-tramas en el interior del FCSM

De este modo, el tráfico Ethernet generado en un equipo origen, perteneciente a una red de área local, accede a la red troncal como tráfico ATM desde el nodo origen al nodo destino y, en él, vuelve a ser transformado en tráfico Ethernet para entregarlo a la red de área local donde se ubica el equipo destino. Este proceso se muestra de forma esquemática en la figura 2.4.

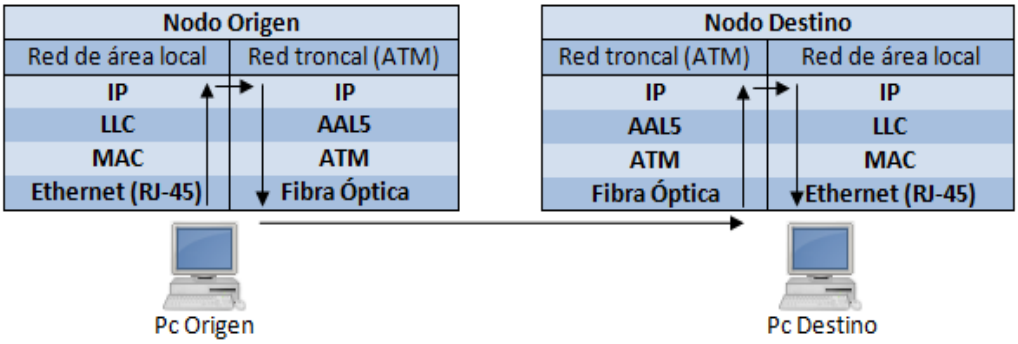


Figura 2.4. Protocolos implicados en la conversión Ethernet-ATM-Ethernet

En la figura 2.5 se muestra el módulo FCSM que incorporan los nodos. Este módulo presenta dos LED, OK1 y OK2, que según su iluminación informan del estado del módulo FCSM y equivalen a los LED de igual etiqueta en el módulo MPM, siendo el primero para realizar un testeo hardware y el segundo para realizar comprobaciones relacionadas con el estado del software. Para su funcionamiento, el módulo FCSM requiere que el módulo de gestión sea MPM-III o MPM-1G.

Figura 2.5. Frame to Cell Switching Module

Se puede concluir que el módulo FCSM posibilita la interconexión LAN-ATM, realizando tareas de fragmentación y reensamblado (SAR) en la conversión entre celdas y tramas.

Aunque el módulo FCSM no posee puertos físicos, sí que posee un puerto interno que puede visualizarse y configurarse mediante software (en los equipos es el puerto 2/1 (slot/puerto)). Se comporta como un puerto externo de ATM conectado a la matriz de conmutación y maneja información de gestión (ILMI, UNI signaling, PNNI). Creando servicios en este puerto, se crea un puente entre equipos conectados a redes nativas ATM y equipos pertenecientes a LAN (Ethernet, Token-Ring…) [3].

2.2.3 Módulo CSM

El módulo de conmutación de celdas contiene las funcionalidades ATM. Aparecen dos clases de módulos CSM durante el desarrollo del proyecto, ambos instalados en el tercer slot:

- El módulo CSM-AB-155F: Presenta dos conectores SC para fibra óptica monomodo a 155 Mbps para dos puertos SONET/SDH full-dúplex. Soporta hasta 4096 VCC punto a punto con un tamaño de buffer de hasta 8192 celdas [3].

  Como se ve en la figura 2.6, cada puerto posee tres LED que indican su estado. De este modo, el LED RED indica si se están recibiendo celdas de

forma correcta, luciendo en color verde si es el caso, o si se están perdiendo celdas de forma persistente o el cable no está conectado si luce en color ámbar. El LED LINK brilla de color verde cuando hay señal presente y el puerto está habilitado. Si el puerto está deshabilitado, este LED permanece apagado. El LED ACT brilla en color verde cuando se transmite o recibe tráfico por el puerto.

El nodo del Servicio de Informática alberga 3 módulos de este tipo (por lo que tiene 6 interfaces), mientras que los demás, únicamente tienen instalado 1 (por lo que tienen 2 interfaces).

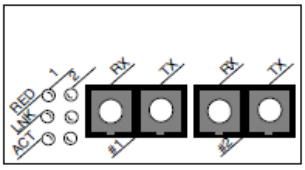


Figura 2.6. CSM-AB-155F

- El módulo CSM-AB-E1 usa conectores RJ48. Recoge tráfico procedente de emulación de circuitos y lo convierte a tráfico ATM. Como aparece en la figura 2.7, cada puerto tiene asociado un LED que indica su estado mediante un código de colores. Así pues, permanece apagado si no hay conexión establecida en el puerto, brilla de color verde cuando hay una conexión establecida, parpadea en este mismo color cuando una transmisión se lleva a cabo y luce de color ámbar cuando se produce un error.

Figura 2.7. CSM-AB-E1

Todos los nodos excepto el SdeI tienen instalado un módulo de este tipo. Se utilizaba cuando los equipos estaban instalados en la red troncal de la Universidad para transmitir el tráfico de voz entre los distintos edificios.

2.2.4 Módulo ESM

Este módulo contiene las funcionalidades propias de Ethernet. Utiliza par trenzado con conectores RJ45 para establecer las conexiones.

Para el desarrollo del proyecto se cuenta en cada nodo con un módulo ESM-100C-32W como el de la figura 2.8, pero como todos los nodos no presentan el mismo chasis, a la hora de asignar puertos es necesario tener en cuenta que este módulo varía de ubicación en función del nodo. Se sitúa en el slot 4 para los nodos de Náutica, Enfermería y Medicina, en el slot 5 del nodo SdeI y en el slot 6 del equipo Paraninfo.

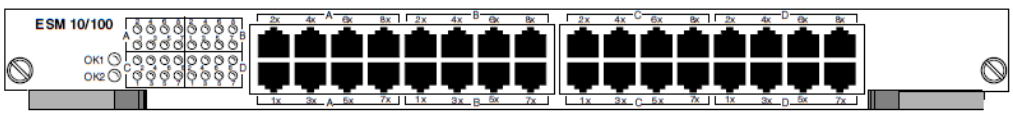


Figura 2.8. ESM 32 puertos

Cada puerto presente en estos módulos puede operar a velocidades de 10Mbps o 100Mbps y puede ser configurado para operar en modo full-dúplex o half-dúplex de forma independiente al resto.

El módulo contiene dos LED que indican su estado y cada puerto, a su vez, posee su propio LED para indicar cómo se encuentra la conexión. De este modo, el significado de los LED es el siguiente [3]:

- OK1: Este LED indica el estado del hardware del módulo, luciendo en color verde cuando se ha llevado a cabo de forma correcta el proceso de arranque y diagnóstico. En caso de que haya sucedido algún error, el LED brilla en ámbar.
- OK2: Indica el estado del software, parpadeando en verde cuando hay una correcta comunicación con el MPM, brillando en color ámbar cuando ocurre algún error y parpadeando en ámbar cuando el sistema se encuentra en un estado transitorio.
- LINK: Para cada puerto, indica que hay una conexión por cable correctamente establecida cuando luce en color verde, si no hay conexión establecida el LED permanece apagado y parpadea cuando el puerto está deshabilitado.
- ACT: Cuando se está llevando a cabo una transmisión o recepción de datos a través del puerto, este LED se ilumina en color verde.

Capítulo 3. Aspectos teóricos

En este capítulo se introducen los conceptos teóricos necesarios para comprender las tecnologías de comunicaciones involucradas en el desarrollo del proyecto.

En primer lugar se describen los tipos de redes presentes en el proyecto, separando la red troncal de la red de acceso de usuario. A continuación, se analizan las tecnologías y protocolos más relevantes que intervienen en la comunicación, comenzando por las tecnologías de capa inferior y ascendiendo de manera lógica hacia las tecnologías de capas más elevadas. Por último, se introducen el simulador y los analizadores usados durante la realización del proyecto.

3.1 Arquitectura de red

La arquitectura de red define los servicios soportados por la red y los protocolos involucrados en la comunicación. Existen varias formas para clasificar una arquitectura de red, siendo las más intuitivas las clasificaciones según la cobertura o la topología de la red. Respecto a la primera, atendiendo a la extensión de las redes y al número de equipos que interconectan se establece la siguiente clasificación [4]:

- **Redes de área local (LAN).** Estas redes son las menos extensas (~1Km), comprendiendo un número reducido de equipos interconectados hasta un máximo teórico de 8000 equipos. La tecnología de comunicaciones más extendida en este tipo de redes es Ethernet con cable de par trenzado (10 Mbps), aunque existen otras tecnologías como Fast Ethernet (100 Mbps) o Gigabit Ethernet (1 Gbps) sobre fibra óptica.

- **Redes de área metropolitana (MAN).** Estas redes interconectan redes locales en el ámbito de un conjunto de edificios (Red de Campus), cubriendo una extensión a nivel regional. En este tipo de redes se concentra el tráfico que proviene de las LAN, de forma que los enlaces deben tener una mayor capacidad. Por ello, este tipo de redes suele poseer enlaces de fibra óptica con tecnologías de comunicaciones como ATM o Gigabit Ethernet.

- **Redes de área extensa (WAN).** Estas redes interconectan las redes de área metropolitana entre sí, cubriendo una gran extensión. El ejemplo de red WAN de mayor dimensión es la red Internet.

En cuanto a la topología de la red, existen varios modelos como son topología en bus, en anillo, en estrella, en árbol… únicamente se van a describir aquellas que influyen en el desarrollo del proyecto [4]:

- **Topología en anillo.** En esta topología, cada nodo es conectado a otros dos más, formando un patrón de anillo. Los nodos interconectados, actúan como repetidores, separando la información destinada al propio nodo, en cuyo caso se procesa, del resto de información, que únicamente se retransmite. Si el anillo es bidireccional, existe la ventaja de que se puede desviar el tráfico por motivos de fallos o congestión en la red.

- **Topología en estrella.** En esta configuración, un nodo actúa como eje central de conexión para el resto de nodos y asume las funciones de gestión y control de las comunicaciones, facilitando caminos para los dispositivos que deseen comunicarse. La ventaja de esta red reside en que el fallo de una conexión en un punto específico, no afecta para nada al resto de conexiones, pero por el contrario, un fallo en el nodo central, produce el bloqueo de toda la red.

En el contexto del desarrollo del proyecto se sitúa, por una parte, la red dorsal que interconecta los distintos nodos mediante enlaces de fibra óptica formando un anillo físico (Red de Campus (MAN)), y por otra, la parte de acceso de usuarios, que se conectan a cada uno de los nodos utilizando cable de par trenzado con conectores RJ45 (Redes LAN).

3.1.1 Red dorsal

Las redes de campus son un tipo particular de redes metropolitanas, de forma que interconectan y dan servicio a un grupo de edificios pertenecientes a una misma corporación. En este caso, la red de la Universidad de Cantabria, que interconecta las distintas áreas geográficas en las que se encuentran los edificios pertenecientes a la universidad. De este modo, conecta a través de un anillo físico los edificios de [2]: Servicio de Informática, Escuela de Náutica, Paraninfo, Escuela de Enfermería y Facultad de Medicina. Se utiliza ATM sobre fibra óptica como tecnología de backbone, usando conexiones virtuales para realizar el intercambio de información (en forma de celdas) entre los nodos.

3.1.2 Red de acceso de usuarios

La red de acceso de usuarios utiliza tecnología Ethernet conmutada. Esto quiere decir que los hosts se conectan mediante enlaces punto a punto a un conmutador de tramas Ethernet (cable par trenzado RJ-45) que resuelve las colisiones y provoca que cada puerto constituya un único dominio de colisión. Mediante esta tecnología se distribuyen las VLANs definidas en los nodos para la conexión de los diferentes colectivos de usuarios.

3.2 Tecnologías de red

Las tecnologías de red que se van a describir en este apartado son las más relevantes dentro de las que participan en el proceso de comunicación. En primer lugar se habla de los protocolos de capa de enlace, estos son, ATM, Ethernet, Spanning Tree y VLAN, siguiendo por los protocolos de capa de red, IP y ARP (en la parte dorsal de la red, la arquitectura IP está definida sobre ATM, mientras que en la parte de acceso de usuarios está definida sobre Ethernet) y por último se hace una breve introducción a los protocolos de capa de aplicación DHCP, SNMP y RMON.

3.2.1 ATM

ATM (Asynchronous Transfer Mode) es un estándar de la ITU-T para dar soporte a la RDSI de banda ancha (B-ISDN) y que fue creado para satisfacer las crecientes necesidades de ancho de banda de las aplicaciones para todo tipo de servicios tales como voz, datos, o video (diferentes perfiles de calidad de servicio) y tratar de encontrar una solución para todo tipo de entornos (LAN, MAN o WAN) [4]. La tecnología ATM se basa en la multiplexación y conmutación de celdas de longitud fija.

El motivo por el que se eligió un tamaño de celda pequeño fue para reducir el tamaño de las colas y el retardo de las mismas. A su vez, al ser celdas de longitud fija, se simplifica la conmutación de datos a alta velocidad [5].

Una red ATM está formada por conmutadores ATM y puntos finales ATM. El conmutador ATM es responsable del tránsito de celdas a través de la red ATM. Acepta las celdas que le llegan de un punto final ATM o un conmutador ATM, lee y actualiza la información en la cabecera de la celda, y rápidamente conmuta la celda a una interfaz de salida hacia su destino. Un punto final ATM o sistema final, contiene un adaptador de interfaz a la red ATM, el cual sí lee los bytes de datos de la celda. Los conmutadores ATM soportan 2 tipos primarios de interfaces [5]:

- **UNI (User to Network Interface).** La interfaz UNI conecta sistemas finales ATM a un conmutador ATM.
- **NNI (Network to Network Interface).** Conecta dos conmutadores ATM.

Para realizar la transmisión, se definen celdas (ver figura 3.1) de 53 octetos, tamaño que consigue el mejor equilibrio entre la eficiencia de transmisión de datos y los requerimientos de retardo para el tráfico de voz y vídeo. Los 5 primeros octetos son de cabecera (poco overhead) y los 48 restantes son de datos.

Figura 3.1. Formato celda ATM

Debido a que los conmutadores ATM soportan 2 interfaces, la cabecera ATM también presenta 2 formatos, tal y como aparece en la figura 3.2.

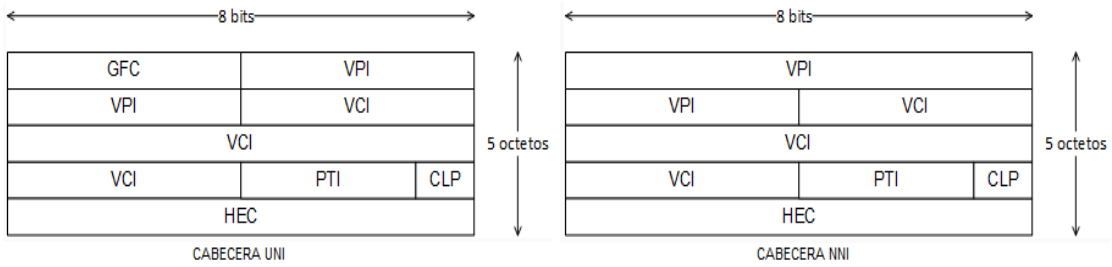


Figura 3.2. Cabeceras UNI y NNI

- **Identificador de canal virtual o VCI (Virtual Channel Identifier) e identificador de camino virtual o VPI (Virtual Path Identifier).** Identifican el siguiente destino de la celda cuando pasa a través de varios conmutadores ATM. Un camino virtual o VP (Virtual Path) no es más que la multiplexación de diversos flujos de tráfico sobre un mismo medio de transmisión, y es identificado por el VPI. Un camino de transmisión es un conjunto de VPs. En ATM cada uno de estos VPs es más tarde multiplexado en un cierto número de canales virtuales o VCs (Virtual Channels), identificados mediante los VCIs. Un VP es, por lo tanto, un conjunto de VCs, cada uno de los cuales es conmutado de forma transparente a través de la red ATM en base a un VPI común. Los VCIs y VPIs sólo tienen un significado local a lo largo de un enlace en particular y se hace una correspondencia, cuando sea apropiado, en cada conmutador.

Si el enlace es bidireccional, se toman los mismos valores de VPI y VCI en ambos sentidos.

- **Identificador del tipo de carga o PTI (Payload Type Identifier).** Indica en el primer bit si la celda contiene datos de usuario o datos de control. Si la celda contiene datos de usuario, el segundo bit indica congestión, y el tercer bit indica si la celda es la última en una serie de celdas que representan una única trama AAL5.

- **Prioridad de pérdida de celda o CLP (Cell Loss Priority).** Indica si la celda debe ser descartada en el caso de que haya congestión en su tránsito por la red. Si el CLP es igual a 1, la celda debe ser descartada antes que las celdas de la misma conexión con el CLP igual a 0.

- **Campo de control de errores o HEC (Header Error Check).** Su valor se calcula a partir de los 4 primeros Bytes de la cabecera. Si ocurren errores en la cabecera ATM, se detectan, y si son menos de 2 se pueden corregir, en caso contrario, la celda será descartada.

- **Campo de control de flujo genérico o GFC (Generic Flow Control).** Campo de la cabecera UNI cuyo valor es siempre 0000 al no haber sido estandarizado.

Las redes ATM son orientadas a conexión, de forma que antes de realizar la transmisión se debe crear un canal virtual. En ATM existen dos formas de establecer una conexión:

- **Virtual Paths Connections o VPC.** Se identifican mediante los VPI.

- **Virtual Channels Connections o VCC.** La conmutación depende de la combinación de un VPI con un VCI.

Cuando se establece un circuito a través de un sistema ATM, todas las celdas relacionadas con ese flujo de datos viajan por la misma ruta durante toda la sesión. Por lo tanto, las celdas llegan en orden, simplificando su procesamiento. Los sistemas de señalización y de gestión reservan un canal virtual con un ancho de banda determinado. En una conexión permanente o PVC (*Permanent Virtual Connection*), el ancho de banda se establece de forma permanente, mientras que en una conexión conmutada o SVC (*Switched Virtual Connection*), el ancho de banda se reserva al iniciar la sesión mediante el sistema de señalización y dicha reserva es liberada por el sistema de señalización cuando se finaliza la llamada. Las conexiones en ATM pueden ser punto a punto o bien punto a multipunto. Un PVC garantiza la disponibilidad de la conexión y no requiere de establecimientos de llamada entre los conmutadores. Un SVC, es más flexible puesto que optimiza el camino de la comunicación y tiene posibilidad de recuperación ante fallos en los enlaces. Otro tipo de conexión existente es la SoftPVC que consiste en crear un PVC entre los extremos del enlace (nodo origen – nodo destino) y manejar SVC en el interior de la red, que se crean sobre el enlace físico en función de las disponibilidades de los enlaces, lo que incrementa el rendimiento de la red y posibilita otros caminos ante fallos inesperados del sistema [5].

En cada conmutador ATM, para cada una de sus interfaces, se tiene una tabla de conmutación introducida manualmente mediante procesos de gestión (en PVCs) o creada dinámicamente por los mecanismos de señalización (en SVCs). La tabla hace

una correspondencia entre los valores VPI/VCI de la celda entrante y los nuevos valores para el trayecto siguiente de la celda, además de indicarse la interfaz de salida del conmutador [5].

Modelo de referencia ATM

La funcionalidad de ATM se corresponde con la capa física y parte de la capa de enlace del modelo OSI. En la figura 3.3 se muestra el modelo de referencia ATM comparado con el modelo de referencia OSI. El modelo de referencia ATM está compuesto por los siguientes planos [5]:

- **Control.** Este plano es responsable de generar y de manejar las peticiones de señalización.
- **Usuario.** Este plano es responsable de manejar la transferencia de datos.
- **Gestión.** Este plano contiene una componente denominada gestión de la capa que maneja funciones específicas de la capa ATM, tales como la detección de fallos y los problemas de protocolo, y otra capa denotada gestión de plano que maneja y coordina funciones relacionadas con el sistema completo.

El modelo de referencia ATM se compone de las siguientes capas [5]:

- **Capa física.** Las funciones de la capa física de ATM son transformar las celdas en una corriente de bits, empaquetando las celdas en el formato que impone el medio de transmisión físico y realizando un control de los límites de las celdas, y el control de la transmisión/recepción de bits por el medio físico. Esta capa se divide en 2 subcapas:
  - **Subcapa PMD (Phisical Medium Dependent).** Es la subcapa inferior y se encarga de la sincronización de la transmisión y recepción, enviando y recibiendo bits de información temporal. Además, especifica el medio físico utilizado incluyendo cables y conectores. Como su propio nombre indica, es dependiente del medio físico de transmisión.
  - **Subcapa TC (Transmission Convergence).** Es la subcapa superior y realiza las funciones de chequeo de errores de cabecera, demarcación de las celdas, adapta las celdas al formato requerido por el medio físico y se encarga de insertar celdas vacías en caso de que sea necesario a fin de mantener la capacidad de transmisión del sistema.
- **Capa ATM.** La capa ATM, en combinación con la capa de adaptación ATM, es análogo al nivel de enlace de datos del modelo de referencia OSI. La capa ATM es responsable del establecimiento de conexiones y del paso de celdas a través de la red ATM. Para ello toma los datos que van a ser enviados y añade la información de la cabecera de 5 bytes que asegura que la celda es enviada por la conexión correcta.
- **Capa de adaptación ATM.** La AAL (ATM Adaptation Layer), combinada con la capa ATM, es semejante al nivel de enlace de datos del modelo de referencia OSI. Para implementar los distintos tipos de servicio ATM, se han especificado 5 capas AAL (AAL1 – AAL5) que adaptan el flujo de celdas ATM a un flujo con

las características requeridas por cada uno de ellos. La más utilizada es la AAL5 para el transporte de IP. La capa AAL se divide en 2 subcapas:

- **Subcapa CS (Convergence Sublayer).** Es responsable de aislar los detalles de los procesos ATM a los protocolos de niveles superior.
- **Subcapa SAR (Segmentation And Reassembly).** Se encarga de asegurar las características de servicio apropiadas y de segmentar cualquier tipo de tráfico en una carga de 48 bytes que será transmitida en las celdas ATM.

- **Capas superiores.** Son las capas que residen sobre la AAL, los cuales aceptan los datos de usuario, los clasifican en paquetes, y los pasan a la AAL.

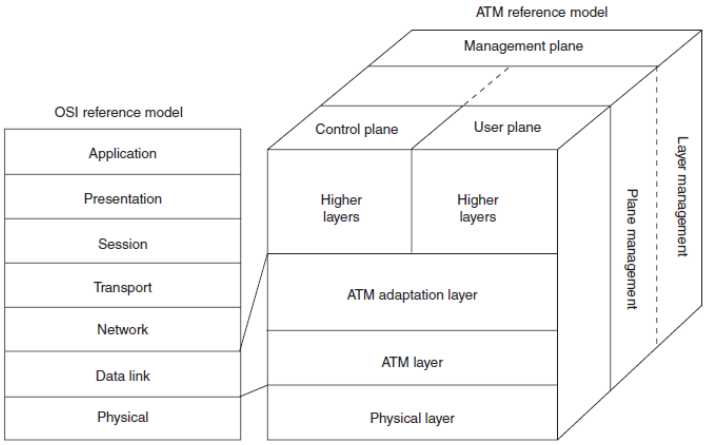


Figura 3.3. Comparativa de los modelos OSI y ATM

AAL5

AAL5 admite celdas dedicadas sin añadir encabezamiento adicional a los 5 Bytes de ATM. La trama formada en la subcapa CS contiene un campo de compensación PAD. En la última celda ATM del mensaje aparecen los 8 Bytes de tráiler que introduce la capa AAL5. No soporta la función de multiplexación y por ello se aplica para datos de señalización y operación sobre ATM, AAL5 se utiliza para transportar IP. Se define la interfaz ILMI (*Interim Local Management Interface*) para operar el protocolo SNMP sobre AAL5.

IP sobre ATM

La forma más sencilla de utilizar una red ATM para transportar tráfico IP es utilizar el VC (Canal Virtual) como si se tratara de una línea dedicada. Para incorporar el soporte multiprotocolo se pueden adoptar dos estrategias (ambas definidas por el IETF en el RFC 1483) [6] [7]:

- Dedicar un VC diferente para cada protocolo; esto es lo que se denomina multiplexado por VC.
- Dedicar un solo VC y diferenciar el protocolo mediante una cabecera 802.2 LLC/SNAP, de forma análoga a lo que se hace en las redes locales.

IP se encapsula dentro de una PDU de AAL5 [6]. El funcionamiento IP/ATM supone la superposición de una topología virtual de routers IP sobre una topología real de conmutadores ATM tal y como aparece en la figura 3.4. El backbone ATM se presenta

como una nube central (el núcleo) rodeada por los routers de la periferia. Cada router comunica con el resto mediante los circuitos virtuales permanentes (PVCs) que se establecen (en base al intercambio de etiquetas entre cada conmutador) sobre la topología física de la red ATM. Los PVCs actúan como circuitos lógicos y proporcionan la conectividad necesaria entre los routers de la periferia. Estos, sin embargo, desconocen la topología real de la infraestructura ATM que sustenta los PVCs. Los routers ven los PVCs como enlaces punto a punto entre cada par. La base del modelo IP/ATM está en la funcionalidad proporcionada por el nivel ATM, es decir, los controles de software (señalización y routing) y el envío de las celdas por hardware (conmutación) [8].

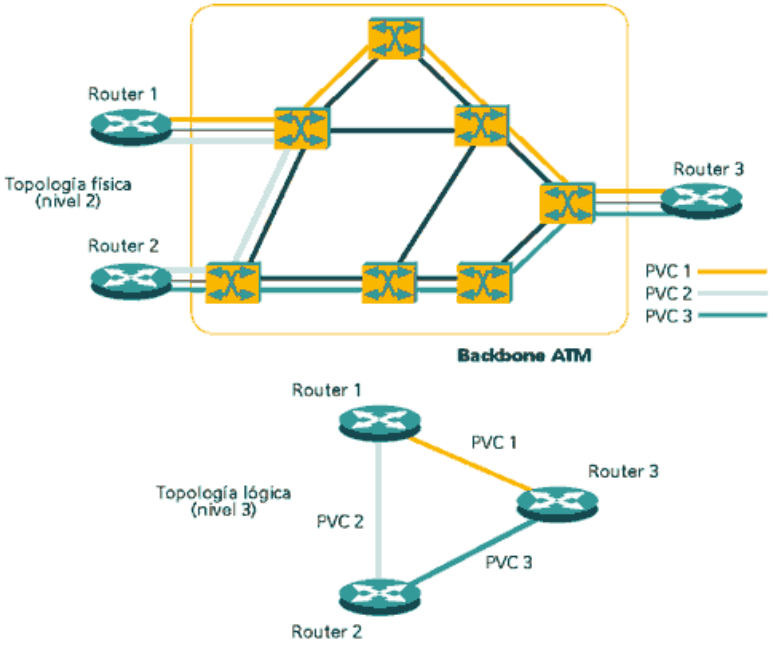


Figura 3.4. Topología física ATM – Topología lógica IP

Encapsulación 802.2 LLC/SNAP (RFC 1483)

La encapsulación 802.2 LLC/SNAP permite multiplexar varios protocolos sobre el mismo circuito virtual. Para que el receptor procese correctamente las AAL5, el campo de datos debe contener una cabecera 802.2 LLC/SNAP que incorpore la información necesaria para identificar el protocolo de la PDU entrante. En la figura 3.5 aparece la encapsulación de un paquete IP mientras que en la figura 3.6 se muestra la encapsulación de una trama Ethernet [6] [9].

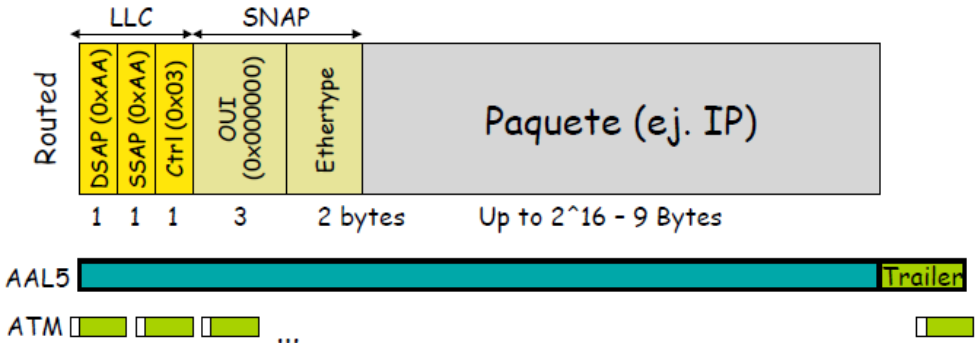


Figura 3.5. Encapsulación de un paquete IP

El valor de Ethertype sería 0x0800 (IP).

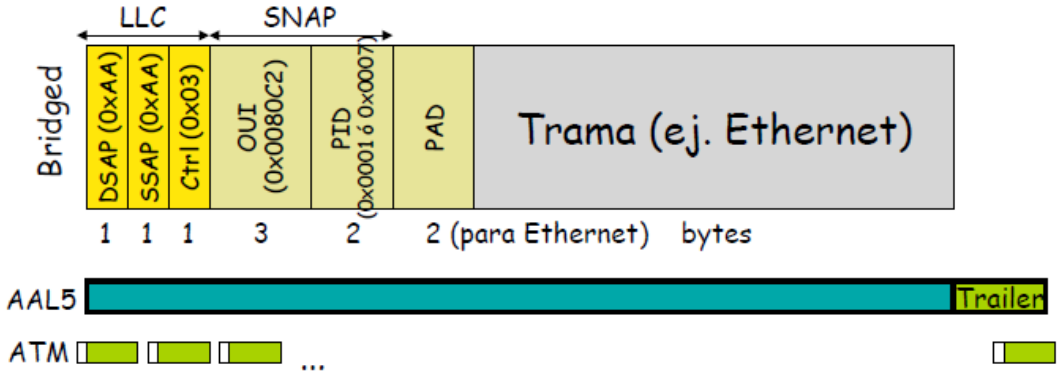


Figura 3.6. Encapsulación de una trama Ethernet

El valor PID (Protocol ID) 0x0001 o 0x0007 identifica una trama IEEE802.3/Ethernet.

Tipos de servicios en el backbone de ATM (Switch Alcatel)

Los servicios ATM operan sobre un backbone de ATM y ofrecen varios mecanismos para conmutar o enrutar tráfico sobre la red ATM. Para interconectar redes IP se pueden definir los siguientes servicios ATM: Classical IP, ATM Trunking y Point to Point (PTOP) Bridging [3].

Los servicios definidos en el backbone de ATM durante el desarrollo del proyecto son:

- **PTOP Bridging.** Permite que 2 grupos (VLANs) se comuniquen a través de la red ATM usando un único circuito virtual, que puede ser de tipo permanente (PVC) o conmutado (SVC). En el desarrollo del proyecto se define como tipo de encapsulación LLC/SNAP (RFC1483, figura 3.6) para el envío de las celdas.

- **ATM Trunking.** Servicio destinado a distribuir las VLANs a través de la red ATM. Los puertos de Trunk encapsulan las VLANs en tramas propietarias que contienen la información necesaria para reproducir la trama de origen en el extremo opuesto del Trunk y mantener las propiedades de cada VLAN. Cada switch solo participará en las VLANs a las que haya sido asignado. Con el Trunking, grupos (VLANs) separados pueden compartir el mismo circuito virtual de ATM.

Información de gestión y señalización

Algunas conexiones virtuales quedan reservadas para que los switches intercambien información de gestión y señalización. Ejemplos de estas conexiones son la 0/5 (UNI Call Signaling), la 0/16 (ILMI) y la 0/18 (PNNI) [9].

- **UNI Call Signaling.** Es un protocolo usado para establecer, mantener y liberar las conexiones virtuales entre el usuario y la red [10].

- **Interim Local Management Interface (ILMI).** Es un protocolo definido por el "ATM Forum" para el establecimiento y la captura de las capas física y ATM y parámetros de caminos y circuitos virtuales en las interfaces ATM. ILMI utiliza mensajes SNMP (sin UDP ni IP) y organiza los objetos gestionados en diferentes MIBs [11].

- **Private Network to Network Interface (PNNI).** Es el protocolo de enrutamiento definido por el "ATM Forum" que indica cómo se deben conectar

los diferentes switch ATM en una red privada. Utiliza una estructura jerárquica para distribuir eficientemente información sobre la topología de red ATM (nodos y enlaces ATM), calcular rutas que cumplan los requisitos de ancho de banda, calidad de servicio… y establecer conexiones entre sistemas finales ATM [12].

3.2.2 Ethernet

Es la tecnología más extendida en redes de área local. En su parte física, está diseñado para poder ser implementado sobre distintos medios físicos con distintas velocidades de transmisión (10, 100, 1.000 y 10.000 Mbps). El tipo de transmisión comúnmente usado es el cable de par trenzado o la fibra óptica.

Como método de acceso al medio se utiliza CSMA/CD, es decir, se escucha el medio antes de transmitir para intentar evitar las colisiones. En caso de que aún así se produzca una colisión, ésta se detecta, se interrumpe la transmisión y se intenta la retransmisión siguiendo el algoritmo de retroceso exponencial binario. Para que sea posible detectar las colisiones, la trama enviada debe tener una longitud mínima de, al menos, 46 bytes en el campo de datos (que sumando el tamaño de las cabeceras hacen 64 bytes) bien sea con datos de usuario o bien con bits de relleno [13].

Ethernet separa las funciones de la capa de enlace de datos en dos subcapas diferenciadas como se ve en la figura 3.7. La subcapa control de enlace lógico (LLC) y la subcapa control de acceso al medio (MAC). Las funciones descritas en el modelo OSI para la capa de enlace de datos se asignan a las subcapas LLC y MAC. La utilización de dichas subcapas contribuye notablemente a la compatibilidad entre diversos dispositivos finales. Para Ethernet, el estándar IEEE 802.2 describe las funciones de la subcapa LLC y el estándar 802.3 describe las funciones de la subcapa MAC y de la capa física. El control de enlace lógico se encarga de la comunicación entre las capas superiores y el software de red, y las capas inferiores, que generalmente es el hardware. La subcapa LLC toma los datos del protocolo de la red, que generalmente son un paquete IPv4, y agrega información de control para ayudar a entregar el paquete al nodo de destino [13].

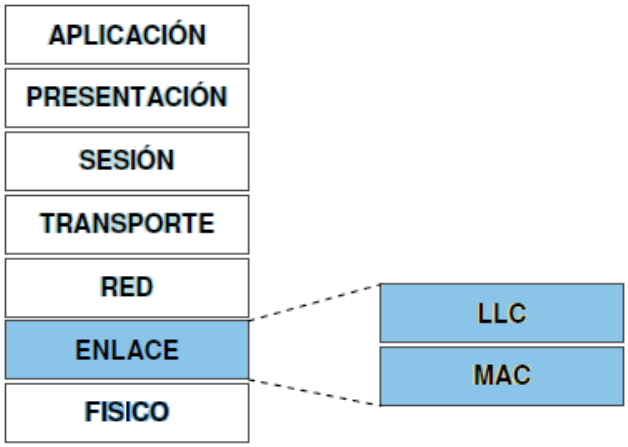


Figura 3.7. Subcapas MAC y LLC

La estructura de la trama de Ethernet agrega encabezados y tráilers a la PDU de Capa 3 para encapsular el mensaje que se envía. Hay dos formatos de tramas de Ethernet: IEEE 802.3 y Ethernet II, siendo este último el formato de trama de Ethernet que se utiliza en redes TCP/IP. Cuando un nodo recibe una trama, debe analizar el campo Longitud/Tipo para determinar qué protocolo de capa superior está presente. Si el

valor de los dos octetos es mayor o igual a 1536 (0x0600 en hexadecimal), significa que se trata de una trama Ethernet II y los contenidos del campo Datos se codifican según el protocolo indicado.

El formato de la trama Ethernet II es el que aparece en la figura 3.8 [4].

Preámbulo (8 octetos)	Dir. de destino (6 octetos)	Dir. de Origen (6 octetos)	Tipo (2 octetos)	Datos (46-1500 octetos)	FCS (4 octetos)

Figura 3.8. Formato de la trama Ethernet II

El campo Tipo permite identificar el protocolo de nivel superior (Ej. 0x0800 para IP). Con este formato de trama no es necesario usar LLC.

El formato de trama IEEE 802.3 es el que aparece en la figura 3.9 [4].

Preámbulo (7 octetos)	SFD (1 oct)	Dir. de destino (6 octetos)	Dir. de Origen (6 octetos)	Longitud (2 octetos)	Datos LLC (46-1500 octetos)	FCS (4 octetos)

Figura 3.9. Formato de la trama IEEE 802.3

El campo Longitud indica el tamaño en bytes del campo Datos (sin relleno). El tráfico IP no se puede encapsular en paquetes IEEE 802.2 LLC sin SNAP, por lo que en el campo Datos se añade la cabecera que aparece en la figura 3.10, en la que el campo Protocol ID representa el identificador de protocolo de capa superior que transporta la trama en el campo de datos. (La cabecera LLC sin SNAP es igual pero eliminando los campos OUI y Protocol ID) [13].

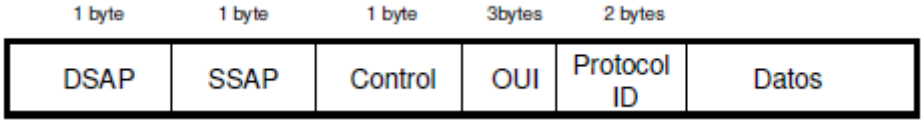


Figura 3.10. Formato de la trama 802.2/LLC SNAP

Por tanto, en una LAN Ethernet se puede realizar encapsulado directo (Ethernet II) o a través de 802.2 LLC/SNAP, tal y como aparece en la figura 3.11 [13].

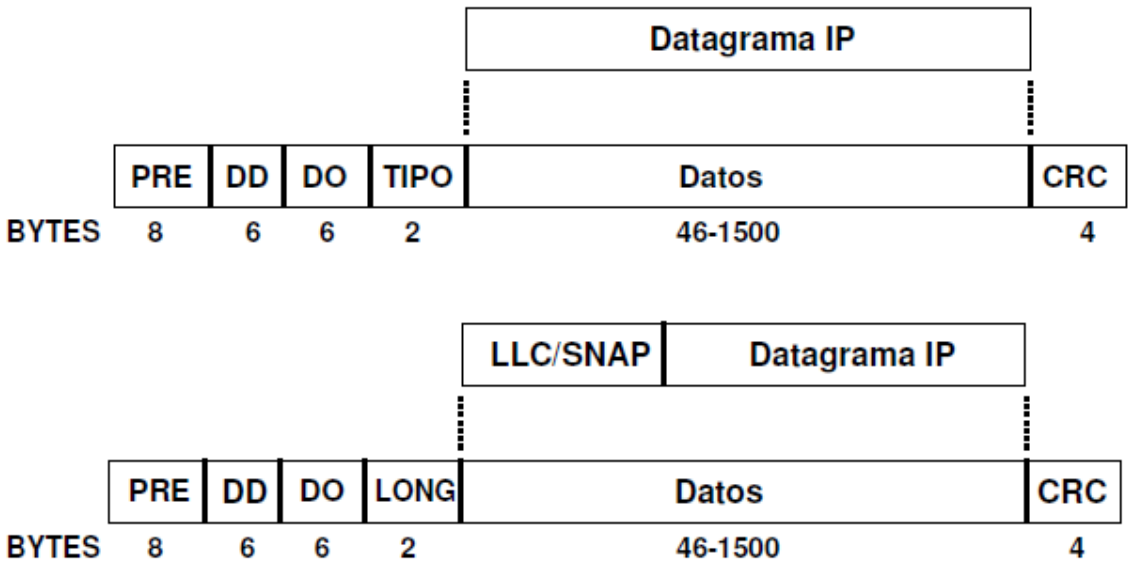


Figura 3.11. IP sobre Ethernet

3.2.3 Spanning Tree

El protocolo ST (Spanning Tree Protocol o protocolo del árbol de expansión) es un protocolo de capa de enlace definido en la especificación IEEE 802.1D que se ejecuta

en bridges y switches. Su principal objetivo es impedir la creación de bucles en trayectos redundantes en la red para proporcionar un canal de comunicación óptimo entre los hosts de una red, siendo transparente para el host del usuario.

Para proporcionar la redundancia de trayecto deseada, así como para evitar la condición de bucle, el STP activa automáticamente los enlaces de ciertas interfaces y bloquea las rutas físicas redundantes para garantizar un sólo camino lógico en cualquier configuración de bridges. Si un enlace activo se vuelve no disponible, el STP reconfigura la red y redirecciona los trayectos de datos mediante la activación del trayecto en espera apropiado. El estado en el que pueden estar las interfaces según el STP aparece en la figura 3.12 [14].

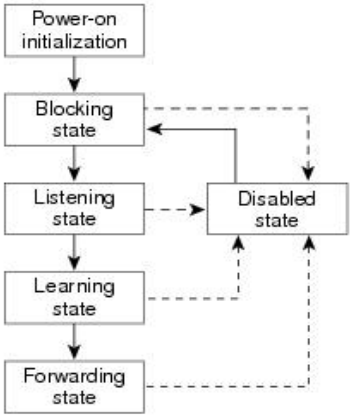


Figura 3.12. Estado de los puertos en el protocolo Spanning Tree

En la figura 3.12 se ve que al encender el switch, el protocolo ST bloquea automáticamente todas las interfaces y después cada una pasa por los estados transitorios de “Listening” y “Learning” hasta que finalmente el protocolo estabiliza las interfaces en los estados de “Forwarding” o “Blocking”. Al estado “Disabled” se puede pasar desde cualquier otro cuando un puerto falla o es bloqueado por el administrador.

Con el STP, la clave es que todos los switches elijan un bridge raíz en la red que se convierta en el elemento fundamental de la red. Todas las demás decisiones en la red, como por ejemplo, qué puerto se bloquea y qué puerto se coloca en el modo de reenvío, se toman desde la perspectiva de este bridge raíz. En un entorno conmutado, que es diferente del de un bridge, suele referirse al bridge raíz como el switch raíz. Si se gestionan varias VLAN, como cada una de ellas es un dominio de difusión independiente, cada VLAN debe tener su propio bridge raíz (lo que se conoce como Multiple Spanning Tree Protocol “MSTP”). Las raíces para las distintas VLAN pueden residir todas en un solo switch o en varios switches [3].

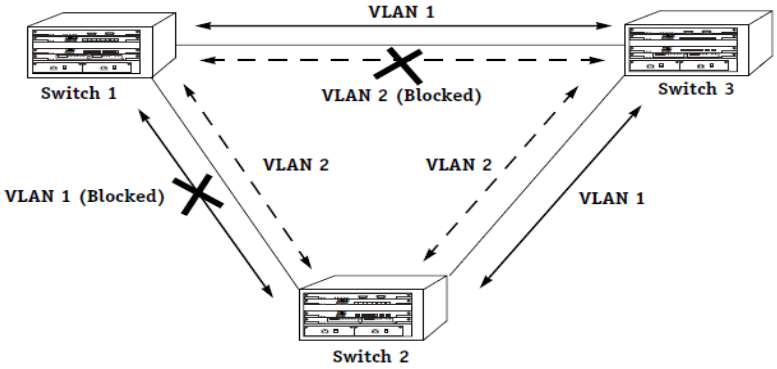


Figura 3.13. Multiple Spanning Tree Protocol (MSTP)

En la figura 3.13 se puede ver un ejemplo de funcionamiento del protocolo MSTP, ya que los switches tratan a cada VLAN de forma independiente. La VLAN 1 presenta el enlace Switch1 – Switch2 bloqueado, mientras que la VLAN 2 tiene bloqueado el paso de paquetes por el enlace Switch1 – Switch3.

Todos los switches intercambian información que se utilizará en la selección del switch raíz. Esta información la transmiten las unidades de datos de protocolo de bridge (BPDU). Cuando los switches se activan por primera vez, comienzan el proceso de selección del switch raíz. Cada switch transmite una BPDU al switch conectado directamente según la VLAN, y a medida que la BPDU sale a través de la red, cada switch compara la BPDU que envía el switch con la BPDU que recibe el switch de sus vecinos. A continuación, los switches concuerdan en qué switch se encuentra el switch raíz que se corresponde con el switch con el ID de bridge más bajo en la red. Todos los switches envían BPDUs usando la dirección MAC de su puerto de origen y una dirección multicast como MAC de destino (01:80:C2:00:00:00). Las BPDUs se encapsulan en LLC con DSAP y SSAP igual a 0x42 [14].

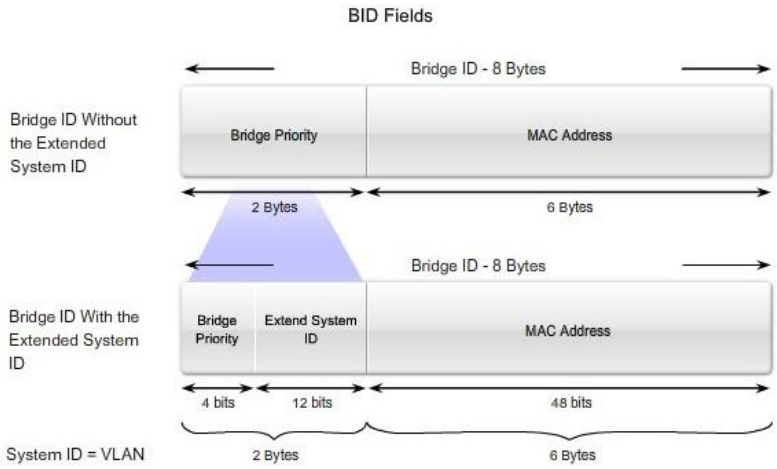


Figura 3.14. Bridge ID

En la figura 3.14 se observa la composición del identificador de Bridge que envían los switches para determinar cuál es el raíz. Por defecto, el campo “Bridge Priority” está fijado a un valor de 32768 (0x8000).

3.2.4 VLAN

La VLAN (Red de área local virtual o LAN virtual) está definida por el estándar IEEE 802.1Q y es una red de área local que agrupa un conjunto de equipos de manera lógica y no física. La comunicación entre los diferentes equipos en una red de área local está regida por la arquitectura física, pero gracias a las redes virtuales (VLAN), es posible liberarse de las limitaciones de la arquitectura física (limitaciones geográficas, limitaciones de dirección, etc.), ya que se define una segmentación lógica basada en el agrupamiento de equipos. Una VLAN permite que un administrador de red cree grupos (en base a distintas políticas) de dispositivos conectados a la red de manera lógica que actúan como si estuvieran en su propia red independiente, incluso si comparten una infraestructura común con otras VLAN. [15]

La diferencia entre una red sin VLAN y una red con VLAN es que en una red sin VLANs configuradas, cuando un switch recibe una trama de broadcast en uno de sus puertos, envía la trama a todos los demás puertos (puesto que los switches solo

separan dominios de colisión), mientras que cuando las VLAN se implementan en un switch, la transmisión del tráfico de unicast, multicast y broadcast desde un host en una VLAN en particular, se limita a los dispositivos presentes en la VLAN (separando de esta forma dominios de difusión). La fragmentación de dominios de broadcast puede realizarse con las VLAN (en los switches) o con routers. Cada vez que dispositivos en diferentes redes de capa 3 necesiten comunicarse, es necesario un router (o un switch con funciones de Capa 3) sin considerar si las VLAN están en uso.

La implementación de la tecnología VLAN añade mayor flexibilidad a la red. Los principales beneficios de utilizar las VLAN son los siguientes [16]:

- **Seguridad.** Los grupos que tienen datos sensibles se separan del resto de la red, disminuyendo las posibilidades de que ocurran violaciones de información confidencial.

- **Reducción de costes.** Se produce un ahorro en el costo puesto que disminuye la necesidad de grandes actualizaciones de red y se utilizan de modo más eficiente los enlaces y el ancho de banda existente.

- **Mejor rendimiento de la red.** La división de las redes planas de Capa 2 en múltiples grupos lógicos de trabajo (dominios de broadcast) reduce el tráfico innecesario en la red (disminuyendo el efecto de las tormentas de broadcast) y potencia el rendimiento.

- **Simplificar la administración de la red.** Las VLAN facilitan el manejo de la red debido a que los usuarios con requerimientos similares de red comparten la misma VLAN, identificando la función de una VLAN fácilmente.

Existen diferentes políticas para definir a los usuarios incluidos en una VLAN [16] [17]:

- **VLAN basada en puertos o VLAN estática**. Mediante esta estrategia, cada puerto se asigna a una VLAN determinada, de modo que una VLAN queda definida mediante una serie de puertos pertenecientes a uno o varios equipos y, para conectarse a dicha VLAN, sólo es necesario conectarse a uno de sus puertos. Es una forma sencilla de definir una VLAN, pero puede ser problemática en redes con cambios constantes o si los usuarios cambian de ubicación con frecuencia. Es una de las políticas que se utiliza para definir las VLANs en el desarrollo del proyecto.

- **VLAN basada en agrupación de direcciones MAC.** Este método consiste en definir a los usuarios de una determinada VLAN mediante su dirección MAC, de forma que un usuario puede cambiar de localización física sin dejar de pertenecer a su VLAN. Es una política que aporta un alto grado de seguridad pero que genera alta carga de trabajo al administrador de la red.

- **VLAN basada en agrupación por protocolo.** Es posible definir una VLAN agrupando a los usuarios por un tipo de protocolo utilizado.

- **VLAN basada en direcciones de red.** Es posible definir una VLAN como un conjunto de direcciones IP, de forma que para el usuario parece una división a nivel 3, pero no deja de ser una división a nivel 2. Junto con la VLAN basada

en puertos, es la política que se utiliza para definir las VLANs en el desarrollo del proyecto.

- **VLAN basada en políticas definidas por el usuario.** Permite definir VLANs en base a la especificación de un modelo de tramas. Todos los dispositivos que generen tramas que respeten el modelo establecido serán asignados a su VLAN correspondiente.

Existen 2 tipos de puerto en un switch para propagar las VLANs, uno entre el switch y el terminal, que se denomina puerto de acceso (“Access port”) y puede contener una única VLAN, y el otro, para comunicación entre los switches, al que se le llama puerto troncal (“trunk port”) y se utiliza para difundir y multiplexar el tráfico de todas las VLAN sobre la misma conexión física. Un enlace troncal es un enlace punto a punto entre dos dispositivos de red, que transporta más de una VLAN y que permite extender las VLAN a través de toda una red. Un enlace troncal de VLAN no pertenece a una VLAN específica, sino que es un conducto para las VLAN entre switches y routers [16].

Cada VLAN debe corresponder a una subred IP única. Si dos dispositivos en la misma VLAN tienen direcciones de subred diferentes, no se pueden comunicar. Los diferentes dispositivos se comunican empleando una etiqueta (“tag”). Para comunicarse con otras VLANs en diferentes subredes, es necesario hacer uso de un dispositivo de Capa 3 (Router) o en su defecto de un Switch compatible con SVI (Switched Virtual Interface) [16].

Etiquetado de trama 802.1Q

Los switches son dispositivos de Capa 2 que solo utilizan la información del encabezado de trama de Ethernet para enviar los paquetes y este encabezado no contiene la información que indique a qué VLAN pertenece la trama. Cuando las tramas de Ethernet se ubican en un enlace troncal, necesitan información adicional sobre las VLAN a las que pertenecen. Esto se logra por medio de la utilización del encabezado de encapsulación 802.1Q. Este encabezado agrega una etiqueta a la trama Ethernet original y especifica la VLAN a la que pertenece la trama. Es decir, cuando una trama circula por un puerto configurado en modo acceso es una trama Ethernet normal, pero cuando circula por un puerto configurado en modo troncal debe indicar a que VLAN pertenece esta trama y por tanto es necesario añadirle esta información, la etiqueta 802.1Q. En realidad, 802.1Q no encapsula la trama original, sino que añade 4 bytes al encabezado Ethernet original. El valor del campo Tipo se cambia a 0x8100 (802.1Q Virtual LAN) para señalar el cambio en el formato de la trama. Debido a que con el cambio del encabezado se cambia la trama, 802.1Q fuerza un recálculo del campo "FCS". El formato del TAG introducido en la trama Ethernet es el que aparece en la figura 3.15 [16].

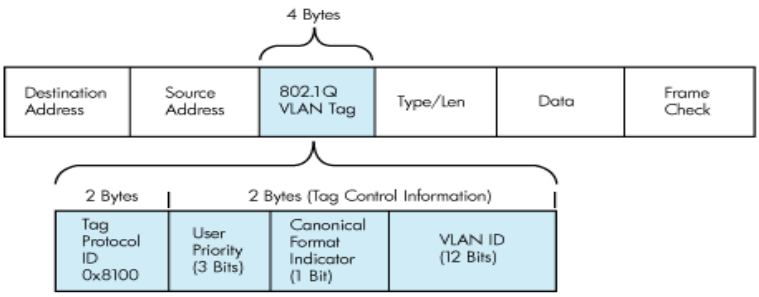


Figura 3.15. Formato del TAG 802.1Q

Los distintos campos del TAG que aparecen en la figura 3.15 son [16]:

- **TPID (Tag Protocol Identifier).** Es un campo de 16 bits que sirve para informar al switch de que se trata de una trama 802.1Q. Por defecto, su valor es 0x8100 lo que la diferencia de cualquier valor que puedan tomar las tramas con campo Longitud (menor de 0x600) o cualquier valor que pueda tomar el campo Tipo.

- **PCP (Priority Code Point).** Definido en el estándar IEEE 802.1p, asigna a la trama niveles de prioridad entre 0-7 para diferenciar clases de servicio.

- **CFI (Canonical Format Identifier).** Se usa para apoyar el bridging entre redes Ethernet y Token Ring (Ethernet/802.3 LSB – Token Ring MSB) - (Token ring encapsulation tag)

- **VID (VLAN Identifier).** Codifica la VLAN en un rango de 0-4095 en el que hay disponibles 4094 valores útiles para etiquetar la VLAN. El valor 000 indica que la trama no corresponde a ninguna VLAN pero se la quiere asignar una prioridad (priority tag). El valor 0xFFF queda reservado para implementación.

Surge un problema provocado por añadir el TAG a una trama del tipo Ethernet/802.3, ya que estas tramas tienen una longitud de 1518 Bytes, pero añadiendo los 4 Bytes del TAG, se generan 1522 Bytes, por lo que hay que asegurarse que todos los switches involucrados en la comunicación dejen pasar la trama y no corten el flujo de las VLANs.

Los modos por los que puede pasar un puerto en el que esté configurado el MSPT son Blocking – Listening – Learning – Forwarding. Los datos de las VLANs se transmitirán y recibirán solo cuando el estado del puerto sea forwarding. Para ello, cuando una trama sale de un dispositivo en una determinada VLAN a un puerto de acceso, debido a su configuración por pertenecer a esa VLAN (MAC, puerto…) se le asigna unos determinados valores que conforman el TAG previamente a que la trama sea enviada por los enlaces de trunk. Una vez la trama ha atravesado los puertos de forwarding necesarios para llegar a su switch destino, se evalúan los puertos por los que tiene que ser enviada basándose en MAC destino y aprendizaje y posteriormente se elimina el tag para que sea enviada por los puertos de acceso y llegue al equipo final [18].

SVI

SVI (interfaz virtual del switch) es una interfaz lógica configurada para una VLAN específica. Es necesario configurar una SVI para una VLAN si se desea enrutar entre las VLAN. Un switch con funciones de Capa 3 tiene capacidad de enrutar transmisiones entre VLANs [16].

Tipos de VLAN

- **VLAN de Datos.** Una VLAN de datos es una VLAN configurada para enviar sólo tráfico de datos generado por el usuario. Es común separar el tráfico de voz y de administración del tráfico de datos. Identifica las VLAN que sólo pueden enviar datos del usuario.

- **VLAN Predeterminada**. Todos los puertos de switch se convierten en un miembro de la VLAN por defecto justo después del arranque inicial del switch. Hacer participar a todos los puertos del switch en la VLAN por defecto los hace a todos parte del mismo dominio de broadcast. La VLAN predeterminada para los switches suele ser la VLAN 1, y presenta todas las características de cualquier VLAN, excepto que no se puede ni renombrar ni eliminar.

- **VLAN Nativa**. Una VLAN nativa está asignada a un puerto troncal 802.1Q. Un puerto de enlace troncal 802.1Q admite el tráfico que llega de muchas VLAN (tráfico etiquetado) como también el tráfico que no llega de una VLAN (tráfico no etiquetado). El puerto de enlace troncal 802.1Q coloca el tráfico no etiquetado en la VLAN nativa. Las tramas pertenecientes a la VLAN nativa no se etiquetan con el ID de VLAN cuando se envían por el trunk.

- **VLAN de Administración.** Una VLAN de administración es cualquier VLAN que se configura para acceder a las capacidades de administración de un switch. La VLAN 1 puede usarse como VLAN de administración. Es necesario asignarle una dirección IP y una máscara de subred a la VLAN de administración para manejar el switch mediante HTTP, Telnet, SSH o SNMP.

- **VLAN de voz.** El motivo por el que se necesita una VLAN separada para admitir la voz sobre IP (VoIP) es porque puede ocurrir que al estar recibiendo una llamada, la calidad de la transmisión se distorsione tanto que no se puede establecer comunicación. El tráfico de VoIP requiere:

  - Ancho de banda garantizado para asegurar la calidad de la voz.

  - Prioridad de la transmisión sobre los tipos de tráfico de la red.

  - Capacidad para ser enrutado en áreas congestionadas de la red.

  - Demora de menos de 150 milisegundos (ms) a través de la red.

En este caso, se presenta una red dorsal ATM mientras que los dispositivos finales siguen la norma Ethernet. Dada esta característica, es posible transportar el tráfico interno a la VLAN entre los switches utilizando circuitos virtuales permanentes (PVC). De este modo, se define un PVC por cada nodo final en el que se pretende difundir una determinada VLAN y al circuito virtual se le asocia un servicio ATM encargado de transportar el tráfico de la VLAN.

3.2.5 IP

El protocolo de Internet (IP) es un protocolo de capa de red que está definido en el RFC 791 (IPv4) y que ofrece un servicio no orientado a conexión y no confirmado. La funcionalidad básica de IP es la entrega de datagramas a través de redes. Estos datagramas presentan la cabecera (IPv4) que aparece en la figura 3.16. La longitud mínima de la cabecera es de 20 Bytes.

0-3	4-7	8-15	16-18	19-31
Versión	Tamaño Cabecera	Tipo de Servicio	Longitud Total	
Identificador			Flags	Posición de Fragmento
Time To Live		Protocolo	Suma de Control de Cabecera	
Dirección IP de Origen				
Dirección IP de Destino				
Opciones				Relleno

Figura 3.16. Cabecera IP

IP recibe los datos que le llegan desde la capa de transporte y añade la cabecera con las direcciones IP origen y destino, y el protocolo de capa de transporte al que se dirige. A su vez, se encarga de acomodar el datagrama en una trama de nivel de enlace, por lo que si el datagrama supera el tamaño máximo permitido (MTU) por el protocolo de enlace, IP se encarga de la fragmentación del paquete.

Utiliza un algoritmo de encaminamiento para guiar el datagrama a través de la red hasta su destino. IP es un protocolo best effort, es decir, no asegura la entrega de los datagramas sino que se limita a “hacer lo que pueda”. Cuando un datagrama llega a su destino, IP se encarga de eliminar su cabecera y entregar los datos al protocolo de capa de transporte correspondiente.

Las direcciones IP tienen una longitud de 4 bytes y se dividen en dos campos, el identificador de red y el identificador de host. El formato de las direcciones IPv4 basado en clases aparece en la figura 3.17. Hay 5 clases de redes, A,B,C,D y E [13].

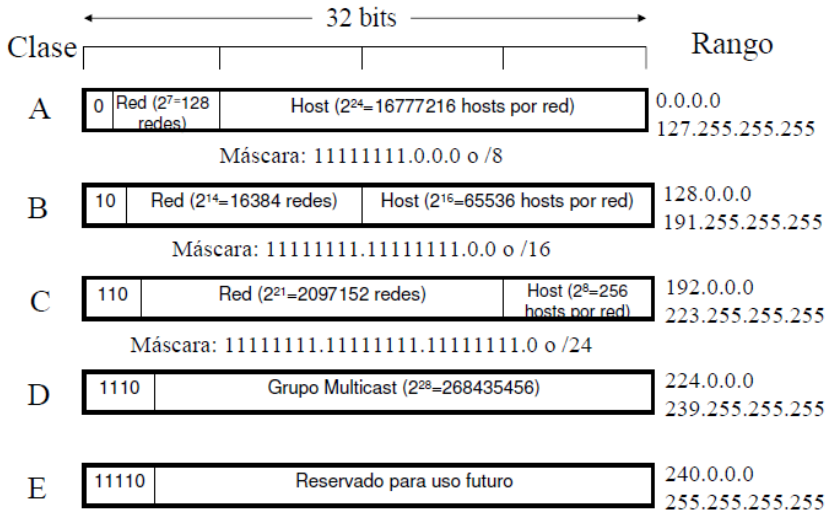


Figura 3.17. Direccionamiento IP basado en clases

Dos equipos pertenecen a la misma red cuando sus identificadores de red son iguales. La longitud de ambos campos viene determinada por la máscara de red, de forma que el campo de red tiene en la máscara todo unos, mientras que el campo host tiene en la máscara todo ceros. De este modo, cuando un datagrama llega al router, este realiza una operación AND lógica entre la dirección IP destino y la máscara de red para conocer a qué subred pertenece dicha dirección y, en base al resultado, saber si dicho datagrama pertenece a la red en la que se encuentra o debe ser encaminado hacia el exterior [4].

Subnetting

Este concepto hace referencia a la necesidad de dividir una red en otras de menor tamaño, creando una o más redes físicas que forman un subconjunto de una red de Internet. Se consigue tomando bits de la máscara de subred pertenecientes a identificación de hosts en la red principal y asignándolos a identificación de red, formando de esta manera un mayor número de redes (de menor tamaño) partiendo de una única red principal, dividiendo a los hosts de cada subred en dominios de difusión.

3.2.6 ARP

El protocolo de resolución de direcciones (ARP) fue desarrollado para permitir las comunicaciones entre redes interconectadas y está definido en el RFC 826. Los dispositivos de capa 3 utilizan el protocolo ARP para asignar direcciones de red IP a direcciones MAC de hardware para que los paquetes IP se puedan enviar a través de la red. Antes de que un dispositivo envíe un datagrama a otro dispositivo, comprueba en su caché ARP si hay una dirección IP con la dirección MAC correspondiente para el dispositivo de destino, si no hay ninguna entrada coincidente, el dispositivo fuente envía un mensaje de difusión a todos los dispositivos en la red y cada uno compara la dirección IP destino del mensaje con la suya propia. Cuando coindicen, el dispositivo con la dirección IP deseada responde al dispositivo emisor con un paquete que contiene su dirección MAC. Entonces, el dispositivo fuente añade a este dispositivo en su tabla ARP por un tiempo (ARP caché) para futuras consultas, y procede a transferir el datagrama oportuno directamente por la trama MAC. En caso de que los dispositivos no estén en la misma subred, la dirección MAC que se le transmite al dispositivo fuente es la del Router que separa a ambos dispositivos, que hace de intermediario para la transmisión de datagramas sin que los hosts puedan percibirlo (lo que se conoce como "Proxy ARP") [19].

El formato de la trama ARP es el que aparece en la figura 3.18 [13].

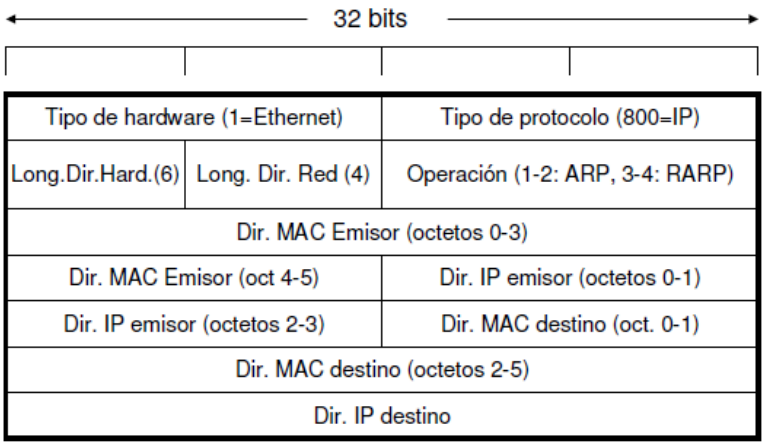


Figura 3.18. Formato de la trama ARP

En el campo de Operación, el valor 1 significa que se trata de una trama ARP Request y el valor 2 quiere decir que se trata de una trama ARP Response.

3.2.7 DHCP

El protocolo de configuración dinámica de Host (DHCP) es un protocolo estándar de tipo cliente/servidor definido en el RFC 2131 y que permite a un servidor distribuir de

forma dinámica el direccionamiento IP y distinta información de configuración a los clientes. Normalmente el servidor DHCP proporciona al cliente al menos una información básica compuesta por dirección IP, máscara de subred y puerta de enlace predeterminada, pero también puede proporcionar otro tipo de información como direcciones de servidores DNS, información relacionada con el propio servidor DHCP… [20]

Cuando un cliente se inicializa por primera vez después de que se configura para recibir información del DHCP, inicia una conversación con el servidor. Existen 3 modos de asignar una dirección a un cliente [13].

- **Asignación manual.** El administrador de la red configura manualmente las direcciones IP de los clientes en el servidor DHCP. Así, cuando el cliente solicita una dirección IP, el servidor mira la dirección MAC del mismo y procede a asignar la que configuró el administrador.

- **Asignación automática.** Al cliente DHCP se le asigna una dirección IP cuando contacta por primera vez con el servidor DHCP. En este método la IP es asignada de forma aleatoria y no es configurada de antemano.

- **Asignación dinámica.** El servidor DHCP asigna una dirección IP a un cliente de forma temporal, es decir, es entregada al cliente que hace la petición por un espacio de tiempo. Cuando este tiempo expira, la IP es revocada y el host ya no puede funcionar en la red hasta que no solicite otra.

El protocolo DHCP utiliza UDP como protocolo de transporte. Los mensajes DHCP de un cliente a un servidor son enviados por el puerto 68 “DHCP client”, y los mensajes enviados de un servidor a un cliente son enviados por el puerto 67 “DHCP server”. A continuación, se muestran los mensajes típicos entre un cliente y un servidor DHCP [20]:

Source MAC addr	Dest MAC addr	Source IP addr	Dest IP addr	Packet Description
Client	Broadcast	0.0.0.0	255.255.255.255	DHCP Discover
DHCPsrvr	Broadcast	DHCPsrvr	255.255.255.255	DHCP Offer
Client	Broadcast	0.0.0.0	255.255.255.255	DHCP Request
DHCPsrvr	Broadcast	DHCPsrvr	255.255.255.255	DHCP ACK

Excepto para el caso de que el administrador haya configurado una asignación manual, si al cliente ya se le había asignado una dirección IP del DHCP y se reinicia, el cliente solicitará específicamente la dirección IP concedida anteriormente en un paquete DHCP Request especial. La información de DHCP obtenida por el cliente de un servidor DHCP tendrá un tiempo de concesión asociado, a partir del cual será necesario solicitar una nueva información de configuración [21].

3.2.8 SNMP y RMON

Simple Network Management Protocol (SNMP) es un protocolo de capa de aplicación que permite intercambiar información de gestión entre los dispositivos de red y que está especificado en el RFC 1157. Una red gestionada por SNMP se compone de tres partes fundamentales: Agentes, dispositivos gestionados (switches, routers…) y al menos un sistema administrador de red (NMS) [22].

Un agente es un software de gestión de red instalado en el dispositivo gestionado que se encarga de recoger estadísticas de gestión del dispositivo, que almacena en su MIB (Management Information Base) local, y que responde a las órdenes de la estación gestora. A su vez, informa mediante el envío de mensajes asíncronos (traps) de cambios significativos en el entorno local.

El NMS es una estación gestora que incluye una aplicación de gestión con un interfaz gráfico que permite al administrador de la red monitorizar el rendimiento de la red, detectar fallos o planificar el crecimiento de la red.

La información de gestión de un dispositivo gestionado se almacena en la base de información de gestión (MIB), que está constituida por una serie de ficheros anidados. La información contenida en dichos ficheros, se encuentra ordenada siguiendo una jerarquía de árbol, de forma que a cada uno de los objetos gestionados, le corresponde un identificador único llamado object identifier (OID). Cada agente SNMP es responsable de su MIB local y controla el uso que hacen de esa MIB las estaciones gestoras.

Para realizar las operaciones de administración, el protocolo SNMP utiliza un servicio no orientado a la conexión (UDP) para enviar mensajes, llamados unidades de datos de protocolo (PDU), entre los administradores y los agentes. Los agentes escuchan en el puerto 161 y la estación gestora escucha los Traps en el puerto 162.

Existen 3 órdenes básicas en el protocolo de gestión SNMP [22]:

- **Get.** Se utiliza para pedir información de gestión al agente. Para ello, el gestor envía el OID del objeto cuyo valor desea conocer y el agente responde con el valor solicitado.

- **Set.** El gestor utiliza esta orden para modificar el valor de una determinada variable en el agente, enviando el OID y el nuevo valor del objeto a modificar.

- **Trap.** El agente notifica al gestor la detección de un evento significativo en la red. En el agente se encuentra definida una lista de eventos que han de ser notificados al gestor en caso de ser detectados.

Los agentes definen una o varias comunidades (“communities”) que hacen el papel de contraseña para acceder a información de la MIB, bien sea según una política de acceso de solo lectura (“read-only”) o de lectura y escritura (“read-write”). Las estaciones gestoras deben proporcionar el nombre de comunidad establecido por el agente en todas sus interacciones con la estación gestionada.

El funcionamiento del protocolo SNMP se muestra en la figura 3.19 en la que se pueden ver los diferentes mensajes PDU enviados desde la estación gestora para ver o modificar información almacenada en la MIB (a los que responde el agente con GetResponse), y el Trap que envía el agente ante un evento en el entorno local [22].

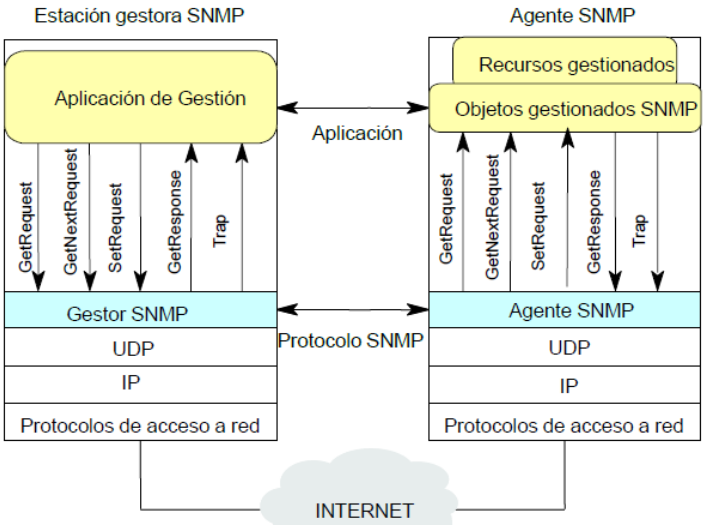


Figura 3.19. Funcionamiento del protocolo SNMP

RMON

Tras generalizarse el uso de SNMP, surgen diversas ampliaciones, de las cuales la de mayor importancia es Remote Monitoring (RMON), un estándar definido en la RFC 1271 para la monitorización de tráfico en puertos Ethernet. Para llevar a cabo la monitorización, se definen una serie de pruebas ("probes") en los puertos deseados. Éstas se encargan de recoger y almacenar los datos que se muestran al administrador de la red cuando este los requiera. También es posible definir una serie de eventos que, en caso de darse en la red, generen algún tipo de notificación o alarma que será enviada al gestor [22].

Existen 3 tipos de pruebas que se pueden habilitar en los nodos:

- **Ethernet.** Muestra las estadísticas actuales de la red.
- **History.** Recoge estadísticas del uso de la red a lo largo del tiempo. Para ello, realiza un sondeo con un intervalo de tiempo establecido y almacena los datos hasta que llena el espacio de memoria asignado. En ese momento elimina las estadísticas más antiguas y las sustituye por las nuevas.
- **Alarm.** Se establecen, para una característica determinada, unos valores máximos superior y/o inferior. Cuando toma algún valor fuera del rango establecido, genera un Trap que informa de este suceso.

3.3 Aplicaciones y hardware utilizado

En el desarrollo del proyecto se han utilizado los analizadores hardware de protocolos: ATM Advisor y LAN Advisor del fabricante Agilent, el software analizador de protocolos Wireshark, la suite de gestión de redes SNMP del fabricante MG- y el simulador de redes Packet Tracer de Cisco.

3.3.1 Hardware de Agilent

Los analizadores portátiles Agilent Advisor permiten capturar y analizar el tráfico en cualquier punto de la red. De esta forma, es posible monitorizar el funcionamiento de la red en tiempo real y prevenir errores en el sistema. Por una parte, se utiliza el

equipo ATM Advisor para comprobar el funcionamiento de la red troncal ATM y por otra, el equipo LAN Advisor para comprobar el funcionamiento de la red de acceso [23] [24].

3.3.2 Wireshark

Es un analizador de protocolos utilizado que permite realizar análisis y capturas de tráfico y solucionar problemas en redes de comunicaciones. Wireshark es un software libre que incorpora una interfaz gráfica en la que se pueden filtrar los paquetes que se analizan y se pueden desplegar los diferentes protocolos incluidos en los mismos [25].

3.3.3 MIB Browser

Es un software propietario de gestión de red creado por MG-SOFT que facilita el manejo de información SNMP. MIB Browser permite supervisar y gestionar cualquier dispositivo SNMP en la red mediante el uso de los protocolos estándar SNMPv1, SNMPv2 y SNMPv3 sobre redes IPv4 o IPv6. Permite realizar las operaciones de SNMP Get, SNMP GetNext, SNMP GetBulk y Set de SNMP. Además, el software permite capturar Traps y paquetes de información SNMP enviados desde dispositivos arbitrarios SNMP o desde otras aplicaciones en la red [26].

3.3.4 Cisco Packet Tracer

Es el simulador desarrollado por Cisco Systems que se ha empleado para verificar el funcionamiento de la red desplegada en este proyecto. Dicho simulador soporta multitud de protocolos de comunicaciones y permite crear topologías de red, configurar dispositivos, insertar paquetes y simular una red con múltiples representaciones visuales que permiten analizar los paquetes enviados sobre una red de comunicaciones.

Permite crear una topología de red de forma intuitiva, simplemente hay que arrastrar los dispositivos deseados a la pantalla. Cada dispositivo de red presenta una consola de configuración en línea de comandos que permite su configuración de la misma forma que se haría sobre un dispositivo de red real, con los comandos propios de su sistema operativo (Cisco OS). Tras la creación de la red, el programa permite hacer simulaciones de conectividad (pings, traceroutes…) desde las consolas para hosts que proporciona, y capturar los paquetes que se envían para analizar los protocolos en las distintas capas de la red [27].

Capítulo 4. Aspectos prácticos

En primera instancia, como paso previo al estudio de la configuración de red, se exponen los métodos de acceso a los nodos, ya que para visualizar la información de configuración es necesario acceder a la interfaz de usuario de los equipos.

Después, se analiza el conexionado de los nodos, tanto de la parte dorsal de la red, como de la parte de acceso de usuario, para posteriormente analizar la configuración funcional existente, obteniendo así diversas conclusiones acerca de los cambios que se deben realizar en los equipos y determinando si es posible conservar alguna configuración previa.

Por último, se realiza la configuración final de la red, para lo cual se modificarán los parámetros necesarios de los nodos, de forma que la parte troncal se base en la comunicación a través de los circuitos virtuales de ATM y la parte de acceso a usuario tenga definidas una serie de VLANs diferenciadas según el colectivo universitario al que pertenezca la persona que se quiere conectar a la red.

4.1 Modalidades de acceso a los nodos

Para poder estudiar la configuración de los equipos y posteriormente modificarla a conveniencia, es necesario acceder a la interfaz de usuario (UI) de los nodos Alcatel. Primeramente, sin haber configurado nada en el nodo, únicamente podemos acceder con las 2 interfaces serie que presenta el módulo de gestión (MPM). Ambas conexiones serie presentan 9 pines (conectores DB-9) y como se puede apreciar en la figura 4.1, la diferencia se establece en que una conexión es macho y la otra es hembra. La conexión macho (DTE) típicamente se conecta a un módem, aunque existe la posibilidad de conectarse directamente a un terminal mediante un cable de módem nulo (líneas de transmisión y recepción cruzadas). La conexión hembra (DCE) se conecta directamente a un PC o terminal.

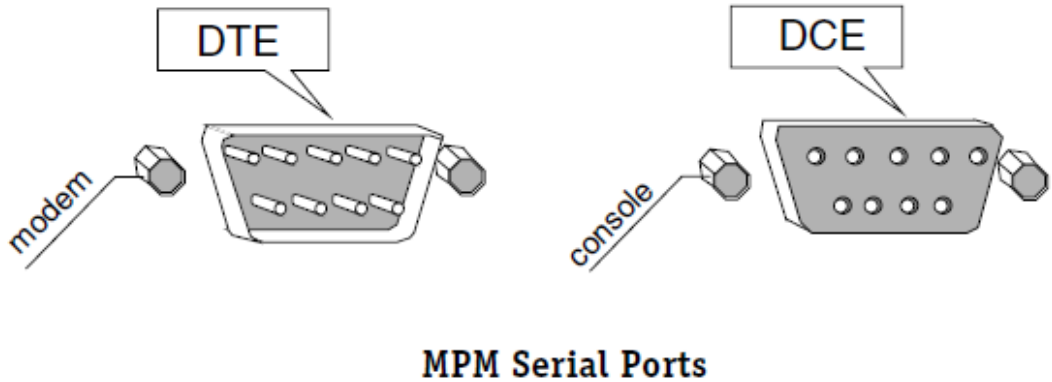


Figura 4.1. Interfaces para acceder al nodo

Para la configuración de los nodos se utiliza un PC del laboratorio, cuyo interfaz serie se conecta mediante un cable RS-232 al interfaz serie (consola) del nodo a configurar. En el PC se utiliza el software Procomm para control y acceso al interfaz de usuario del nodo. La configuración (por defecto) del puerto serie es la siguiente [3]:

- 9600 bps.

- 8 bits de datos.
- 1 bit de stop.
- Sin paridad.
- Sin control de flujo por hardware.

A continuación, el sistema de los nodos requiere autenticación mediante usuario y contraseña. Existen 2 usuarios disponibles [2]:

- Usuario: “admin”, Contraseña: “botello”. Tiene los permisos de lectura “R”, escritura “W” y administración “A”. El permiso “W” da acceso de lectura y escritura para comandos de configuración del nodo mientras que el permiso “A” da acceso de lectura y escritura para todos los comandos existentes.
- Usuario: “diag”, Contraseña: “switch”. Tiene los mismos permisos que el usuario “admin” además de uno adicional de gestión del nodo “M” que permite realizar pruebas de diagnóstico en el nodo.

Una vez autenticados, el sistema despliega el menú principal de la figura 4.2 en el que se visualizan los diferentes apartados que se pueden configurar.

```
Welcome to the Alcatel OmniSwitch! Version 4.3.2 GA
login   : admin
password:
*******************************************************************************
Alcatel OmniSwitch
Copyright (c), 1994-2001 Alcatel Internetworking, Incorporated. All rights
reserved.
OmniSwitch is a trademark of Alcatel Internetworking, Incorporated,
registered in the United States Patent and Trademark Office.
            System Name:       SdeI
        System Location:       V-Pino
    Command      Main Menu
    ------------ ------------------------------------------------------------
    File         Manage system files
    Summary      Display summary info for VLANs, bridge, interfaces, etc.
    VLAN         VLAN management
    Networking   Configure/view network parameters such as routing, etc.
    Interface    View or configure the physical interface parameters
    Security     Configure system security parameters
    System       View/set system-specific parameters
    Services     View/set service parameters
    Switch       Enter Any to Any Switching Menu
    Help         Help on specific commands
    Diag         Display diagnostic level commands
    Exit/Logout  Log out of this session
    ?            Display the current menu contents
```

Figura 4.2. Menú principal de la UI

Para navegar por la UI, se escriben los comandos del menú principal que aparecen en la figura 4.2 y posteriormente se pulsa la tecla “*?*” para desplegar su submenú específico. Si se conoce de antemano algún comando de configuración y se desea ejecutar, también es posible introducirlo directamente sin navegar por los distintos submenús. Si no se conoce la sintaxis exacta de un comando, tecleando el principio y pulsando retorno de carro, la UI devolverá los comandos existentes con el inicio especificado como se ve en el ejemplo de la figura 4.3. Para obtener información básica sobre un comando se teclea “*lookup* + *comando*” y el sistema explicará su función, tal y como aparece en la figura 4.4 para el comando *“userview”*, que se ejecuta para comprobar los permisos de los usuarios descritos anteriormente. A su vez, si un comando requiere de ciertos parámetros que se desconocen para su

correcta ejecución, se puede introducir sin ningún complemento adicional y la UI especificará su modo de utilización, como se puede apreciar en la figura 4.5.

```
SdeI/ >user
Non-unique command match, possible commands:
         useradd  userdel  usermod  userview
```

Figura 4.3. Ejemplo de sintaxis de comando no conocida al completo

```
SdeI/ >lookup userview
View the users in the local user database
SdeI/ >userview
Username         Privileges
admin            R W A
diag             R W A M
```

Figura 4.4. Consulta de función y ejecución del comando *"userview"*

```
SdeI/ >addvp
Usage: addvp group_id vport_list
   as in:
          "addvp 110 2/1-3,3/5,4/7-10"
```

Figura 4.5. Modo de utilización del comando *"addvp"*

Para regresar al menú principal se emplea el comando "*Help*". Por último, si al ejecutar un comando sus resultados no son visibles por completo debido a que exceden el número de líneas establecidas (por defecto 22), se pulsará retorno de carro para mostrar la siguiente línea de resultados o la tecla espacio para mostrar una nueva página con las siguientes líneas de resultados hasta alcanzar el número máximo de líneas establecidas.

Los submenús más relevantes en este proyecto son los de ATM, VLAN e IP (dentro de un submenú puede haber comandos u otro submenú diferente). Por ejemplo, para ver y modificar información sobre diferentes datos de red (tabla de rutas IP, estadísticas TCP y UDP…) sería necesario navegar por la UI como se muestra en las figuras 4.6 y 4.7.

```
$SdeI/  >networking
$SdeI/Networking >?
    Command      Networking Menu
    ------------ ------------------------------------------------------------
    snmps        View SNMP statistics
    snmpc        Configure SNMP
    Names        Configure the DNS resolver
    probes       Display all RMON probes
    events       Display all logged RMON events
    IP           Enter IP networking command sub-menu
    IPX          Enter IPX networking command sub-menu
    Monitor      Enter port monitor utilty command sub-menu
    Filtering    Enter network filtering command sub-menu
    IPMR         Enter IPMR routing sub-menu
    IPMS         Enter IPMS networking command sub-menu
    PNNI         Enter the PNNI menu
```

Figura 4.6. Submenú Networking

```
$SdeI/Networking >ip
$SdeI/Networking/IP >?
Command      IP Menu
------------ ------------------------------------------------------------
xlat         View the address translation table
ips          View IP stats & errors
ipr          View IP routes
aisr         Add an IP static route
risr         Remove an IP static route
icmps        View ICMP stats & errors
ping         Ping a system
udps         View UDP stats and errors
udpl         View the UDP listener table
rips         View RIP stats and errors
```

```
tcps          View TCP-related statistics
tcpc          View the TCP Connection table
telnet        Remote login to another system using TELNET
traceroute    Trace an IP route
relay         Use 'relayc' or 'relays'
fwconfig      Configure the IP Firewall
ripflush      Flush all routes obtained by RIP
ipfilter      Add/delete an IP RIP filter
ipf           Display IP RIP filters
ipmac         View the IP to MAC Address Association table
ipclass       Turn on/off IP Class Address Checking
ipdirbcast    Turn on/off IP directed broadcast
```

Figura 4.7. Submenú IP

Una vez localizado el comando deseado se ejecutará junto con los parámetros necesarios. Otra alternativa para configurar los nodos es mediante la línea de comandos (CLI) tal y como se observa en la figura 4.8.

```
$SdeI/ >cli
Entering command line interface.  Type quit to exit
->
```

Figura 4.8. Línea de comandos

Una vez conectado desde un PC al puerto consola de un nodo y tras haberlos configurado, existe la posibilidad de acceder remotamente a cualquier otro nodo de la red mediante la ejecución de un telnet a la dirección IP de una de sus interfaces. Además, es posible conectarse directamente al nodo SdeI a través de un cable Ethernet (RJ-45) desde un equipo de la misma red dado que su módulo de gestión es diferente y tiene un conector que no está presente en los demás nodos. Estos modos de acceso se probarán más adelante puesto que previamente es necesario configurar adecuadamente los equipos. Es importante tener en cuenta que como máximo se pueden mantener 4 conexiones simultáneas con un nodo y que solo una de ellas podrá tener permiso de escritura [2].

4.2 Conexionado físico de la red

En este apartado se va a estudiar el conexionado físico de los equipos para que la red funcione de manera correcta dentro del entorno del laboratorio de telemática.

En primer lugar, se analizará la parte dorsal y se comprobará que las conexiones de las fibras ópticas que transportan el tráfico entre los nodos son las adecuadas, obteniendo las configuraciones física y lógica existentes en esta parte troncal de la red.

A continuación se describe el conexionado de la red de acceso que posibilita que un usuario pertenezca a una VLAN de un determinado nodo.

4.2.1 Situación de los módulos en cada nodo

Antes de exponer capturas provenientes de ejecutar comandos a través de la UI, es necesario conocer en qué posición se sitúan los módulos en los diferentes nodos y las opciones de configuración que tiene cada uno para interpretar correctamente la sintaxis de los comandos introducidos.

Como ya se introdujo en el segundo capítulo, existen 2 tipos diferentes de chasis, uno que incorpora 9 slots (SdeI y Paraninfo) y otro que incorpora 5 slots (Náutica, Enfermería y Medicina). Todos los nodos tienen instalado un módulo de gestión (MPM) y 3 módulos de conmutación (FCSM, CSM y ESM). El módulo de gestión está

instalado en el slot 1 de todos los nodos, pero no es relevante en el proceso de configuración de los equipos. El módulo FCSM se sitúa en el slot 2 de todos los nodos, y aunque no tenga puertos físicos configurables, si que incorpora una interfaz interna en la que se definen los servicios ATM, la interfaz 2/1. En cuanto al módulo CSM, también ocupa el mismo slot en todos los nodos, el slot 3. Este módulo incorpora los conectores de fibra a través de los cuales se realizan las conexiones físicas en la red dorsal. Cada nodo presenta 2 conectores, uno para enlazar con el nodo previo del anillo y otro para enlazar con el posterior. Aunque no se configuran por consola, sus interfaces 3/1 y 3/2 serán visibles al ejecutar determinados comandos. Por último, el módulo ESM varía de slot en los diferentes nodos. Mientras que para los nodos con chasis de 5 slots se sitúa en el slot 4, en el SdeI está instalado en el slot 5 y en el Paraninfo en el slot 6. Este módulo se utiliza para realizar el conexionado físico de la red de acceso a usuario y consta de 32 puertos Ethernet en cada nodo, con lo que, por ejemplo, en el SdeI se configurarán las interfaces 5/1 a 5/32.

4.2.2 Conexionado de la red dorsal

Conexionado físico

En un primer momento, se observa el conexionado físico de la parte dorsal de la red. Los equipos están enlazados tal y como se presentaban cuando formaban parte de la red universitaria. Como se expuso en el primer capítulo, los nodos forman físicamente un anillo mediante fibra óptica monomodo a 155 Mbps. El anillo presenta el siguiente conexionado físico [2]:

SdeI – Náutica – Paraninfo – Enfermería – Medicina – SdeI

Para corroborar el buen conexionado de los nodos, es necesario realizar una serie de comprobaciones previas al proceso de configuración. La primera opción a revisar está relacionada con los LED incorporados en el módulo CSM de los equipos; Ha de comprobarse que los LED “ACT” lucen de color verde. Si no es así, es probable que haya algún problema con el conexionado del equipo. Una vez revisados dichos LED, aunque estos luzcan de color verde, no quiere decir que los nodos estén correctamente conectados puesto que existe la posibilidad que los cables estén intercambiados y por tanto el conexionado físico no respete el sentido preestablecido del anillo.

En este punto es necesario conectarse por consola mediante el cable RS-232 a cada nodo y valiéndose de las direcciones ATM de cada uno, comprobar que están conectados en el lugar adecuado. Para ello se utilizan los comandos “*vap”* y “*pgstats*”, el primero sirve para obtener la dirección ATM del nodo en que se ejecute y el segundo muestra las estadísticas ATM de los puertos conectados al nodo en el slot 3 (CSM).

En la figura 4.9 se muestra la salida del comando *“vap”* en el nodo SdeI. En esta figura se puede observar que el puerto 1 del slot 2 (FCSM) es el encargado del transporte en ATM, y por tanto, para obtener la dirección ATM del nodo, se anota la dirección que aparece resaltada en ella.

```
$SdeI/Interface/ATM >vap

ATM Port Table

                                                Conn Tran   Media UNI Max  VPI  VCI
Slot Port       ATM Port Description            Type Type   Type  Typ VCC  bits bits
==== ==== ============================ ==== ====== ===== === ==== ==== ====
2    1     ATM PORT                      SVC    --    --   Pri 1023 0    10
……
                                      End System   Sig  Sig  ILMI   ILMI ILMI
Slot Port      ATM Network Prefix     Identifier   Ver  VCI  Enable VCI  Poll
==== ==== ========================  ============ === ==== ====== ==== ====
2    1   3903488001bc90000101dbe2a0 00d09540d850 3.0 5    True   16    Off

Status
========
……
Slot Port            Phy Up                  Phy Down      Up    Dn   Status
==== ==== ======================= ================== ===== ===== ======
2    1    WED FEB 11 12:33:17 2015       --------          1    0  Enb(SVC)
Slot Port Tx Seg Sz Rx Seg Sz Tx Buff Sz Rx Buff Sz
==== ==== ========== ========== ========== ==========
2    1        131072     131072       8192       8192
……
                                                    Max  Max  Cfgd Cfgd
Slot Port         ATM Address                       VPCs VCCs VPCs VCCs
==== ==== ========================================== ==== ==== ===== ====
2    1    3903488001bc90000101dbe2a00020da00004000 3    1022 0     23
3    1    3903488001bc90000101dbe2a00020da00008000 3    1022 0     8
3    2    3903488001bc90000101dbe2a00020da00008800 3    1022 0     7
3    3    3903488001bc90000101dbe2a00020da00009000 3    1022 0     1
3    4    3903488001bc90000101dbe2a00020da00009800 3    1022 0     0
3    5    3903488001bc90000101dbe2a000d0950000a000 3    1022 0     0
3    6    3903488001bc90000101dbe2a000d0950000a800 3    1022 0     1
…
```

Figura 4.9. Salida del comando vap (SdeI)

Tras ejecutar el comando en el resto de los nodos del anillo, se obtienen las siguientes direcciones ATM para las interfaces 2/1:

```
SdeI:        3903488001bc90000101dbe2a00020da00004000

Náutica:     3903488001bc90000101fe7a300020da00004000

Paraninfo:   3903488001bc90000101ff28b00020da00004000

Enfermería:  3903488001bc90000101fe7e800020da00004000

Medicina:    3903488001bc90000101fe6be00020da00004000
```

A continuación, tras conocer estas direcciones, es posible ejecutar el comando "*pgstats"* para saber los nodos adyacentes del nodo en el que se ejecute; Por ejemplo para el nodo de Enfermería se obtiene la salida del comando *"pgstats"* que aparece en la figura 4.10.

```
$Enfermeria /Networking/PNNI >pgstats
                PNNI Port Basic Statistical Information

                                    Hellos      PTSPs    Dbase Sum Pdus
     Neighbor             Intf  Xmtd/Rcvd  Xmtd/Rcvd  Xmtd/Rcvd
==================== ====== ========== ========== ==========
3903488001bc90000101   3/ 1       1532        141          7
fe6be00020dafe6be000                1402        118          3

3903488001bc90000101   3/ 2       1530        152          7
ff28b00020daff28b000                1528        110          2
```

Figura 4.10. Salida del comando pgstats (Enfermería)

Si se contrastan las direcciones que aparecen en la figura 4.10 con las direcciones ATM presentadas anteriormente, se comprueba que no coinciden por completo, esto es debido a que en la figura 4.10 los primeros 26 caracteres se corresponden con el prefijo de red ATM y los 14 restantes hacen referencia al identificador de la estación final. Teniendo en cuenta únicamente el prefijo de red ATM, es posible diferenciar a que nodo corresponde cada dirección. Por tanto, a la interfaz 3/1 del nodo de Enfermería se conecta el nodo de Medicina y a la interfaz 3/2 se conecta el nodo del Paraninfo. Agrupando la información en cada nodo se obtiene el diagrama físico de la red que se presenta en la figura 4.11 siendo cada par de conectores de fibra óptica como los que se muestran en la figura 4.12.

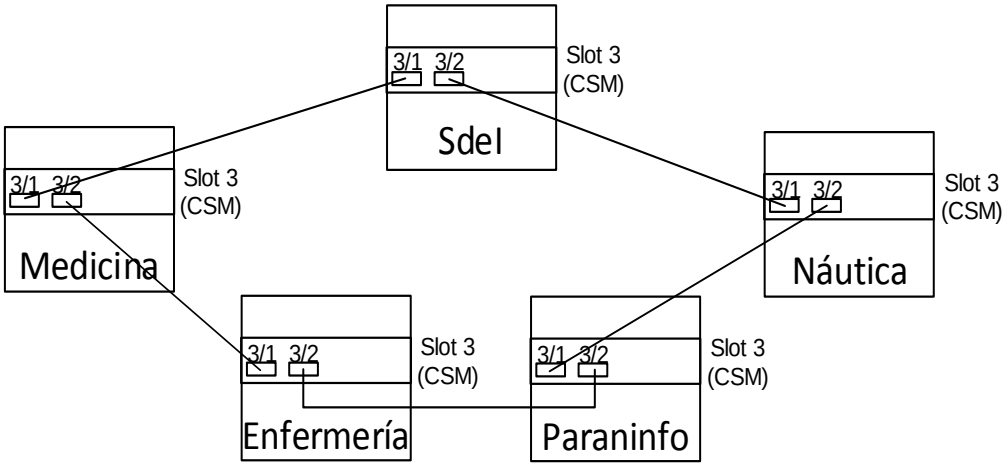


Figura 4.11. Conexionado físico de la red dorsal

Figura 4.12. Conectores de fibra en el slot CSM

Conexionado lógico

Sobre la configuración física analizada en el apartado anterior, se implementa la configuración lógica que se muestra en la figura 4.15. Dicha configuración lógica tiene una topología en forma de estrella a diferencia del anillo visto en la configuración física. A continuación se comprueba que dicha estrella es tal y como se muestra en la figura 4.15.

Es necesario conocer los servicios ATM de datos asociados a cada nodo. Para ello, se hace uso del comando *"vas"*, que muestra todos los servicios ATM creados en el nodo. Dado que el nodo central de la estrella es el nodo del SdeI, se ejecuta el comando en dicho nodo tal y como se muestra en la figura 4.13.

```
$SdeI/Services >vas
                          ATM Services

           Serv              Service              Service
Slot  Port Num             Description            Type
==== ==== ==== ============================== =========
2     1    6    Enlace Datos Torrelavega       PTOP 1483
2     1    7    Enlace Datos Enfermeria        PTOP 1483
2     1    8    Enlace Datos Paraninfo         PTOP 1483
2     1    9    Enlace Datos Medicina          PTOP 1483
2     1    10   Enlace Datos Marina            PTOP 1483

                          ATM Services

           Serv VC    Oper
Slot  Port Num  Typ   Status   SEL Groups      Conn VPI/VCI (Addrs Index)
==== ==== ==== === ======== === ==========  ==========================
2     1    6    PVC Enabled  N/A 9              0/179
2     1    7    PVC Enabled  N/A 6              0/202
2     1    8    PVC Enabled  N/A 7              0/201
2     1    9    PVC Enabled  N/A 4              0/203
2     1    10   PVC Enabled  N/A 3              0/200
```

Figura 4.13. Salida del comando *"vas"* (Sdel)

De la información mostrada en la figura 4.13 hay que fijarse en el número de conexión VPI/VCI que corresponde a cada enlace de datos, para así, poder identificar en la tabla que se obtiene tras ejecutar el comando "*vvc"* (con el que se obtiene información relevante sobre la configuración ATM) la conexión del slot 3 que le corresponde a cada nodo. Para ello, en la primera tabla de la figura 4.13 se obtiene el número de servicio que tiene asignado cada enlace de datos y posteriormente, en la segunda, se localiza el número de circuito virtual que tiene asociado cada uno (Enfermería: 0/202, Paraninfo: 0/201, Medicina: 0/203 y Náutica: 0/200). Por último se ejecuta el comando "*vvc"* tal y como se muestra en la figura 4.14.

```
$SdeI/Interface/ATM >vvc
……
                              CSM Connections
      Incoming                Outgoing
------------------- ------------------- Connection       Chan  Transport
Slot Port VPI  VCI  Slot Port VPI  VCI   Description      Type  Priority
==== ==== ==== ==== ==== ==== ==== ==== ================ ===== ========
2    1    0    5    2    1    0    1022 Connection 5     VC UNI UBR     &
2    1    0    16   2    1    0    1021 Connection 16    VC UNI UBR     &
2    1    0    18   2    1    0    1020 Connection 18    VC UNI UBR     &
2    1    0    200  3    2    0    35   Connection 200   VC UNI UBR     @
2    1    0    201  3    2    0    34   Connection 201   VC UNI UBR     @
2    1    0    202  3    1    0    36   Connection 202   VC UNI UBR     @
2    1    0    203  3    1    0    33   Connection 203   VC UNI UBR     @
2    1    0    300  3    1    0    35   Connection 300   VC UNI UBR     @
……
```

Figura 4.14. Salida del comando *"vvc"* (Sdel)

En dicha figura se observa que las conexiones virtuales de cada nodo anotadas anteriormente pasan de la interfaz FCSM 2/1 (Incoming) a las interfaces de salida CSM (Outgoing) y se ve que el tráfico sale hacia los nodos de Náutica y Paraninfo por la interfaz 3/2 mientras que para los nodos de Medicina y Enfermería lo hace por la interfaz 3/1. De esta forma, se obtiene la configuración lógica de la figura 4.15.

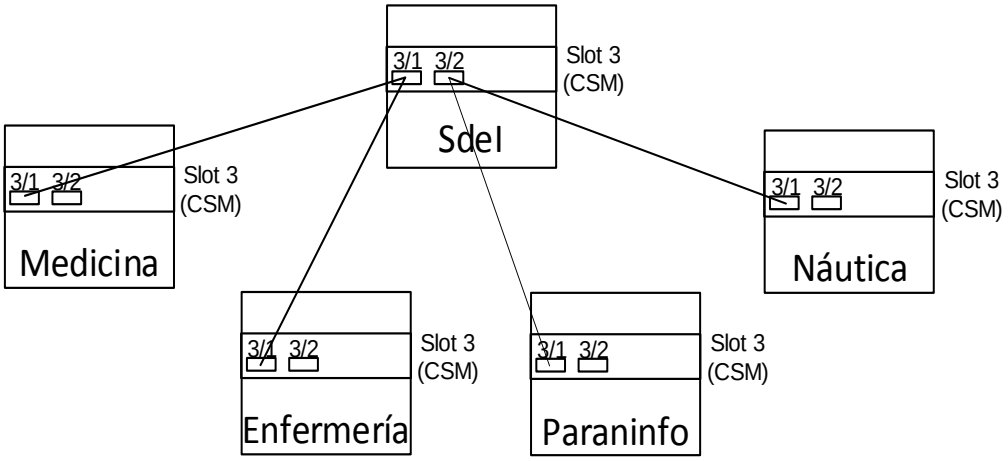


Figura 4.15. Configuración lógica de la red dorsal

4.2.3 Conexionado de la red de acceso de usuario

Como se puede apreciar en la figura 4.16, el laboratorio dispone de un total de 12 ordenadores de sobremesa, sirviendo los equipos “pc1” a “pc10” como equipamiento docente para las distintas asignaturas que se imparten en el aula. El equipo situado más a la derecha en la fila superior (tlmat-28327af28) se utiliza para el acceso por consola a los nodos. El Laboratorio de Aplicaciones Telemáticas dispone de un armario de conexiones en el que se encuentran un Switch de 16 puertos, un patch panel de 32 puertos que interconecta los cables provenientes de las tomas de pared a las que se conectan los equipos y otro patch panel de 16 puertos que enlaza con las tomas situadas sobre los nodos. En un primer momento, si no se realiza ningún cambio en el cableado del laboratorio, todos los equipos destinados para uso docente se encuentran conectados por cable Ethernet (conectores RJ45) a una toma de pared cercana que los transporta al patch panel de 32 puertos y cada uno de estos cables se encuentra conectado a un puerto del Switch tal y como se ve en la figura 4.17.

Como se describió en el capítulo 1 cuando se detalló la organización del Laboratorio de Telemática, los dispositivos a tener en cuenta para proporcionar conectividad al Laboratorio de Aplicaciones Telemáticas son el Router Cisco2600 y el Servidor Atlas. Para realizar la función de dar salida a Internet al laboratorio se utiliza el nodo del SdeI mediante una conexión directa entre el puerto 5/1 de este nodo y el router Cisco2600 del Laboratorio de Telemática. Cuando se enciende el nodo SdeI, el equipo “Júpiter” actúa como servidor DHCP para los equipos conectados al Switch situado en el patch panel. Esta funcionalidad es debida a que existe una conexión entre el equipo “Júpiter” con el puerto 5/29 del nodo SdeI, y a su vez, el nodo SdeI está conectado al puerto 1 del Switch a través de la conexión entre el puerto 5/32 y la toma de pared número 22.

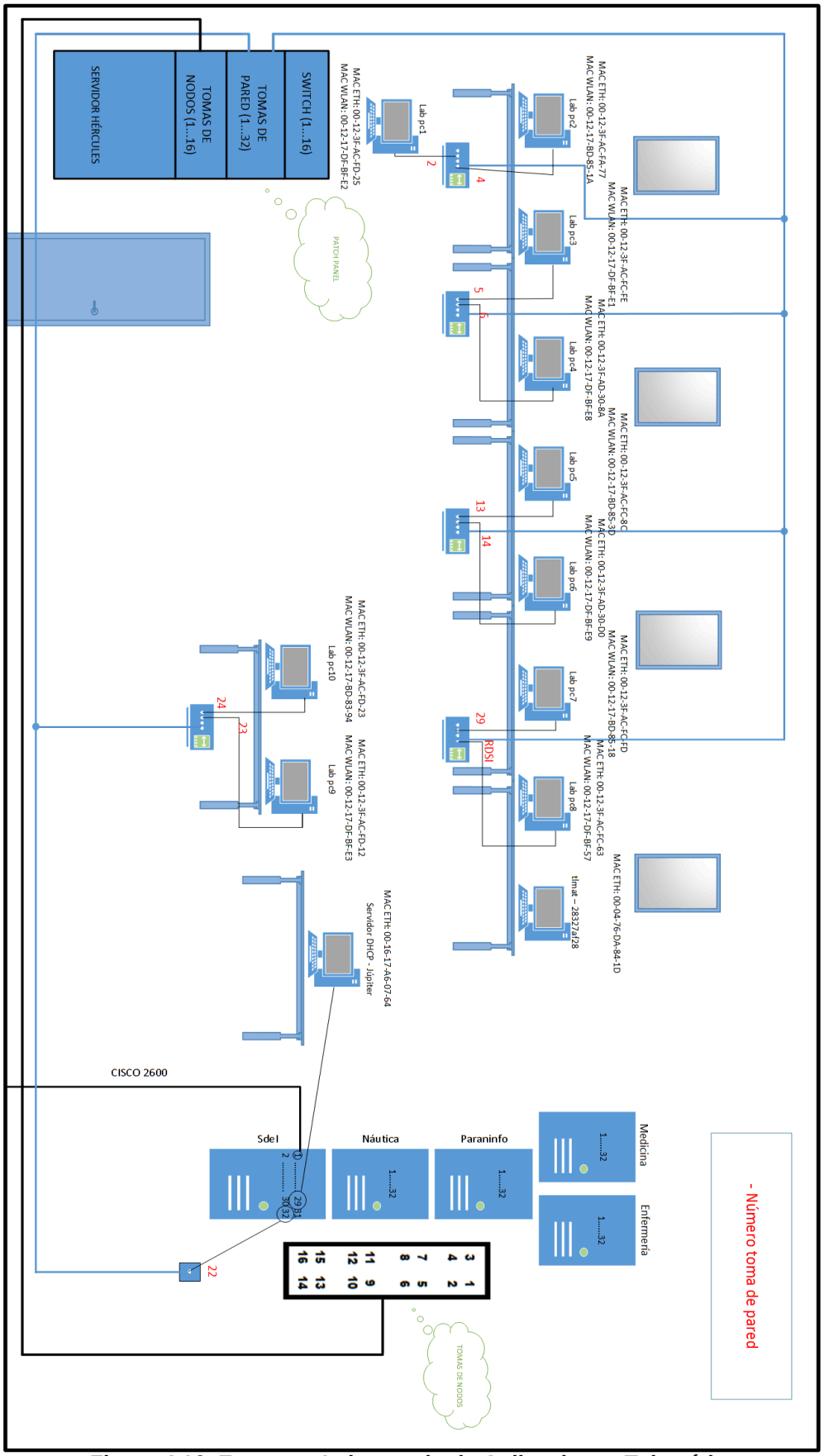


Figura 4.16. Esquema Laboratorio de Aplicaciones Telemáticas

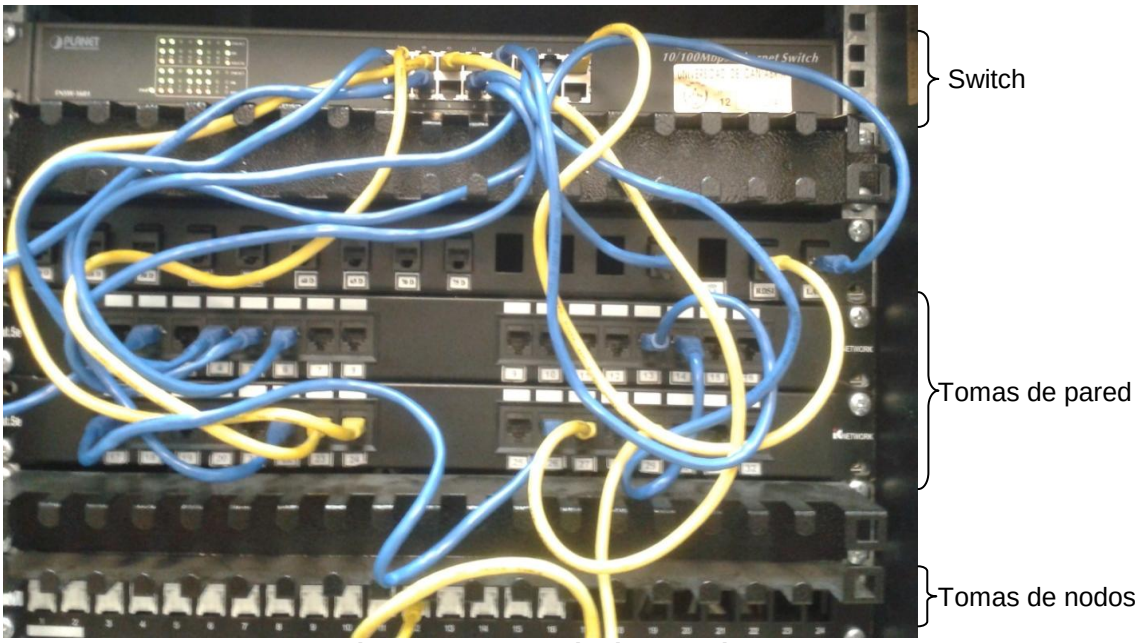


Figura 4.17. Armario de conexiones

Si se quiere conectar un PC a un nodo, es necesario tener en cuenta que las tomas de pared tienen asignados puertos del 1 al 32, y el Switch y las tomas de los nodos tienen un rango de puertos entre 1 y 16 y por tanto, para algunos equipos no se corresponde el número de toma de pared con el número de puerto asignado en el Switch. Debido a esto, la forma más simple de conectar un equipo directamente a un nodo, es conectar el número de toma de pared que se corresponda con el equipo deseado a una toma de nodo siguiendo la asignación que tenía previamente en el Switch. Para aclarar este método de conexión, se va a utilizar la figura 4.18 que representa de forma más simplificada las conexiones en el patch panel.

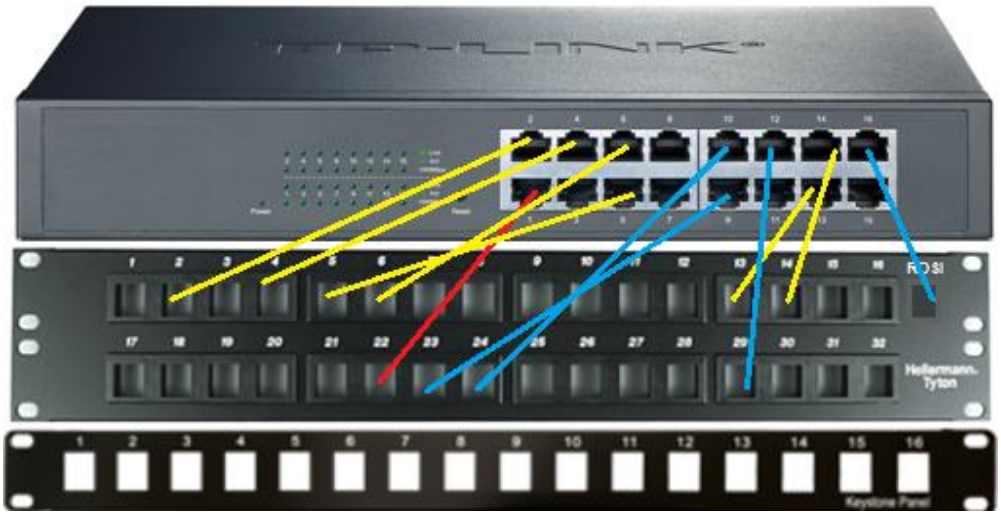


Figura 4.18. Armario de conexiones simplificado

En la figura anterior, el enlace rojo representa la conexión entre el servidor DHCP, a través del nodo Sdel, y el Switch. Los enlaces amarillos representan las conexiones entre los equipos y el Switch con un número de toma de pared menor de 16 y los enlaces azules representan, por el contrario, las conexiones entre los equipos y el Switch con un número de toma de pared mayor de 16 y que, por tanto, tienen un número asignado en el Switch diferente. Por tanto, a modo de resumen, las conexiones existentes son:

Toma pared Switch

- 2 → 2 (pc1)
- 4 → 4 (pc2)
- 5 → 5 (pc3)
- 6 → 6 (pc4)
- 13 → 13 (pc5)
- 14 → 14 (pc6)
- 23 → 9 (pc9)
- 24 → 10 (pc10)
- 29 → 12 (pc7)
- RDSI → 16 (pc8)

Aunque no es obligatorio, para conectar un equipo a un nodo, la mejor forma es conectarlo al mismo número de toma de nodo que tenía el equipo asignado en el Switch. Por ejemplo, el equipo "pc7" conectado a la toma de pared número 29 está conectado al puerto 12 del Switch, y para posibilitar que se pueda conectar a un nodo la mejor opción es conectarlo a la toma de nodo número 12. Posteriormente para conectar el equipo a un nodo, se conectaría el cable Ethernet de la toma número 12 del cajetín situado sobre los nodos al nodo que corresponda.

Es necesario distinguir la dirección física de cada ordenador, ya que a la hora de analizar el tráfico de datos con el analizador de protocolos "Wireshark" se usará esta dirección para identificar el equipo que envía o recibe la trama. Las direcciones MAC de los distintos equipos que aparecen en la figura 4.16 se pueden extraer de varias formas. La más cómoda es utilizar el símbolo del sistema (cmd) e introducir el comando *"ipconfig/all"* para poder ver entre otras cosas la dirección Ip de la máquina, la puerta de enlace…y su dirección física. Para que aparezca únicamente la dirección física, existe la opción de escribir el comando *"getmac /fo list /v"*.

4.3 Configuración de la red

En este apartado se analiza la configuración de partida de la red con el objetivo de obtener conclusiones sobre las modificaciones que se han de realizar. Posteriormente, se configuran los nodos de forma adecuada para que la red funcione como se desea y se muestran los resultados de configuración, obteniendo el dimensionado completo de los Laboratorios de Ingeniería Telemática.

4.3.1 Configuración inicial

En este punto, como se ha indicado previamente, se estudia la configuración inicial de los nodos para poder discernir qué modificaciones deben realizarse.

En la configuración inicial, todos los nodos presentan 2 grupos dedicados a la difusión de VLANs (ver figura 4.19), uno correspondiente al colectivo universitario "Group

1:University" y otro correspondiente a un colectivo externo "Group 2:Other", que tienen asignados todos los puertos en cada uno de los nodos tal y como se puede ver en la figura 4.20 a través del comando *"via"* (el grupo 101 tiene 28 puertos asignados y el grupo 102 los 4 puertos restantes).

```
$Nautica / >gp
Group                                Network Address  Proto/
 ID          Group Description      (IP Subnet Mask)  Encaps
(:VLAN ID)                          or (IPX Node Addr)
===== ============================== =============== ========
    1 Default GROUP (#1)             192.168.3.1       IP  /
                                       (ff.ff.ff.00 )   ETH2
    2 Enlace Marina-SdI              192.168.0.2       IP  /
                                       (ff.ff.ff.fc )   ETH2
  101 Group1:University              192.168.101.33    IP  /
                                       (ff.ff.ff.e0 )   ETH2
  102 Group2:Other                   192.168.102.33    IP  /
                                       (ff.ff.ff.e0 )   ETH2
```

Figura 4.19. Salida del comando *"gp"* (Náutica)

```
$Nautica / >via 101
                  GROUP Interface Attachments For GROUP 101
GROUP:                                Service/                  Admin
Slot/Intf         Description          Instance       Protocol   Status
========== ========================== ============   ============ =======
  101.1 :* Group1:University              Rtr / 2      IP         Enabled
  101:4/1  Virtual port (#1)              Brg / 1      Tns        Enabled
  ……
  101:4/28 Virtual port (#28)             Brg / 1      Tns        Enabled
$Nautica / >via 102
                  GROUP Interface Attachments For GROUP 102
GROUP:                                Service/                   Admin
Slot/Intf         Description          Instance       Protocol   Status
========== ========================== ============   ============ =======
  102.1 :* Group2:Other                   Rtr /  3      IP         Enabled
  102:4/29 Virtual port (#29)             Brg /  1      Tns        Enabled
  ……
  102:4/32 Virtual port (#32)             Brg /  1      Tns        Enabled
```

Figura 4.20. Salida del comando *"via"* (grupos 101 y 102 de Náutica)

Las direcciones IP de la figura 4.19 incluidas tanto para el grupo por defecto (que no debería tener ninguna asignada) como para los grupos creados para difundir las VLANs son incorrectas, ya que el router Cisco2600 del Laboratorio de Telemática no tiene rutas configuradas para direccionar estas VLANs. Este hecho es fácilmente comprobable observando la figura 4.21, en la que se ve la realización de un telnet al router Cisco2600 y se muestra la tabla de rutas ejecutando la orden *"show ip route"*.

```
alumnos@labpc8:~$ telnet 192.168.0.22
Trying 192.168.0.22...
Connected to 192.168.0.22.
Escape character is '^]'.
User Access Verification
Password: (git)
c2600>show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
…
* - candidate default, U - per-user static route, o - ODR
Gateway of last resort is 192.168.110.11 to network 0.0.0.0
C 192.168.110.0/24 is directly connected, FastEthernet0/0
S 192.168.10.0/24 [1/0] via 192.168.0.21
S 192.168.11.0/24 [1/0] via 192.168.0.21
192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
S 192.168.0.0/24 [1/0] via 192.168.0.21
C 192.168.0.20/30 is directly connected, FastEthernet0/1
S 192.168.1.0/24 [1/0] via 192.168.0.21
S 192.168.2.0/24 [1/0] via 192.168.0.21
S 192.168.3.0/24 [1/0] via 192.168.0.21
S* 0.0.0.0/0 [1/0] via 192.168.110.11
```

Figura 4.21. Telnet al router Cisco2600

Como se puede ver en la figura 4.21, el Router Cisco2600 direcciona una serie de redes (192.168.10.0/24, 192.168.11.0/24, 192.168.0.0/24, 192.168.1.0/24, 192.168.2.0/24 y 192.168.3.0/24) a través de su interfaz FastEthernet0/1 vía la dirección 192.168.0.21 perteneciente al nodo SdeI. Estas redes se utilizarán para dimensionar el Laboratorio de Aplicaciones Telemáticas y posibilitar la transmisión de VLANs por los nodos.

Siguiendo con las comprobaciones del estado inicial, mediante el comando *"atvl"* que se muestra en la figura 4.22 se comprueba que el grupo 101 contiene las 3 VLANs a difundir, y se llega a la conclusión de que la configuración inicial es incorrecta, ya que para cada grupo solo debe configurarse una VLAN (que aparece automáticamente tras la creación del grupo), porque en caso contrario no se difunden de forma correcta [2].

```
$Nautica / >atvl
VLAN   VLAN   VLAN                              Admin     Operational
Group:Id      Description                       Status    Status
-------------------------------------------------------------------
  101: 2      Vlan1:Staff                     Enabled   Inactive
  101: 3      Vlan2:Research                  Enabled   Inactive
  101: 4      Vlan3:Students                  Enabled   Inactive
```

Figura 4.22. Salida del comando *"atvl"* (Náutica)

Debido a estos errores en la configuración, se hace necesario comenzar desde el principio con la creación de VLANs, así como con la creación de los circuitos ATM para que éstas puedan difundirse a través de los nodos.

Sin embargo, siguiendo con el repaso del estado de configuración inicial de los nodos, se podrán mantener algunas configuraciones iniciales tales como el direccionamiento y los circuitos de datos punto a punto entre el nodo SdeI y el resto de nodos, parte de la configuración de las traps SNMP que se verá más adelante, o los parámetros de red necesarios (establecidos por defecto) para conectar directamente desde un PC al nodo SdeI mediante un cable Ethernet que aparecen en la figura 4.23.

```
$SdeI/Interface >ethernetc

                          Ethernet Port Configuration

 1) Port Admin status UP    : Yes
 2) IP Address              : 192.168.11.1
 3) Subnet Mask             : 255.255.255.0
 4) Bcast Address           : 192.168.11.255
 5) Gateway Address         : UNSET
 6) Remote Host Address     : UNSET
 7) Remote Host Subnet Mask : UNSET
 8) RIP Mode                : Inactive

Command {Item=Value/?/Help/Quit/Redraw/Save} (Redraw)   : q
```

Figura 4.23. Salida del comando *"ethernetc"*

Por tanto, la conexión directa con el nodo SdeI (mediante cable Ethernet al módulo MPM) tendrá que realizarse desde un equipo perteneciente a la red 192.168.11.0/24.

4.3.2 Configuración final

Tras la comprobación del estado de configuración inicial de los nodos y como ya se avanzó en el punto anterior, se decidió comenzar desde el principio con la creación de las reglas necesarias para poner la red operativa. Por esto, la primera tarea a realizar será borrar la configuración anterior para que no cause conflicto con la que se desea implantar. Como ejemplo se expondrá a continuación el borrado de la configuración inicial en el nodo de Náutica.

En primera instancia es necesario comprobar los grupos creados en cada nodo para localizar cuáles han de ser eliminados. Esta comprobación se realizó en el apartado 4.3.1 mediante el comando "*gp*", que aparece en la figura 4.19. Los grupos a eliminar son el 101 "*Group1:University*" y el 102 "*Group2:Other*". Un grupo no se puede eliminar mientras tenga puertos asignados o VLANs configuradas, y como se observó previamente en las figuras 4.20 y 4.22, el grupo 101 tenía 28 puertos y 3 VLANs asignadas mientras que el grupo 102 tenía también 4 puertos configurados que son necesarios eliminar para completar el borrado del grupo. Los comandos a utilizar para realizar esta tarea son: *"rmvp"* comando que posibilita el borrado de puertos añadiendo el grupo y el slot/puerto a eliminar (que automáticamente pasará a formar parte del grupo por defecto) y que se puede ver en la figura 4.24, "*rmatvl"* para suprimir las VLANs configuradas (ver figura 4.25) y finalmente el comando *"rmgp"* para eliminar definitivamente el grupo tal y como se observa en la figura 4.26.

```
$Nautica / >rmvp 101 4/1
Local port 1 (Virtual po...) is attached to this slot/interface - remove?
(n)y
 BRIDGE port on 4/1 moved to GROUP 1.
……
$Nautica / >rmvp 101 4/28
Local port 28 (Virtual po...) is attached to this slot/interface - remove?
(n)y
 BRIDGE port on 4/28 moved to GROUP 1.

$Nautica / >rmvp 102 4/29
Local port 29 (Virtual po...) is attached to this slot/interface - remove?
(n)y
……
$Nautica / >rmvp 102 4/32
Local port 32 (Virtual po...) is attached to this slot/interface - remove?
(n)y
 BRIDGE port on 4/32 moved to GROUP 1.
```

Figura 4.24. Borrado puertos grupos 101 y 102 (Náutica)

```
$Nautica / >rmatvl 101:2
Delete VLAN 101: 2 ? (n): y
VLAN 101: 2 deleted
$Nautica / >rmatvl 101:3
Delete VLAN 101: 3 ? (n): y
VLAN 101: 3 deleted
$Nautica / >rmatvl 101:4
Delete VLAN 101: 4 ? (n): y
VLAN 101: 4 deleted
```

Figura 4.25. Borrado VLANs grupo 101 (Náutica)

```
$Nautica / >rmgp 101
 GROUP 101 removed.
$Nautica / >rmgp 102
 GROUP 102 removed.
```

Figura 4.26. Borrado definitivo grupos 101 y 102 (Náutica)

Para comprobar que el borrado se ha completado correctamente, se ejecuta de nuevo el comando *"gp"* en el nodo de Náutica como se puede ver en la figura 4.27 y se compara con la figura 4.19, observando que los grupos 101 y 102 han sido eliminados.

```
$Nautica / >gp
Group                                Network Address  Proto/
 ID          Group Description      (IP Subnet Mask)  Encaps
(:VLAN ID)                          or (IPX Node Addr)
===== ============================== ============== ========
    1 Default GROUP (#1)             192.168.3.1       IP  /
                                       (ff.ff.ff.00 )   ETH2
    2 Enlace Marina-SdI              192.168.0.2       IP  /
                                       (ff.ff.ff.fc )   ETH2
```

Figura 4.27. Comprobación borrado grupos 101 y 102 (Náutica)

Después de completar el borrado de grupos en todos los nodos, se realizan algunas modificaciones básicas en la configuración como paso previo a la modelación de la red final. En la figura 4.28 aparecen cambios de datos relacionados con el sistema (persona de contacto, nombre y descripción) haciendo uso del comando "*syscfg"* en el nodo SdeI y en la figura 4.29 se ve el cambio de hora efectuado en el nodo de Medicina usando en este caso el comando *"dt"*.

```
$SdeI/System >syscfg

System Contact                : Pilar
System Name                   : SdI
System Location               : V-Pino
System Description            : Nodo ATM SdI
Duplicate MAC Aging Timer     : 0 (not configured)
Change any of the above {Y/N}? (N) : y
System Contact (Pilar) : Eugenio
System Name (SdI) : SdeI
System Location (V-Pino) :
System Description (Nodo ATM SdI) : Nodo ATM SdeI
Duplicate Mac Aging Timer (0) :
```

Figura 4.28. Cambio datos de sistema (SdeI)

```
$Medicina /System >dt

                      Modify Date and Time Configuration

 1) Local time                    : 16:12:23
 2) Local date                    : 11/06/14
 3) Timezone(-13..12, name)       : UTC+1 hrs
 4) Daylight Savings Time active  : Enabled
   41) DST Start Month (1..12)      : MARCH
   42) DST Start Week (1..4, Last)  : Last
   43) DST Start Day of Week (1..7) : SUNDAY
   44) DST Start Time (hh:mm)       : 2:00
   45) DST End Month (1..12)        : OCTOBER
   46) DST End Week (1..4, Last)    : Last
   47) DST End Day of Week (1..7)   : SUNDAY
   48) DST End Time (hh:mm)         : 3:00
   49) DST Offset (hh:mm)           : 1:00

Command {Item=Value/?/Help/Quit/Redraw/Save} (Redraw)  : 1=15:40:00

                      Modify Date and Time Configuration

 1) Local time                    : 15:40:00
 2) Local date                    : 11/06/14
Command {Item=Value/?/Help/Quit/Redraw/Save} (Redraw)  : save
UTC date and time:    THU NOV 06 14:40:00 2014
Local date and time:  THU NOV 06 15:40:00 2014
```

Figura 4.29. Cambio hora (Medicina)

Una vez comprobadas las configuraciones iniciales de la red, se realiza la nueva configuración para completar el dimensionado del sistema.

Circuitos y servicios ATM

La primera parte consiste en crear las conexiones virtuales (VPI/VCI) necesarias para posibilitar el tráfico entre los nodos. Como se ha descrito a lo largo del presente documento, se utiliza ATM como tecnología de backbone y el intercambio de datos entre switches ATM se realiza mediante circuitos virtuales. Se mantienen las conexiones de datos (0/200, 0/201, 0/202 y 0/203) que estaban creadas previamente y se crean los circuitos que posibilitan el transporte de VLANs a lo largo del anillo.

Los circuitos a crear, al igual que los circuitos de datos, son del tipo SoftPVC desde el SdeI hasta los distintos nodos. Un SoftPVC se beneficia de las ventajas de un circuito tipo PVC y de uno tipo SVC, puesto que se crea un PVC entre el nodo origen y el nodo

destino, mientras que en la parte interna de la red se establecen circuitos SVC (que conmutan en función del número de saltos para llegar al destino) lo que posibilita un cambio en la configuración en caso de fallo en los enlaces del anillo. Por esto, la configuración lógica de la figura 4.15 es válida cuando el sistema funciona con normalidad pero puede sufrir modificaciones si ocurren fallos inesperados en la red.

Posteriormente, se asocia un servicio de Trunking al circuito SoftPVC creado. Este servicio tiene que configurarse en cada extremo (nodos) y se debe asociar al SoftPVC establecido desde el SdeI. Una vez se hayan creado las VLANs a difundir, es necesario asociar los grupos a estos servicios de Trunking con el fin de permitir que distintas VLANs viajen por el mismo circuito virtual.

El comando necesario para la creación del SoftPVC es *"scvc 2/1 VPI/VCI"* y para la creación del servicio de Trunking *"cas 2/1"*, especificando en cada uno de ellos los parámetros concretos de cada nodo. En ambos casos se trabaja sobre la interfaz interna 2/1 (módulo FCSM) que no tiene puertos físicos pero que configurando los servicios ATM en ella posibilita la comunicación entre switches. En las figuras 4.30 y 4.31 se muestra la creación del circuito SoftPVC y el servicio ATM necesarios para posibilitar que se difundan las VLANs SdeI – Paraninfo (En Paraninfo también se debe crear el servicio de Trunking siguiendo el mismo procedimiento).

```
$SdeI/ >scvc 2/1 0/403
Slot 2 Port 1 Connection VPI 0 VCI 403 Configuration
Available bandwidth: Tx=353208 Rx=353208
1)  Description (30 chars max)  : Connection 403
2)  Endpoint Id (1)             : 1
3)  Terminating ATM Address     : 00000000000000000000000000000000000000000000
4)  Other End VPI (0..4095)     : 1
5)  Other End VCI (0..65535)    : 1
6)  Channel Type { vc-nni(3), vc-uni(4) }              : VC-UNI
7)  Transport Priority {CBR(1), CBR_PRS(2), VBR_RT(3), : UBR
VBR_NRT(4), ABR(5), UBR(6) }
8)  Point to Multipoint { disable(0), enable(1) }      : Disabled
10) AAL5 Discard Continue { disable(0), enable(1) }    : Disabled
11) Traffic Parameters
13) Advanced Parameters
14) Target Selector Type {required(1), any(2) }        : required
15) SoftPvc Retry parameters
16) Broadband Bearer Capability Parameters
Enter (option=value/save/cancel) : 1=Difusion VLANs Paraninfo
Enter (option=value/save/cancel):3=3903488001bc90000101ff28b00020da00004000
Enter (option=value/save/cancel) : 4=0
Enter (option=value/save/cancel) : 5=403
```

Figura 4.30. Creación SoftPVC SdeI-Paraninfo

```
$SdeI/ >cas 2/1
   Slot 2 Port 1 Service 3 Configuration
1)  Description (30 chars max)        : PTOP Bridging Service 3
2)  Service type { LANE client(1),
                   1483 Scaling (2)
                   Trunking (4),
                   Classical IP(5),
                   PTOP Bridging(6),
                   VLAN cluster(7)  } : PTOP Bridging
    10) Encaps Type { Private(1),
                      RFC1483(2) }    : Private
3)  Connection Type { PVC(1),
                      SVC(2) }        : PVC
4)  PTOP Group                        : 1
5)  PTOP connection                   : none
6)  Admin Status { disable(1),
                   enable(2) }        : Enable
7)  BandWidth Group (1-8)             : 1

Enter (option=value/save/cancel) : 2=4
```

➢ Servicio de Trunking

```
    Slot 2 Port 1 Service 3 Configuration
1)  Description (30 chars max)        : Trunking Service 3
2)  Service type { LANE client(1),
                   1483 Scaling (2)
                   Trunking (4),
                   Classical IP(5),
                   PTOP Bridging(6),
                   VLAN cluster(7)  } : Trunking
3)  Connection Type { PVC(1),
                      SVC(2) }        : PVC
4)  Trunked Groups                    : 1
5)  Connection                        : none
6)  Admin Status { disable(1),
                   enable(2) }        : Enable
7)  BandWidth Group (1-8)             : 1
Enter (option=value/save/cancel) : 5=403
Enter (option=value/save/cancel) : save
Creating service, please wait...
Enabling service...
```

Figura 4.31. Creación servicio Trunking SdeI-Paraninfo

Para comprobar que los circuitos se han creado correctamente, se ejecuta el comando *"svvc"* en ambos extremos tal y como aparece en la figura 4.32 para el nodo del SdeI y en la figura 4.33 para el nodo del Paraninfo.

```
$SdeI/ >svvc
                              Incoming Soft PVCs
Slot Port VPI  VCI         Originating Atm Addresss                OtherEnd
==== ==== ==== ==== ======================================      ====     ====

 +  ==> PVC Connections
 #  ==> MPLS Connections
 *  ==> SVC Connections which cannot be modified by the user
 @  ==> Soft PVC Connections
 &  ==> Control Connections
                              CSM Connections
     Incoming           Outgoing
------------------ ------------------   Connection         Chan  Transport
Slot  Port VPI VCI  Slot Port VPI  VCI   Description         Type  Priority
==== ==== ==== === ==== ==== ==== ==== ================   ====== =========
2    1    0    200  3    2    0    33   Connection 200       VC UNI UBR    @
2    1    0    201  3    2    0    35   Connection 201       VC UNI UBR    @
2    1    0    202  3    1    0    36   Connection 202       VC UNI UBR    @
2    1    0    203  3    1    0    35   Connection 203       VC UNI UBR    @
2    1    0    300  3    1    0    34   Connection 300       VC UNI UBR    @
2    1    0    402  3    2    0    32 Difusion VLANs SdI-Nau VC UNI UBR    @
2    1    0    403  3    2    0    34 Difusion VLANs Paranin VC UNI UBR    @
2    1    0    404  3    1    0    33 Difusion VLANs SdI-Enf VC UNI UBR    @
2    1    0    405  3    1    0    32 Difusion VLANs SdI-Med VC UNI UBR    @

Slot Port VPI  VCI  EndPt       Terminating Atm Address             OtherEnd
                    Id                                            Vpi   Vci
==== ==== ==== ==== ===== ================================      ==== =====
2    1    0    200  1     3903488001bc90000101fe7a300020da00004000  0    200
2    1    0    201  1     3903488001bc90000101ff28b00020da00004000  0    201
2    1    0    202  1     3903488001bc90000101fe7e800020da00004000  0    202
2    1    0    203  1     3903488001bc90000101fe6be00020da00004000  0    203
2    1    0    300  1     3903488001bc90000101fe7e800020da00004000  0    300
2    1    0    402  1     3903488001bc90000101fe7a300020da00004000  0    402
2    1    0    403  1     3903488001bc90000101ff28b00020da00004000  0    403
2    1    0    404  1     3903488001bc90000101fe7e800020da00004000  0    404
2    1    0    405  1     3903488001bc90000101fe6be00020da00004000  0    405
……
```

Figura 4.32. Comprobación circuitos SoftPVC (SdeI)

```
$Paraninfo / >svvc
                              Incoming Soft PVCs
Slot Port VPI  VCI         Originating Atm Addresss                OtherEnd
                                                                   Vpi      Vci
==== ==== ==== ==== ======================================      ====     ====
2    1    0    201  3903488001bc90000101dbe2a00020da00004000     0        201
2    1    0    403  3903488001bc90000101dbe2a00020da00004000     0        403
……
```

Figura 4.33. Comprobación circuitos SoftPVC (Paraninfo)

En la figura 4.32 se pueden ver todos los circuitos SoftPVC creados en el SdeI y se resaltan los correspondientes al enlace SdeI-Paraninfo. Si se comparan las direcciones ATM que aparecen con las direcciones ATM de cada nodo expuestas en el apartado 4.2.2, se obtiene que las conexiones virtuales creadas se corresponden con:

Náutica: 0/200 y 0/402

Paraninfo: 0/201 y 0/403

Enfermería: 0/202 y 0/404 (la 0/300 no es de relevancia para el proyecto)

Medicina: 0/203 y 0/405

Por su parte, en la figura 4.33 se observan los circuitos virtuales que llegan al Paraninfo desde el SdeI y que coinciden con los resaltados en la figura 4.32.

Para comprobar la creación de los servicios de Trunking se ejecuta el comando *"vas"*, utilizado para ver los servicios ATM creados en el nodo (ver figura 4.34). Posteriormente, tras crear las VLANs, será necesario modificar los servicios de Trunking con el fin de asociar cada una a su servicio correspondiente.

```
$SdeI/ >vas
                          ATM Services
           Serv           Service        Service
Slot  Port Num           Description      Type
==== ==== ==== ======================== =========
2     1    1    Trunking Service 1       Trunking                  →Medicina
2     1    2    Trunking Service 2       Trunking                   →Náutica
2     1    3    Trunking Service 3       Trunking                 →Paraninfo
2     1    4    Trunking Service 4       Trunking                →Enfermería
2     1    6    Enlace Datos Torrelavega PTOP 1483
2     1    7    Enlace Datos Enfermeria  PTOP 1483
2     1    8    Enlace Datos Paraninfo   PTOP 1483
2     1    9    Enlace Datos Medicina    PTOP 1483
2     1    10   Enlace Datos Marina      PTOP 1483
                          ATM Services
           Serv VC    Oper
Slot  Port Num  Typ  Status  SEL Groups      Conn VPI/VCI (Addrs Index)
==== ==== ==== === ======== === ==========  ==========================
2     1    1    PVC Enabled  N/A 1              0/405
2     1    2    PVC Enabled  N/A 1              0/402
2     1    3    PVC Enabled  N/A 1              0/403
2     1    4    PVC Enabled  N/A 1              0/404
2     1    6    PVC Enabled  N/A 9              0/179
2     1    7    PVC Enabled  N/A 6              0/202
2     1    8    PVC Enabled  N/A 7              0/201
2     1    9    PVC Enabled  N/A 4              0/203
2     1    10   PVC Enabled  N/A 3              0/200
……
```

Figura 4.34. Comprobación servicios ATM (SdeI)

Según la figura 4.34, por un lado se tiene un circuito virtual (SoftPVC) por cada enlace lógico entre nodos de la red, son los denominados "circuitos de datos" y sobre ellos se define un servicio ATM punto a punto con encapsulación 802.2 LLC/SNAP (RFC1483). Los enlaces de datos del SdeI a los distintos nodos son: 0/200 (Náutica), 0/201 (Paraninfo), 0/202 (Enfermería) y 0/203 (Medicina). También aparece el 0/179 que se usó en la configuración inicial para la comunicación con el nodo de Torrelavega pero que no se usa en la nueva configuración. Mientras que por el otro lado, aparecen los circuitos virtuales 402 (Náutica), 403 (Paraninfo), 404 (Enfermería) y 405 (Medicina), también de tipo SoftPVC, sobre los que está definido un servicio de Trunking ATM para difundir las VLANs a través de los nodos.

En este punto, una vez finalizada la configuración de los circuitos virtuales y de los servicios ATM, es necesaria alguna aclaración sobre los circuitos virtuales utilizados en cada uno de los enlaces físicos. Como se comentó anteriormente, todas las conexiones (VPI/VCI) están creadas sobre la interfaz interna 2/1, pero los enlaces físicos entre los nodos se realizan a través de las conexiones de fibra de las interfaces 3/1 y 3/2. Internamente, los circuitos virtuales que aparecen son los que se han ido viendo a lo largo del proceso de configuración, estos son: 200, 201, 202, 203, 402, 403, 404, 405 y algún otro sin relevancia en el proyecto (179 y 300). Pues bien, estos circuitos para salir al exterior, sufren una transformación interna por ser circuitos conmutados (SVC) al pasar del módulo 2 (FCSM) al módulo 3 (CSM) y alteran la numeración seguida hasta el momento. En el caso habitual de que todos los nodos incluidos en el anillo funcionen con normalidad, se respeta la configuración lógica expuesta en la figura 4.15, estando definidos los circuitos de Náutica y Paraninfo por un lado (máximo 2 saltos) y los circuitos de Medicina y Enfermería por el otro (máximo 2 saltos) balanceando de esta forma el tráfico por el anillo. Para esta situación, y observando los resultados de ejecutar el comando *"vvc"* en cada uno de los equipos (ejemplo para SdeI en la figura 4.35) es posible obtener los circuitos empleados sobre cada enlace físico, resultando la figura 4.36:

```
$SdeI/ >vvc
…
                              CSM Connections
      Incoming                Outgoing
------------------- -------------------   Connection          Chan  Transport
Slot Port VPI  VCI  Slot Port VPI  VCI    Description         Type  Priority
==== ==== ==== ==== ==== ==== ==== ==== ================== ====== =========
……
2    1    0    200  3    2    0    33     Connection 200      VC UNI UBR  @
2    1    0    201  3    2    0    35     Connection 201      VC UNI UBR  @
2    1    0    202  3    1    0    36     Connection 202      VC UNI UBR  @
2    1    0    203  3    1    0    35     Connection 203      VC UNI UBR  @
2    1    0    300  3    1    0    34     Connection 300      VC UNI UBR  @
2    1    0    402  3    2    0    32 Difusion VLANs SdI-Nau VC UNI UBR  @
2    1    0    403  3    2    0    34 Difusion VLANs Paranin VC UNI UBR  @
2    1    0    404  3    1    0    33 Difusion VLANs SdI-Enf VC UNI UBR  @
2    1    0    405  3    1    0    32 Difusion VLANs SdI-Med VC UNI UBR  @
……
3    1    0    5    2    1    0    1019   Connection 5        VC UNI UBR  &
3    1    0    16   2    1    0    1018   Connection 16       VC UNI UBR  &
3    1    0    18   2    1    0    1017   Connection 18       VC UNI UBR  &
3    1    0    32   2    1    0    405    Connection 32       VC UNI UBR  *
3    1    0    33   2    1    0    404    Connection 33       VC UNI UBR  *
3    1    0    34   2    1    0    300    Connection 34       VC UNI UBR  *
3    1    0    35   2    1    0    203    Connection 35       VC UNI UBR  *
3    1    0    36   2    1    0    202    Connection 36       VC UNI UBR  *
3    2    0    5    2    1    0    1016   Connection 5        VC UNI UBR  &
3    2    0    16   2    1    0    1015   Connection 16       VC UNI UBR  &
3    2    0    18   2    1    0    1014   Connection 18       VC UNI UBR  &
3    2    0    32   2    1    0    402    Connection 32       VC UNI UBR  *
3    2    0    33   2    1    0    200    Connection 33       VC UNI UBR  *
3    2    0    34   2    1    0    403    Connection 34       VC UNI UBR  *
3    2    0    35   2    1    0    201    Connection 35       VC UNI UBR  *
3    3    0    180  2    1    0    180    Connection 180      VC UNI UBR  +
```

Figura 4.35. Salida del comando "*vvc*" (SdeI)

Tal y como se observa en la figura 4.35, los circuitos creados internamente en la interfaz 2/1 (200-203 y 402-405), entran y salen del nodo repartidos por las interfaces 3/1 y 3/2 y lo hacen mediante su homólogo para el enlace físico (32-35 para la interfaz 3/1 y 32-36 para la interfaz 3/2). No representa un problema que el circuito físico esté replicado en la red mientras sea único para el enlace en el que transita y se corresponda con un único circuito virtual. Si, por ejemplo, fallase el enlace SdeI-Náutica (interfaz 3/2), todos los circuitos irían por el enlace SdeI-Medicina (interfaz 3/1) y no podría haber ningún circuito replicado.

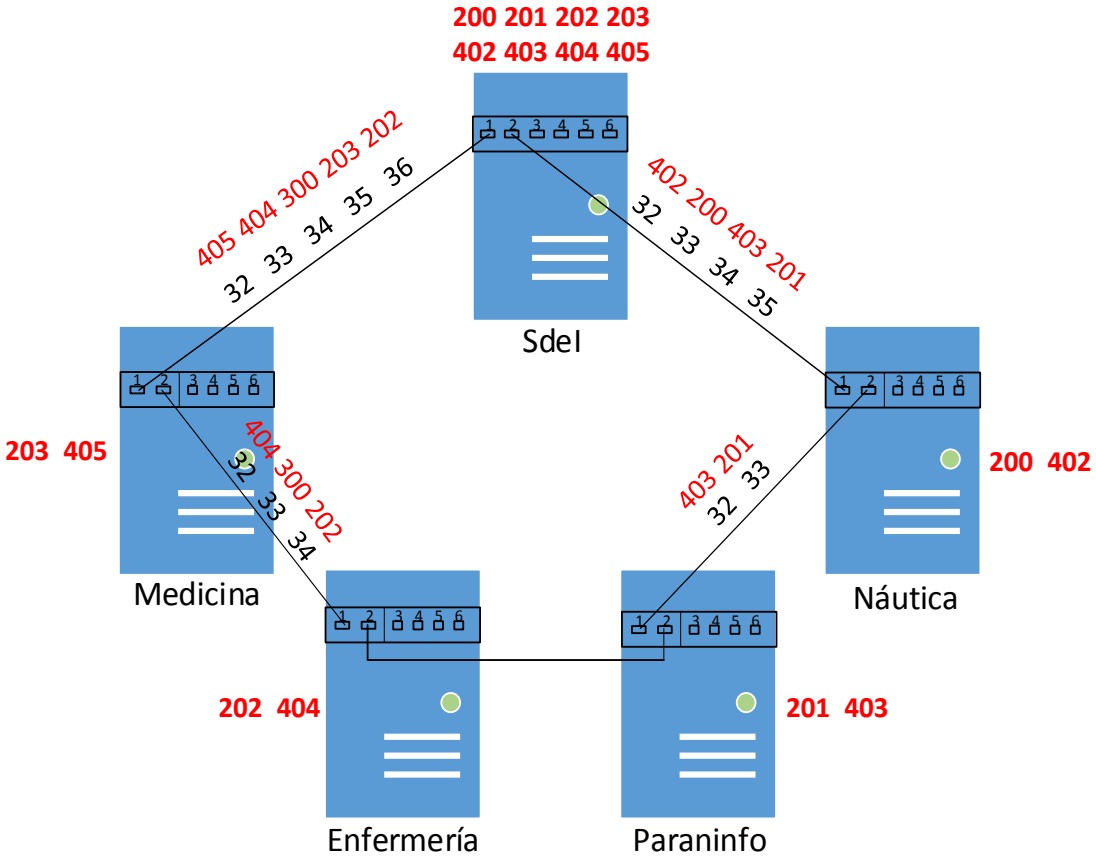


Figura 4.36. Circuitos virtuales y físicos en la red

En la figura 4.36, en negro se representan los circuitos utilizados en cada enlace físico, y justo encima de cada uno aparece su homólogo virtual con el que trabajan los nodos internamente. Los circuitos que aparecen a un lado del nodo son los que el equipo detecta que están destinados para uso en el propio nodo debido a que la dirección destino ATM del circuito virtual coincide con la suya propia, por lo que los identifica y los transforma en los circuitos virtuales ATM creados desde el SdeI. En cada nodo los circuitos en tránsito conmutan, haciendo uso de otras etiquetas libres en el enlace saliente. Como ejemplo, a Náutica llegan los circuitos 32~402, 33~200, 34~403 y 35~201. Los circuitos con destino Náutica son el 200 y el 402, por lo que los circuitos 32 y 33 llegan a su destino y son transformados internamente por su equivalente virtual, pero los circuitos 34 y 35 tienen que seguir por la red para alcanzar su objetivo, y en Náutica son conmutados a nuevas etiquetas de salida, 32 y 33 que en este enlace no estaban siendo utilizadas. Como su destino es el Paraninfo, una vez allí son captados por el módulo FCSM para trabajar internamente con ellos. Estas transformaciones pueden verse en la figura 4.37 tras ejecutar el comando *"vvc"* en el nodo de Náutica.

```
$Nautica / >vvc
…
 *   ==> SVC Connections which cannot be modified by the user
 @   ==> Soft PVC Connections
 &   ==> Control Connections
                              CSM Connections
      Incoming                Outgoing
-------------------- --------------------   Connection        Chan  Transport
Slot Port VPI  VCI   Slot Port VPI  VCI     Description       Type  Priority
==== ==== ==== ====  ==== ==== ==== ====  ================= ====== =========
2    1    0    5     2    1    0    1010  Connection 5        VC UNI UBR      &
2    1    0    16    2    1    0    1009  Connection 16       VC UNI UBR      &
2    1    0    18    2    1    0    1008  Connection 18       VC UNI UBR      &
2    1    0    200   3    1    0    33    Connection 200      VC UNI UBR      @
2    1    0    402   3    1    0    32    Connection 402      VC UNI UBR      @
2    1    0    1002  3    2    0    18    Connection 1002     VC UNI UBR      &
2    1    0    1003  3    2    0    16    Connection 1003     VC UNI UBR      &
2    1    0    1004  3    2    0    5     Connection 1004     VC UNI UBR      &
2    1    0    1005  3    1    0    18    Connection 1005     VC UNI UBR      &
2    1    0    1006  3    1    0    16    Connection 1006     VC UNI UBR      &
2    1    0    1007  3    1    0    5     Connection 1007     VC UNI UBR      &
2    1    0    1008  2    1    0    18    Connection 1008     VC UNI UBR      &
2    1    0    1009  2    1    0    16    Connection 1009     VC UNI UBR      &
2    1    0    1010  2    1    0    5     Connection 1010     VC UNI UBR      &
3    1    0    5     2    1    0    1007  Connection 5        VC UNI UBR      &
3    1    0    16    2    1    0    1006  Connection 16       VC UNI UBR      &
3    1    0    18    2    1    0    1005  Connection 18       VC UNI UBR      &
3    1    0    32    2    1    0    402                       VC UNI UBR      *
3    1    0    33    2    1    0    200                       VC UNI UBR      *
3    1    0    34    3    2    0    32                        VC UNI UBR      *
3    1    0    35    3    2    0    33                        VC UNI UBR      *
3    2    0    5     2    1    0    1004  Connection 5        VC UNI UBR      &
3    2    0    16    2    1    0    1003  Connection 16       VC UNI UBR      &
3    2    0    18    2    1    0    1002  Connection 18       VC UNI UBR      &
3    2    0    32    3    1    0    34    Connection 32       VC UNI UBR      *
3    2    0    33    3    1    0    35    Connection 33       VC UNI UBR      *
3    3    0    258   3    3    0    258   Connection 258      VC UNI CBR      @
```

Figura 4.37. Salida del comando "*vvc*" (Náutica)

Así, en la figura 4.37 se aprecia que dos de los circuitos que entran por la interfaz 3/1 se quedan en el nodo siendo conmutados a la interfaz 2/1 y los otros dos salen por la interfaz 3/2 sufriendo un cambio de numeración de la etiqueta. Igualmente en la figura 4.37 aparecen los mismos circuitos para el enlace de vuelta al SdeI (interfaz 3/1), indicando que los circuitos son bidireccionales.

Para explicar de forma más detallada la forma en la que los nodos trabajan con los circuitos (tanto internamente como a través de la red dorsal) es de gran utilidad la figura 4.38, en la que aparece el tránsito de los circuitos entre SdeI y Paraninfo explicado anteriormente. En dicha figura se representan en rojo los circuitos virtuales con los que trabaja internamente el nodo y en negro los circuitos virtuales que aparecen en los enlaces físicos de la red. Como los circuitos son bidireccionales, los mismos circuitos definidos en la figura 4.38, posibilitan la comunicación en ambos sentidos.

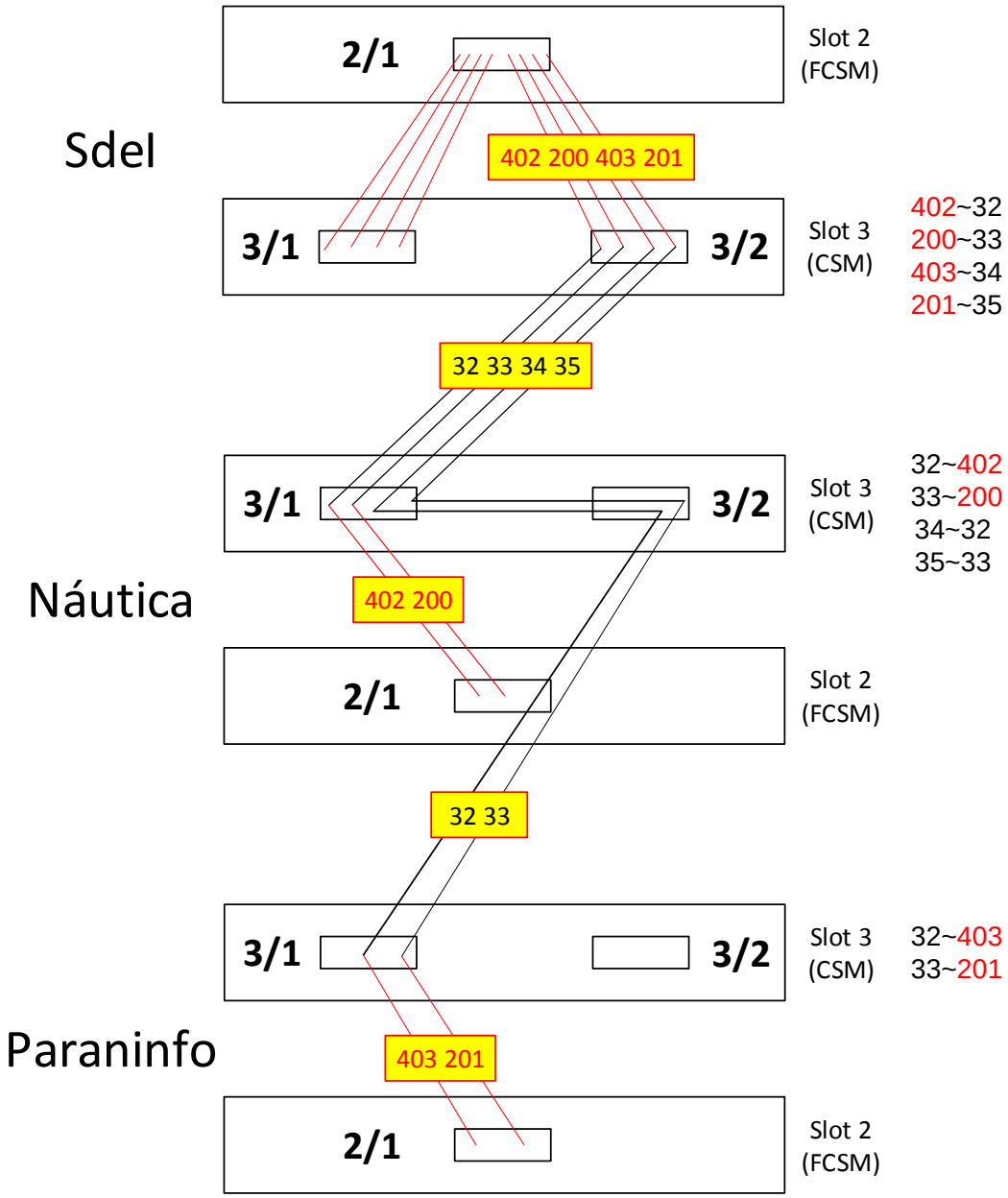


Figura 4.38. Conmutación de circuitos en los nodos

Aparte de los circuitos explicados hasta el momento, por el enlace viajan unos circuitos de control, que son los circuitos 5, 16 y 18 y que están presentes en todos los enlaces bidireccionalmente. El 5, usado para controlar la señalización UNI, el 16 para gestión ILMI~SNMP, y el 18 para controlar el routing PNNI. Además, desde todos los nodos excepto el del SdeI existe un circuito SoftPVC diferente, con una prioridad de transporte CBR (Constant Bit Rate) y que se comunica por la interfaz 3/3, y que se empleaba para enviar el tráfico procedente de las centralitas telefónicas hacia una central Ibercom que centralizaba el tráfico de voz en la UC. (En la figura 4.37 se puede ver la conexión 0/258).

VLANs

Previamente a la realización de cambios, y relacionados con los circuitos de datos que estaban creados, existían una serie de grupos con direcciones IP asignadas para establecer comunicación entre los distintos nodos. Todas las direcciones presentan la forma 192.168.0.X/30, de tal forma que hay una subred por cada enlace lógico de la

estrella. Por cada conexión lógica aparece un grupo que tiene asignada una de estas direcciones y ejerce como punto de acceso a los nodos. Además, existe una conexión adicional fundamental entre el nodo del SdeI y el router del Laboratorio de Telemática que permite dar salida a Internet al laboratorio. Para ilustrar de forma más gráfica esta situación, en la figura 4.39 se muestra la salida del comando *"gp"* en el SdeI con los grupos que ya estaban creados en el nodo, obteniendo la figura 4.40.

```
$SdeI/ >gp
Group                                    Network Address   Proto/
 ID          Group Description          (IP Subnet Mask)   Encaps
(:VLAN ID)                              or (IPX Node Addr)
===== ============================== ================ ========
    1 Default GROUP (#1)
    3 Enlace SI-Nautica                192.168.0.1        IP   /
                                         (ff.ff.ff.fc )    ETH2
    4 Enlace SI-Medicina               192.168.0.5        IP   /
                                         (ff.ff.ff.fc )    ETH2
    6 Enlace SI-Enfermeria             192.168.0.9        IP   /
                                         (ff.ff.ff.fc )    ETH2
    7 Enlace SI-Paraninfo              192.168.0.13       IP   /
                                         (ff.ff.ff.fc )    ETH2
    8 Enlace SI-Router Telematica      192.168.0.21       IP   /
                                         (ff.ff.ff.fc )    ETH2
    9 Enlace SI-Torrelavega            192.168.0.17       IP   /
                                         (ff.ff.ff.fc )    ETH2
```

Figura 4.39. Salida del commando "*gp*" (SdeI)

En la figura 4.39 se muestran las máscaras de subred 255.255.255.252, y las redes que aparecen son: 192.168.0.0/30 (SdeI-Náutica), 192.168.0.4/30 (SdeI-Medicina), 192.168.0.8/30 (SdeI-Enfermería), 192.168.0.12/30 (SdeI-Paraninfo) y 192.168.0.20/30 (SdeI-Router Telemática). Al plasmar este direccionamiento gráficamente da como resultado la figura 4.40.

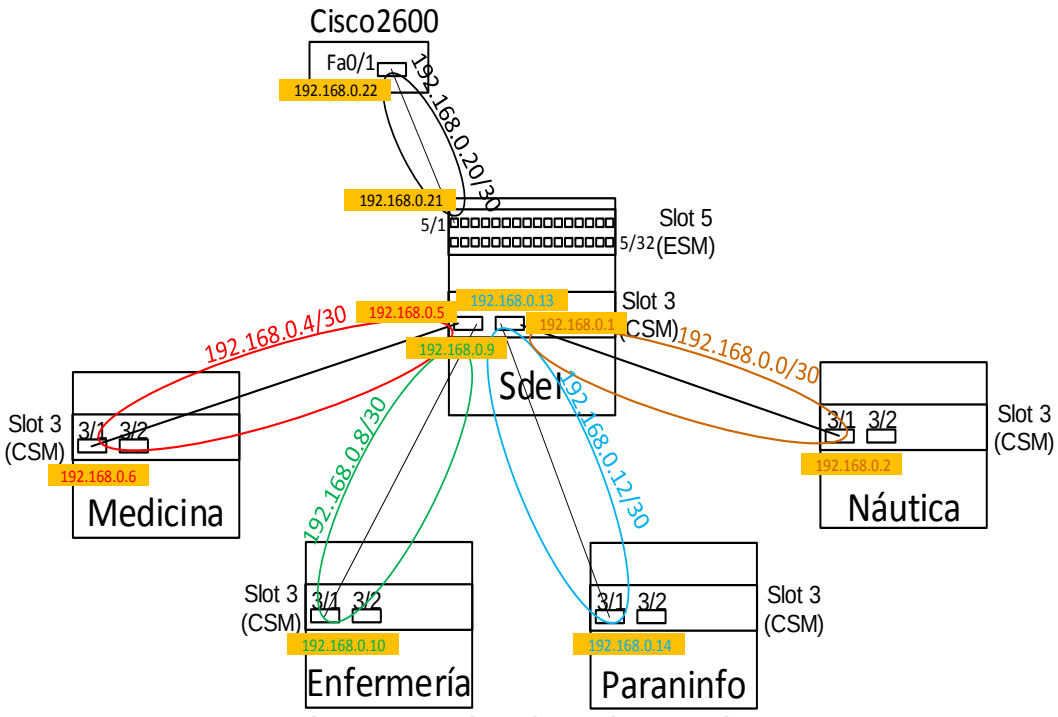


Figura 4.40. Direccionamiento nodos

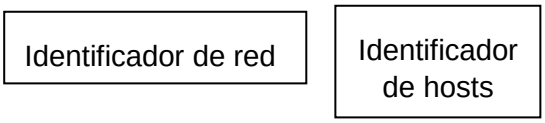
Tal como se muestra en la figura 4.40, la interfaz 5/1 del SdeI tiene asignada la dirección 192.168.0.21/30 y se une directamente a la interfaz FastEthernet0/1 del Router Cisco2600 con dirección 192.168.0.22/30, lo que conecta ambos laboratorios y

permite que el Laboratorio de Aplicaciones Telemáticas tenga salida a Internet a través del Servidor Atlas (ver figura 1.3 del Capítulo 1).

En cuanto a la creación de VLANs para la parte de acceso a usuario, se decidió separar el acceso de usuarios en 3 colectivos bien diferenciados, el primero para profesorado, el segundo para administración y por último una VLAN destinada para el acceso de los alumnos. Las redes asignadas para la creación de estos perfiles son la 192.168.1.0/24, la 192.168.2.0/24 y la 192.168.3.0/24 que se integran en el direccionamiento del Laboratorio de Telemática a través de la conexión entre el Router Cisco2600 y la interfaz 5/1 del SdeI comentada anteriormente.

En cada nodo se van a crear 3 VLANs para separar los accesos de los colectivos descritos anteriormente. De esta forma, cada grupo estaría aislado en la red en su VLAN según el colectivo al que pertenezca de cada facultad. Para ello, es necesario dividir las redes 192.168.1.0/24, la 192.168.2.0/24 y la 192.168.3.0/24 en otras de menor tamaño, es decir, es necesario hacer subnetting.

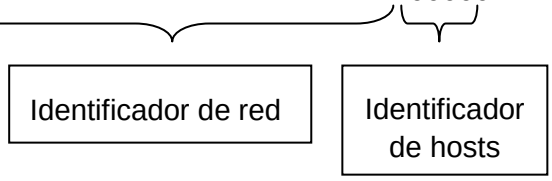
Teniendo en cuenta que se está trabajando con redes de Clase C, 192.168.X.0 con máscara 255.255.255.0 (/24) → 11111111.11111111.11111111.00000000



Tan solo puede existir una red con 254 equipos posibles.

Para dividir la red en otras más pequeñas, se toman prestados bits correspondientes a identificación de hosts de la dirección IP. Dado que hay que dividir las redes originales en, al menos, 5 subredes de menor tamaño, la red más grande que se puede definir es una red con máscara /27, ya que tomando 3 bits, que previamente identificaban hosts en la red original, se divide esta red en 8 de menor tamaño $(2^3 = 8)$. Es fácilmente comprobable que si se cogen únicamente 2 bits, solo se pueden formar 4 subredes, lo que sería insuficiente, y cogiendo los 3 bits sugeridos ya se tiene la holgura suficiente para diseñar las nuevas subredes.

Por tanto, las redes resultantes son de la forma 192.168.X.Y con máscara 255.255.255.224 (/27) → 11111111.11111111.11111111.**111**00000



Pudiendo existir hasta 8 subredes con un máximo de 30 equipos en cada una.

Al necesitar 5 subredes, quedarán 3 restantes sin usar, pudiendo ser utilizadas para otros propósitos si fuera necesario. Las subredes se van a asignar de manera consecutiva, y el orden a seguir será:

SdeI – Náutica – Paraninfo – Medicina – Enfermería.

Para obtener las direcciones entre las que estará situada cada subred, se comienza dando valores a los números que aparecen remarcados en negrita en la máscara de la parte superior:

Subred SdeI: 192.168.X.**000**00000(/27)→ 192.168.X.0 (Bcast: 192.168.X.31)

Subred Náutica: 192.168.X.**001**00000(/27)→ 192.168.X.32 (Bcast: 192.168.X.63)

Subred Paraninfo: 192.168.X.**010**00000(/27)→ 192.168.X.64 (Bcast: 192.168.X.95)

Subred Medicina: 192.168.X.**011**00000(/27)→ 192.168.X.96 (Bcast: 192.168.X.127)

Subred Enfermería: 192.168.X.**100**00000(/27)→ 192.168.X.128 (Bcast: 192.168.X.159)

Subred Libre 1: 192.168.X.**101**00000(/27)→ 192.168.X.160 (Bcast: 192.168.X.191)

Subred Libre 2: 192.168.X.**110**00000(/27)→ 192.168.X.192 (Bcast: 192.168.X.223)

Subred Libre 3: 192.168.X.**111**00000(/27)→ 192.168.X.224 (Bcast: 192.168.X.255)

Dependiendo del colectivo de usuarios, la "X" tomará los valores de 1 para profesorado, 2 para administración y 3 para alumnos, estableciendo un máximo de 30 equipos en cada subred ya que $2^5 = 32$ y descontando la dirección de subred y la dirección de broadcast, quedan un máximo de 30 direcciones asignables. La primera dirección libre será establecida en todas las VLANs como puerta de enlace predeterminada, creando de esta forma un router virtual que la permita comunicarse por la red.

En este momento ya se ha diseñado todo el sistema, quedando únicamente pendiente por decidir qué número de grupo corresponderá a las VLANs y cómo van a quedar asignados los puertos pertenecientes en cada nodo. Con la intención de facilitar el estudio y el manejo de los equipos, los grupos y los puertos asignados a cada VLAN serán los mismos en todos los nodos. Para crear las VLANs, los grupos serán el 10, el 11 y el 12, dado que en el SdeI son los primeros consecutivos que están libres (ver figura 4.39). En lo referente a los puertos, en principio, todos los existentes en el módulo ESM están libres, o lo que es lo mismo, corresponden al grupo por defecto, pero en el SdeI, es importante recordar que la interfaz 5/1 debe pertenecer al grupo 8 (conexión con Laboratorio de Telemática) para dar salida a Internet. Además, como se explicó en el apartado 4.2.2, la interfaz 5/29 permanece conectada al Servidor DHCP y la 5/32 enlaza el nodo con el Switch situado en el Patch Panel. Por esto, y debido a que se convino que con 4 puertos para cada VLAN sería suficiente, en todos los nodos, las VLANs se configurarán en el módulo ESM de la siguiente manera:

- VLAN P (10): Pertenecerán a esta VLAN los puertos 3, 4, 5 y 6.
- VLAN A (11): Pertenecerán a esta VLAN los puertos 7, 8, 9 y 10.
- VLAN Alumnos (12): Pertenecerán a esta VLAN los puertos 11, 12, 13 y 14.

Existen varias formas para crear VLANs, pero la mejor es emplear los comandos [2]: *"crgp"* utilizado para la creación de un grupo (que lleva implícita una VLAN por defecto), *"gmstat"* para habilitar a posteriori la movilidad del grupo, no imprescindible, pero aporta mayor flexibilidad a la red al soportar asignación dinámica de puertos y "*modvl*" para editar las propiedades de la VLAN creada previamente. En las figura 4.41

y 4.42 se puede ver la creación de la VLAN para alumnos en el nodo del Paraninfo. Primero, en la figura 4.41 se crea la VLAN (grupo 12) y se le asignan los puertos reservados para el colectivo de alumnos (11, 12, 13 y 14) y después en la figura 4.42 se habilita la movilidad del grupo y el direccionamiento IP asignando a la VLAN la puerta de enlace 192.168.3.65/27 puesto que el Paraninfo tiene asignada la subred 192.168.X.64/27 y a la VLAN de alumnos le corresponde la 192.168.3.64/27.

```
$Paraninfo / >crgp
    GROUP Number (  4) : 12
    Description (no quotes) : VLAN ALUMNOS
    Enable WAN Routing? (n):
    Enable ATM CIP? (n):
    Enable IP (y) : n
    Enable IPX? (y): n
    Enter a priority level (0...7)(0):
Enable Group Mobility on this Group ? [y/n](n):
This Group will not participate in Group Mobility
Do you wish to configure the interface group for this Virtual LAN at this
time? (y)
Initial Vports(Slot/Phys Intf. Range) - For example, first I/O Module
(slot 2), second Interface would be 2/2. Specify a range of interfaces
and/or a list as in:   2/1-3, 3/3, 3/5, 4/6-8.

    Initial Slot/Interface Assignments: 6/11-14
 6/14-This interface is currently assigned to GROUP 1-(Default GROUP (#1)).
 Do you wish to remove it from that GROUP and assign it (with
 new configuration values) to this GROUP [y|n|c to Accept defaults] (n)? y
......
 6/11-This interface is currently assigned to GROUP 1-(Default GROUP (#1)).
 Do you wish to remove it from that GROUP and assign it (with
 new configuration values) to this GROUP [y|n|c to Accept defaults] (n)? y
                  Modify ESM 100C 32 Vport 6/14 Configuration
 1) Vport/Group/Instance/Type   : 94/12/1/Brg
 2) Description                 :
 3) Bridge Mode                 : Auto-Switched
   31) Switch Timer                : 60
 4) Flood Limit                 : 192000
 5) Output Format Type          : Default(IP-Eth II, IPX-802.3)
 6) Ethernet 802.2 Pass Through : Yes
 7) Admin, Operational Status   : Enabled, inactive
 8) Mirrored Port Status        : Disabled, available
 9) MAC address                 : 000000:000000
Command {Item=Value/?/Help/Quit/Redraw/Save} (Redraw)  : q
......
                  Modify ESM 100C 32 Vport 6/11 Configuration
 1) Vport/Group/Instance/Type   : 91/12/1/Brg
 2) Description                 :
 3) Bridge Mode                 : Auto-Switched
   31) Switch Timer                : 60
 4) Flood Limit                 : 192000
 5) Output Format Type          : Default(IP-Eth II, IPX-802.3)
 6) Ethernet 802.2 Pass Through : Yes
 7) Admin, Operational Status   : Enabled, inactive
 8) Mirrored Port Status        : Disabled, available
 9) MAC address                 : 000000:000000
Command {Item=Value/?/Help/Quit/Redraw/Save} (Redraw)  : q
    Adding port 6/14 to GROUP 12...
    Adding port 6/13 to GROUP 12...
    Adding port 6/12 to GROUP 12...
    Adding port 6/11 to GROUP 12...
You may modify interfaces to this group using the addvp, modvp and rmvp
commands at a later date if you choose.
```

Figura 4.41. Creación VLAN Alumnos Paraninfo (Parte 1)

```
$Paraninfo / >gmstat 12
Group Mobility is OFF for Group 12
Change Group Mobility Status for Group 12 to ON ? [y/n] (y):
Configure rules for this group ? [y/n](y): n
Configure Auto-Activated LANE service ? [y/n](y): n
$Paraninfo / >modvl 12:1
 Current values associated with GROUP 12.1 are as follows:
  1) GROUP Number          - 12:1
  2) Description           - VLAN ALUMNOS
IP parameters:
  3) IP enabled            - N
IPX parameters:
  4) IPX enabled           - N

(save/quit/cancel)
   : 3=Y
Enter IP router information:

  1) GROUP Number          - 12:1
  2) Description           - VLAN ALUMNOS
IP parameters:
  3) IP enabled            - Y
  4) IP Network Address    - 0.0.0.0
  5) IP Subnet Mask        - 0.0.0.0
  6) IP Broadcast Address  - 0.0.0.0
  7) Router Description    -
  8) RIP Mode              - Silent
       {Active(a), Inactive(i), Deaf(d), Silent(s)}
  9) Routing disabled      - N
 10) NHRP enabled          - N
 11) Default Framing       - Ethernet II
       {Ethernet II(e), Ethernet 802.3(8), fddi(f),
        token ring(t), source route token ring(s)}
IPX parameters:
 12) IPX enabled           - N

   : 4=192.168.3.65
  New IP address generates new subnet and broadcast addresses.
  Enter '?' to view the changes.
   : 5=255.255.255.224
  New mask caused change in broadcast address.
   : save
```

Figura 4.42. Creación VLAN Alumnos Paraninfo (Parte 2)

Recordando ahora lo que se comentó en el momento en que se crearon los servicios de Trunking ATM, para hacer que las VLANs viajen por los circuitos virtuales es necesario asociar las VLANs creadas a dichos servicios. Para ello, se ejecuta la orden "*mas 2/1 nºservicio*", comando que se utiliza para modificar un servicio creado con anterioridad, tal y como se observa en la figura 4.43 en el equipo del Paraninfo en donde se añaden los grupos 10, 11 y 12 al servicio 2 de ATM (Trunking), servicio que corresponde a la conexión virtual 0/403.

```
$Paraninfo / >vas
                          ATM Services

          Serv            Service              Service
Slot Port Num           Description             Type
==== ==== ==== ============================== =========
2    1    1    PTOP Bridging Service 1        PTOP 1483
2    1    2    Trunking Service 2             Trunking
                          ATM Services
          Serv VC    Oper
Slot Port Num  Typ   Status   SEL Groups       Conn VPI/VCI (Addrs Index)
==== ==== ==== === ======== === ==========  ==========================
2    1    1    PVC Enabled  N/A 3            0/201
2    1    2    PVC Enabled  N/A 1            0/403
$Paraninfo / >mas 2/1 2
   Slot 2 Port 1 Service 2 Configuration
1)  Description (30 chars max)        : Trunking Service 2
2)  Trunked Groups                    : 1
3)  Connection                        : 403
4)  Admin Status { disable(1),
                   enable(2) }        : Enable
```

```
6)  Connection Type { PVC(1),
                      SVC(2) }          : PVC
Enter (option=value/save/cancel) : 2=10
   Slot 2 Port 1 Service 2 Configuration
1)  Description (30 chars max)          : Trunking Service 2
2)  Trunked Groups                      : 1 10
3)  Connection                          : 403
4)  Admin Status { disable(1),
                   enable(2) }          : Enable
6)  Connection Type { PVC(1),
                      SVC(2) }          : PVC
Enter (option=value/save/cancel) : 2=11
   Slot 2 Port 1 Service 2 Configuration
1)  Description (30 chars max)          : Trunking Service 2
2)  Trunked Groups                      : 1 10 11
3)  Connection                          : 403
4)  Admin Status { disable(1),
                   enable(2) }          : Enable
6)  Connection Type { PVC(1),
                      SVC(2) }          : PVC
Enter (option=value/save/cancel) : 2=12
   Slot 2 Port 1 Service 2 Configuration
1)  Description (30 chars max)          : Trunking Service 2
2)  Trunked Groups                      : 1 10 11 12
3)  Connection                          : 403
4)  Admin Status { disable(1),
                   enable(2) }          : Enable
6)  Connection Type { PVC(1),
                      SVC(2) }          : PVC
Enter (option=value/save/cancel) : save
Modifying service, please wait...
Enabling service...
```

Figura 4.43. Asociación de VLANs con servicio de Trunking (Paraninfo)

Tras este paso, el proceso de configuración principal ya ha finalizado, habiendo creado todas las VLANs asociadas a un servicio de Trunking ATM y con toda la red completamente operativa, de manera que todos los nodos pueden comunicarse entre ellos y a su vez tienen conexión a la red Internet pública. En la figura 4.44 se muestra el direccionamiento final de la red que se ha ido explicando a lo largo de este capítulo.

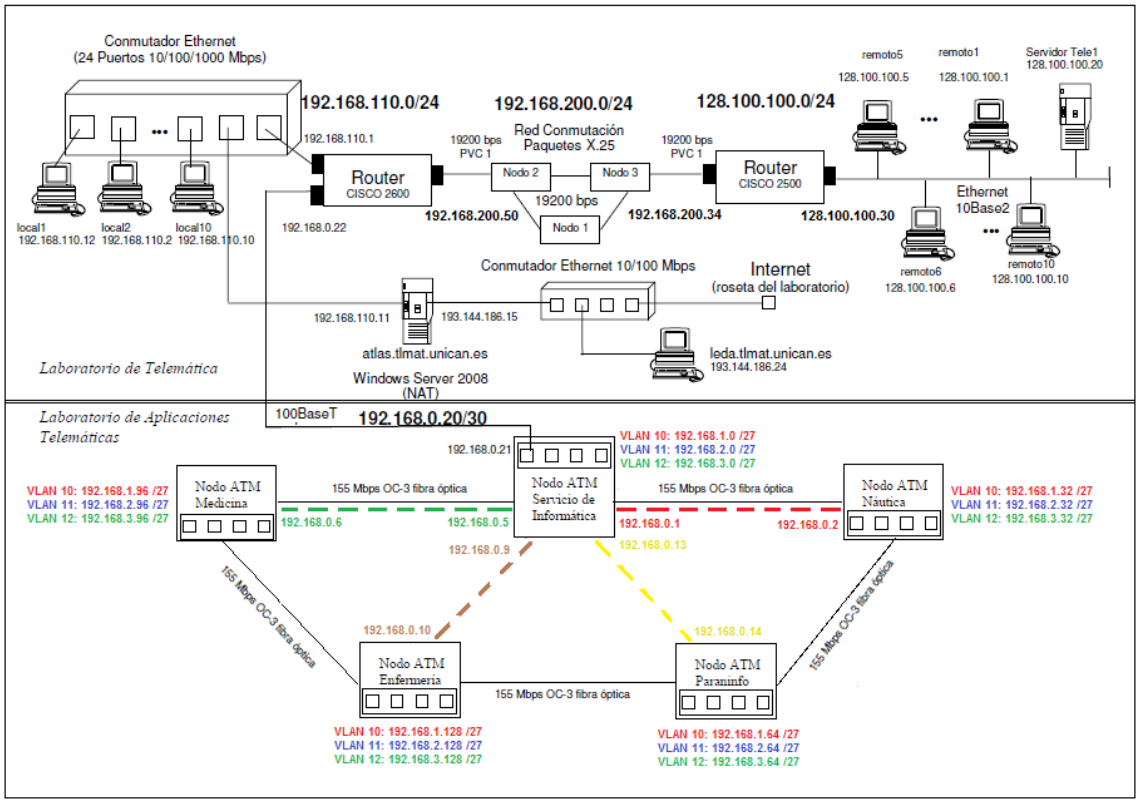


Figura 4.44. Red telemática final

Si ahora se quiere conectar un PC a una VLAN determinada, al no estar configurado un DHCP para cada VLAN, es necesario configurar los parámetros de red manualmente para cada PC. Por ejemplo, para conectar un ordenador a la VLAN 11 (A) de Medicina, se debe conectar el interfaz Ethernet del PC al nodo de Medicina (a través del patch panel y las tomas de los nodos) en uno de los puertos asignados a esta VLAN (7, 8, 9 o 10) y posteriormente configurar el protocolo de Internet versión 4 (TCP/IP v4) de la siguiente forma:

Dirección IP. . . . . : 192.168.2.(98-126)

Máscara de subred . . . . . : 255.255.255.224

Puerta de enlace predeterminada : 192.168.2.97

Servidor DNS. . . . . : 192.168.110.11

DHCP

Para los PC del Laboratorio de Aplicaciones Telemáticas se plantea configurar un Servidor DHCP que aporte direcciones automáticamente al iniciar un ordenador. Este Servidor se instala en un equipo del laboratorio (Júpiter) y permanece conectado a la interfaz 5/29 del nodo SdeI tal y como se ha descrito en el apartado 4.2.2. Si no se realizan modificaciones en el conexionado del laboratorio, inicialmente todos los equipos permanecen conectados al Switch situado en el armario de conexiones. Este Switch se enlaza con el nodo SdeI mediante una conexión entre su puerto 1 y la interfaz 5/32 del nodo. Para que el Servidor funcione correctamente y asigne direcciones a los equipos conectados al Switch, tiene que configurarse en el nodo SdeI un nuevo grupo que incluya las interfaces 5/29 y 5/32. A instancias de mantener la misma configuración en las redes dispuestas para las VLANs, se decidió establecer una nueva red exclusiva para que los equipos reciban una dirección válida del DHCP, la red 192.168.4.0 /24.

Como primer paso, se tiene que comprobar que esta red se encuentra incluida en el Router Cisco2600 y el Servidor Atlas que son los equipos que dan acceso a Internet a la Intranet del Laboratorio de Aplicaciones Telemáticas. Se comprueba que Atlas tiene incluida la siguiente entrada:

Network Destination	Netmask	Gateway
192.168.0.0	255.255.0.0	192.168.110.11

Por lo que la red 192.168.4.0 /24 está incluida dentro en la tabla de rutas.

Por el contrario, como se comprobó a la hora de estudiar la configuración previa (figura 4.21), el Router Cisco2600 no tiene incluida una ruta que direccione la red 192.168.4.0/24 con el exterior, por tanto, es necesario incluirla tal y como aparece en la figura 4.45. Para ello se utiliza el comando *"ip route Network Netmask Gateway"* y posteriormente se ejecuta la orden *"write"* para sobrescribir el archivo de memoria y evitar que la nueva ruta se pierda al apagar el router.

```
alumnos@labpc8:~$ telnet 192.168.0.22
Trying 192.168.0.22...
Connected to 192.168.0.22.
Escape character is '^]'.
User Access Verification
Password:
Password: (git)
c2600>enable
Password:
Password: (telematica)
c2600# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
c2600(config)#ip route 192.168.4.0 255.255.255.0 192.168.0.21
c2600#write
Building configuration...
[OK]
c2600(config)#exit
```

Figura 4.45. Ruta añadida al Router Cisco2600

Para comprobar que la ruta se ha añadido correctamente se ejecuta *"show ip route"* al igual que se hizo en la figura 4.21 y se observa que ahora sí que aparece una ruta que direccione la red 192.168.4.0/24 (ver figura 4.46).

```
c2600>show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
I - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
Gateway of last resort is 192.168.110.11 to network 0.0.0.0
C 192.168.110.0/24 is directly connected, FastEthernet0/0
S 192.168.10.0/24 [1/0] via 192.168.0.21
S 192.168.11.0/24 [1/0] via 192.168.0.21
C 192.168.200.0/24 is directly connected, Serial0/0
128.100.0.0/24 is subnetted, 1 subnets
S 128.100.100.0 [1/0] via 192.168.200.34
S 192.168.4.0/24 [1/0] via 192.168.0.21
192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
S 192.168.0.0/24 [1/0] via 192.168.0.21
C 192.168.0.20/30 is directly connected, FastEthernet0/1
S 192.168.1.0/24 [1/0] via 192.168.0.21
S 192.168.2.0/24 [1/0] via 192.168.0.21
S 192.168.3.0/24 [1/0] via 192.168.0.21
S* 0.0.0.0/0 [1/0] via 192.168.110.11
```

Figura 4.46. Comprobación tabla de rutas router Cisco2600

Posteriormente, se creó una VLAN en el nodo SdeI (grupo 22, de la misma forma que las VLANs creadas anteriormente)) y se le asignaron los puertos 29, 30, 31 y 32 tal y como se puede ver en la figura 4.47.

```
$SdeI/ >vi 22
               Virtual Interface Summary Information- For GROUP 22
                                                        Status
      Slot/ Type/                                    --------------------
Group Intf   Inst/Srvc   MAC Address  Prt Encp Admin   Oper  Spn Tr  Mode
===== ==== ============ ============= === ==== ====== ====== ====== =======
   22 All  Rtr/  1       00d095:4e469d IP  ETH2 Enabld Active   N/A    N/A
   22 5/29 Brg/  1/ na   00d095:2acd7f Tns DFLT Enabld Active Disabl AutoSw
   22 5/30 Brg/  1/ na   02d095:2acd7d Tns DFLT Enabld Active Disabl AutoSw
   22 5/31 Brg/  1/ na   02d095:2acd7e Tns DFLT Enabld Inactv Disabl AutoSw
   22 5/32 Brg/  1/ na   02d095:2acd7f Tns DFLT Enabld Active Disabl AutoSw
```

Figura 4.47. Grupo 22 (Internet Switch)

En este momento, y al igual que se hizo a la hora de crear las otras VLANs, se modifican las propiedades de la VLAN para añadir el direccionamiento IP tal y como se muestra en la figura 4.48.

En la figura 4.49 se comprueba mediante el comando *"gp"* el estado de los grupos creados en el SdeI para confirmar que existen tanto las VLANs destinadas a los

diferentes colectivos universitarios (P, A y Alumnos) como la VLAN dedicada para el Servidor DHCP.

```
$SdeI/ >modvl 22:1
 Current values associated with GROUP 22.1 are as follows:
  1) GROUP Number          - 22:1
  2) Description           - INTERNET SWITCH
IP parameters:
  3) IP enabled            - N
IPX parameters:
  4) IPX enabled           - N
(save/quit/cancel)
   : 3=Y
Enter IP router information:
  1) GROUP Number          - 22:1
  2) Description           - INTERNET SWITCH
IP parameters:
  3) IP enabled            - Y
  4) IP Network Address    - 0.0.0.0
  5) IP Subnet Mask        - 0.0.0.0
  6) IP Broadcast Address  - 0.0.0.0
  7) Router Description    -
  8) RIP Mode              - Silent
       {Active(a), Inactive(i), Deaf(d), Silent(s)}
  9) Routing disabled      - N
 11) Default Framing       - Ethernet II
       {Ethernet II(e), Ethernet 802.3 SNAP(8), fddi(f),
        token ring(t), source route token ring(s)}
IPX parameters:
 12) IPX enabled           - N
   : 4=192.168.4.1
  New IP address generates new subnet and broadcast addresses.
  Enter '?' to view the changes.
   : 5=255.255.255.0
  New mask caused change in broadcast address.
   : save
```

Figura 4.48. Direccionamiento VLAN Internet Switch

```
$SdeI/ >gp
Group                                  Network Address  Proto/
 ID          Group Description        (IP Subnet Mask)  Encaps
(:VLAN ID)                            or (IPX Node Addr)
===== ============================== ================ ========
    1 Default GROUP (#1)
    3 Enlace SI-Nautica               192.168.0.1        IP  /
                                        (ff.ff.ff.fc )    ETH2
……
   10 VLAN P                          192.168.1.1        IP  /
                                        (ff.ff.ff.e0 )    ETH2
   11 VLAN A                          192.168.2.1        IP  /
                                        (ff.ff.ff.e0 )    ETH2
   12 VLAN ALUMNOS                    192.168.3.1        IP  /
                                        (ff.ff.ff.e0 )    ETH2
   22 INTERNET SWITCH                 192.168.4.1        IP  /
                                        (ff.ff.ff.00 )    ETH2
```

Figura 4.49. Comprobación grupos SdeI

En la figura 4.50 se comprueba mediante el comando *"ipr"* que la tabla de rutas del nodo incluye un gateway erróneo para la red 192.168.4.0/24 y se elimina dicha ruta errónea ejecutando el comando "*risr*" para provocar que la tabla de rutas se actualice a la nueva configuración.

```
$SdeI/ >ipr
23 routes in forwarding table
                                IP FORWARDING TABLE
                                -------------------
+ = Equal Cost Multipath routes
                                                                  Group:VLAN
  Network          Mask            Gateway          Metric      Id      Protocol
  ------------------------------------------------------------------------------
-
  0.0.0.0          0.0.0.0         192.168.0.22        1        8:1      STATIC
  192.168.0.0    255.255.255.252   192.168.0.1         1        3:1      DIRECT
  192.168.0.4    255.255.255.252   192.168.0.5         1        4:1      DIRECT
  192.168.0.8    255.255.255.252   192.168.0.9         1        6:1      DIRECT
  192.168.0.12   255.255.255.252   192.168.0.13        1        7:1      DIRECT
  192.168.0.16   255.255.255.252   192.168.0.17        1        9:1      DIRECT
  192.168.0.20   255.255.255.252   192.168.0.21        1        8:1      DIRECT
  192.168.1.0    255.255.255.224   192.168.1.1         1       10:1      DIRECT
  192.168.1.32   255.255.255.224   192.168.0.2         1        3:1      STATIC
  192.168.1.64   255.255.255.224   192.168.0.14        1        7:1      STATIC
  192.168.1.96   255.255.255.224   192.168.0.6         1        4:1      STATIC
  192.168.1.128  255.255.255.224   192.168.0.10        1        6:1      STATIC
  192.168.2.0    255.255.255.224   192.168.2.1         1       11:1      DIRECT
  192.168.2.32   255.255.255.224   192.168.0.2         1        3:1      STATIC
  192.168.2.64   255.255.255.224   192.168.0.14        1        7:1      STATIC
  192.168.2.96   255.255.255.224   192.168.0.6         1        4:1      STATIC
  192.168.2.128  255.255.255.224   192.168.0.10        1        6:1      STATIC
  192.168.3.0    255.255.255.224   192.168.3.1         1       12:1      DIRECT
  192.168.3.32   255.255.255.224   192.168.0.2         1        3:1      STATIC
  192.168.3.64   255.255.255.224   192.168.0.14        1        7:1      STATIC
  192.168.3.96   255.255.255.224   192.168.0.6         1        4:1      STATIC
  192.168.3.128  255.255.255.224   192.168.0.10        1        6:1      STATIC
  192.168.4.0    255.255.255.0     192.168.0.18        1        9:1      STATIC

$SdeI/ >risr
Do you want to see the current route table? (y or n) (y) : n
Destination IP address of host or network : 192.168.4.0
Host or network mask (255.255.255.0)     : 255.255.255.0
IP address of next hop                   : 192.168.0.18
Route successfully deleted
```

Figura 4.50. Eliminar entrada en tabla de rutas nodo SdeI

Después de esto, mediante la figura 4.51 se comprueba que la ruta se ha actualizado ejecutando de nuevo el comando *"ipr"* y a su vez, se comprueba también que el gateway 192.168.4.1 presenta conectividad tras ejecutar un *"ping"* a esa dirección.

```
$SdeI/ >ipr
23 routes in forwarding table
                                IP FORWARDING TABLE
                                -------------------
+ = Equal Cost Multipath routes
                                                                  Group:VLAN
  Network            Mask                  Gateway              Metric       Id
Protocol
  ------------------------------------------------------------------------------
-
  0.0.0.0          0.0.0.0         192.168.0.22        1        8:1      STATIC
  192.168.0.0    255.255.255.252   192.168.0.1         1        3:1      DIRECT
  192.168.0.4    255.255.255.252   192.168.0.5         1        4:1      DIRECT
……
  192.168.3.128  255.255.255.224   192.168.0.10        1        6:1      STATIC
  192.168.4.0    255.255.255.0     192.168.4.1         1       22:1      DIRECT

 $SdeI/ >ping
     Host () : 192.168.4.1
     Count (0 for infinite) (1) :
     Size (64) :
     Timeout (1) :
Ping starting, hit <RETURN> to stop
PING 192.168.4.1: 64 data bytes
   [0          ] .
----192.168.4.1 PING Statistics----
1 packets transmitted, 1 packets received, 0% packet loss
Round-trip (ms)  min/avg/max = 0/0/0
```

Figura 4.51. Comprobación tabla de rutas y conectividad gateway DHCP

Para finalizar, es necesario modificar la configuración del propio Servidor DHCP. El programa que se utiliza es Open DHCP Server y únicamente se tiene que cambiar un fichero de texto en el que aparecen multitud de opciones configurables comentadas, pero en el que solo es necesario establecer las opciones que aparecen sin ";" tal y como se muestra en la figura 4.52.

```
[RANGE_SET]
…
;DHCPRange=192.168.0.1-192.168.0.254
DHCPRange=192.168.4.3-192.168.4.254
#Following are range specific DHCP options.
#You can copy more options names from [GLOBAL_OPTIONS]
SubnetMask=255.255.255.0
DomainServer=192.168.110.11
Router=192.168.4.1
```

Figura 4.52. Fichero de Open DHCP Server

Así, los nuevos valores configurados son; La dirección IP del gateway de la subred o puerta de enlace (192.168.4.1), la máscara de red (255.255.255.0), el Servidor DNS (192.168.110.11) y el rango en el que asignará direcciones el DHCP (192.168.4.3 – 192.168.4.254) puesto que la 192.168.4.1 es la puerta de enlace y la dirección 192.168.4.2 se configuró de manera estática para el propio PC que ejerce como Servidor DHCP.

Servicio Ethernet 802.1Q

Para poder monitorizar mediante Wireshark tráfico Ethernet con las etiquetas VLAN, se va a crear también en cada nodo, un grupo Alcatel que solamente tenga asignado un puerto Ethernet y que esté asociado a un servicio Ethernet 802.1Q por cada VLAN a difundir. Para no complicar el análisis posterior, se hará coincidir la etiqueta que se le dará al servicio con el número de grupo de la VLAN, de modo que en Wireshark cuando se vea una etiqueta con valor 10 se sabrá que se corresponde a un paquete enviado desde la VLAN P. El número de grupo seleccionado es el 99 "802.1Q" y se le asignará el puerto 15 en cada nodo. Para crear este servicio 802.1Q, a diferencia del resto de servicios ATM en los que se utilizaba la interfaz lógica 2/1, se utiliza el puerto físico Ethernet deseado, quedando el comando a utilizar *"cas slot/port"*. En la figura 4.53 se crea el servicio en el nodo de Náutica para la VLAN 10.

```
$Nautica / >cas 4/15
   Slot 4 Port 15 Ethernet 802.1Q Service
  1)  Description (30 chars max)           :
  2)  Group ID                             : 0
  3)  Tag                                  : 0
  4)  Priority                             : 0
  5)  Mode                                 : 0
        Multiple Spanning tree (3)
        Single Spanning tree   (4)
   : 1=Vlan 10
   : 2=10
   : 5=3
   Slot 4 Port 15 Ethernet 802.1Q Service
  1)  Description (30 chars max)           : Vlan 10
  2)  Group ID                             : 10
  3)  Tag                                  : 10
  4)  Priority                             : 0
  5)  Mode                                 : 3
   : save
     Created 802.1Q service for Group 10 on 4/15 (slot/port)
```

Figura 4.53. Creación servicio 802.1Q (Náutica)

Como se puede ver en la figura 4.53, a la hora de crear el Servicio 802.1Q se especifica que utilice una configuración de Spanning Tree múltiple (MSTP) debido a

que el protocolo MSTP configura un árbol de expansión independiente para cada grupo de VLAN y bloquea todos menos uno de los posibles caminos alternativos dentro de cada árbol de expansión, tratando a cada VLAN de forma independiente. Para que las VLANs se difundan correctamente, es importante que los servicios 802.1Q se creen en el mismo orden en ambos extremos [2].

Tras la creación del Servicio Ethernet 802.1Q, las configuraciones relacionadas con las VLANs y los servicios ATM han finalizado. En la figura 4.54 se muestra el estado final de los grupos y los servicios ATM del nodo de Náutica y en la figura 4.55 se representa el estado en el que han quedado asignados los puertos correspondientes al módulo ESM en los nodos.

```
$Nautica / >gp
Group                                  Network Address  Proto/
 ID          Group Description        (IP Subnet Mask)  Encaps
(:VLAN ID)                            or (IPX Node Addr)
===== ============================== =============== ========
    1 Default GROUP (#1)
    2 Enlace Marina-SdI              192.168.0.2       IP  /
                                       (ff.ff.ff.fc )   ETH2
   10 VLAN P                         192.168.1.33      IP  /
                                       (ff.ff.ff.e0 )   ETH2
   11 VLAN A                         192.168.2.33      IP  /
                                       (ff.ff.ff.e0 )   ETH2
   12 VLAN ALUMNOS                   192.168.3.33      IP  /
                                       (ff.ff.ff.e0 )   ETH2
   99 802.1Q

$Nautica / >vas
                          ATM Services
          Serv            Service             Service
Slot Port Num           Description            Type
==== ==== ==== ============================== =========
2    1    2    Enlace Datos SdI              PTOP 1483
2    1    1    Trunking Service 1            Trunking
                          ATM Services
          Serv VC    Oper
Slot Port Num  Typ  Status  SEL Groups      Conn VPI/VCI (Addrs Index)
==== ==== ==== === ======== === ==========  ==========================
2    1    2    PVC Enabled  N/A 2           0/200
2    1    1    PVC Enabled  N/A 1     10    0/402
                                 11    12
FDDI Services do not exist!
Gigabit Ethernet 802.1Q Services do not exist.
                              Ethernet Services
Slot Port Inst Vport Group  Tag  Pri Tagging Mode  Description
==== ==== ==== ===== =====  ==== === ============  =============
  4   15    1    37    10     10  0  Mult STree    Vlan 10
  4   15    2    38    11     11  0  Mult STree    Vlan 11
  4   15    3    40    12     12  0  Mult STree    Vlan 12
```

Figura 4.54. Configuración final Náutica

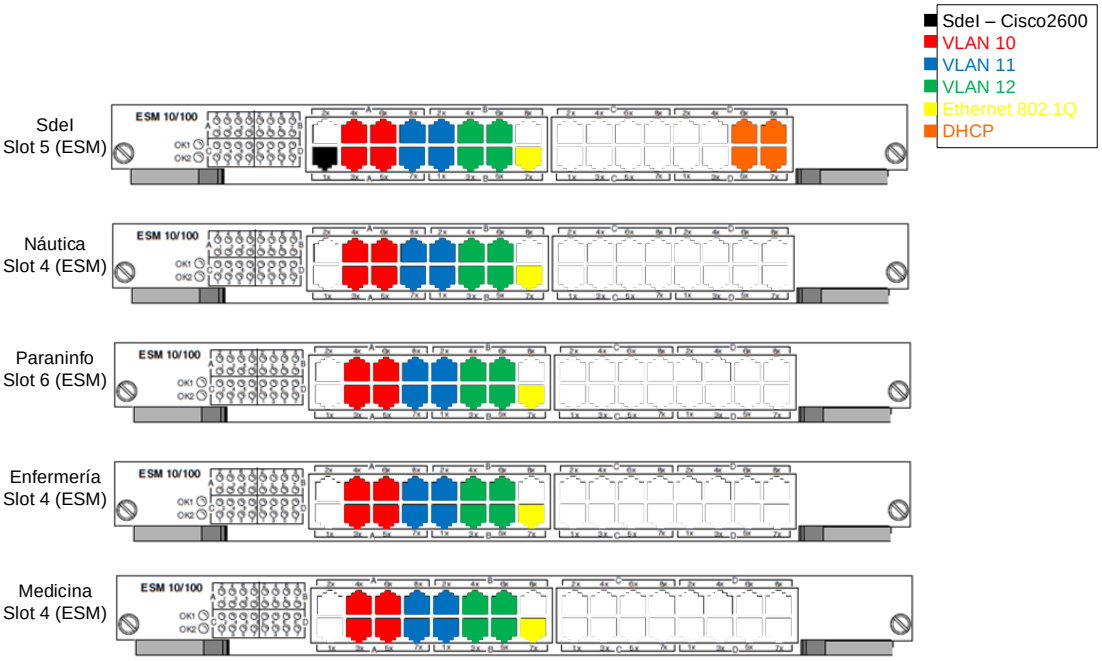


Figura 4.55. Asignación puertos módulo ESM

SNMP

Como se comentó en el apartado 4.3.1, la generación de traps SNMP por parte de los nodos ya estaba configurada de antemano, y como posteriormente se va a hacer uso de esta configuración, es necesario hacer algunas modificaciones y aclaraciones al respecto.

Los nodos permiten la activación de traps SNMP de forma multicast o unicast. En este caso, interesa que la generación sea unicast y que se envíen a un PC del laboratorio que realiza el papel de Gestor de Red (el PC tiene instalado el programa gestor SNMP MG – Soft MIB Browser).

El comando para configurar SNMP es *"snmpc"* y en el caso de que se quieran ver estadísticas relacionadas con gestión SNMP existe el comando *"snmps"*.

```
$SdeI/Networking >snmpc
SNMP current configuration:

 1) Process SNMP Packets   - enabled
 2) Set Community Name     - miramucho
 3) Get Community Name     - solomira
 4) Trap Community Name    - public
 5) Broadcast Traps        - disabled
 6) 2  Unicast Traps       - enabled
 7) NMS IP address         - 192.168.110.5 /162    -- 0000000d:0002000f
                                                   --  0000000c:00000000  (on)
(SA)

 8) NMS IP address         - 192.168.4.3   /162    -- 0000000d:0002000f
                                                   --  0000000c:00000000  (on)
(SA)
(save/quit/cancel)
   : q
```

Figura 4.56. Configuración SNMP

Existen varios parámetros configurables dentro de la gestión SNMP. Como se observa en la figura 4.56, se establecen las comunidades de escritura (set) y lectura (get), se añade la dirección de los equipos que presentarán el gestor SNMP y una máscara con determinados valores que activa las traps deseadas. El puerto 162 es el puerto

asignado en UDP para el envío de las traps SNMP, y se añade a las direcciones de dos equipos que hacen el papel de Gestor de Red, uno del Laboratorio Principal de Telemática (Local 5 – 192.168.110.5) y otro en el Laboratorio de Aplicaciones Telemáticas (192.168.4.3). La máscara por defecto activa todas las traps posibles, pero en este caso se ha establecido una máscara con las traps que se han considerado más interesantes. Observando en los manuales los valores que toman los bits en cada trap, esta máscara indica que las traps activas son [3]:

0000000d:0002000f 0000000c:00000000

Word 0 Word 1 Word 2 Word 3

- Cold start → Word 0, bit 0 = 1
- Link down → Word 0, bit 2 =1
- Link up → Word 0, bit 3 = 1

} 0000 0000 … 1 1 0 1 → 0000000d (b3 b2 b1b0; d (hexadecimal))

- Temp alarm → Word 1, bit 0 = 1
- Module change → Word 1, bit 1 = 1
- Power event → Word 1, bit 2 = 1
- Controller (MPM) event → Word 1, bit 3 = 1
- System event → Word 1, bit 17 = 1

} … 0010 0000 0000 0000 1111 → 0002000f

- Duplicate IP address → Word 2, bit 2 = 1
- Duplicate MAC address → Word 2, bit 3 = 1

} 0000 0000 …1100 → 0000000c

Cada uno de los nodos incorpora un agente SNMP que se encarga de la monitorización del propio nodo y envía la información al gestor. Los agentes SNMP se encuentran en las direcciones: 192.168.0.1 (SdeI), 192.168.0.2 (Náutica), 192.168.0.6 (Medicina), 192.168.0.10 (Enfermería) y 192.168.0.14 (Paraninfo).

Una vez finalizado el apartado correspondiente a la configuración de los nodos, se hace un volcado del estado de los nodos en un fichero de texto utilizando la línea de comandos. Este proceso es el que se realiza en la figura 4.57, en el que se crea el fichero de texto con las configuraciones del nodo SdeI.

```
$SdeI/ >cli
Entering command line interface.  Type quit to exit
->  dump all
Dump file: asc.4.snap
->  exit
```

Figura 4.57. Creación fichero de configuración (SdeI)

Posteriormente el fichero de texto creado puede ser visualizado a través de la propia interfaz de usuario utilizando el comando *"view"*. Un ejemplo de fichero de configuración final se muestra en el Anexo III.

Capítulo 5. Pruebas de funcionamiento

En este capítulo se exponen las pruebas de funcionamiento realizadas tras la configuración del sistema. En primer lugar se prueban nuevos métodos de acceso a la interfaz de usuario de los nodos como alternativa al uso de la conexión serie y el servidor DHCP configurado. Posteriormente, se analiza la configuración tanto de la red dorsal (ATM), como de la red de acceso de usuario (VLANs), estudiando los paquetes que viajan por cada una y comprobando el buen funcionamiento de la red. Del mismo modo, se presentan también las estadísticas de gestión de red obtenidas a través de los agentes instalados en cada uno de los nodos. Los resultados obtenidos se contrastarán más adelante en la red diseñada con el simulador Cisco Packet Tracer.

5.1 Métodos alternativos de acceso a los nodos

Como ya se introdujo en el apartado 4.1, la primera opción para acceder a la interfaz de usuario de los nodos es a través de una conexión serie. Pero tras configurar el direccionamiento de las interfaces de los nodos, es posible acceder haciendo telnet a dichas interfaces empleando, por ejemplo, el símbolo del sistema (cmd). En la figura 5.1 se observa un acceso al SdeI a través de la dirección 192.168.0.1 definida en el propio nodo, una vez establecida la conexión, puede configurarse el nodo de la misma forma que a través de la conexión serie. Como máximo pueden establecerse 2 conexiones simultáneas a través de un telnet, y solo la primera autenticación en el nodo tendrá permiso de escritura (si es que el usuario con el que se accede lo tiene habilitado). Una vez se ha establecido la conexión, se puede comprobar en el nodo que se está accediendo vía telnet ejecutando el comando *"tcpc"* (ver figura 5.2) con el que se muestran las conexiones tcp activas en ese momento. Si se intenta acceder vía telnet y ya hay 2 usuarios conectados, el sistema devuelve el mensaje de la figura 5.3.

```
C:/Documents and Settings/alumnos>telnet 192.168.0.1
……
Welcome to the Alcatel OmniSwitch! Version 4.3.2 GA
……
$SdeI/ >exit
Se ha perdido la conexión con el host.
```

Figura 5.1. Acceso a la UI vía telnet

```
$SdeI/ >tcpc
                        TCP Connection/Listener Table
Local Address/Port      Remote Address/Port     Recv-Q Send-Q Conn State
----------------------- ----------------------- ------ ------ ----------
192.168.0.1     /    23 192.168.4.3     /  1153      0      0 ESTABLISHED
0.0.0.0         /    23 0.0.0.0         /     0      0      0 LISTEN
0.0.0.0         /    21 0.0.0.0         /     0      0      0 LISTEN
```

Figura 5.2. Comprobación de telnet activo

```
alumnos@labpc3:~$ telnet 192.168.0.1
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.
Sorry, reached maximum number of sessions.
```

Figura 5.3. Error acceso vía telnet

Existe otra alternativa para conectarse al nodo SdeI debido a que presenta un módulo de gestión MPM diferente al que está instalado en el resto de los nodos de la red. El modelo MPM III-T que incorpora el nodo SdeI presenta un puerto Ethernet que permite el acceso a la interfaz de usuario haciendo telnet desde un equipo perteneciente a la

subred que esté configurada. Como se observó en la figura 4.23, la dirección IP del puerto de gestión es 192.168.11.1 con máscara 255.255.255.0 y, por tanto, el equipo que se conecte a este puerto de gestión debe estar configurado con un direccionamiento apropiado en la red 192.168.11.0/24. Tras conectar mediante un cable Ethernet las interfaces de un equipo del laboratorio y el puerto Ethernet incluido en el módulo MPM-III-T del nodo SdeI y establecer en el equipo del laboratorio la configuración de red de la figura 5.4, se procede a realizar un telnet a una interfaz del nodo SdeI (como en la figura 5.1) y se comprueba que aunque el proceso de configuración es el mismo al que se accede a través del puerto serie, con esta conexión se aprecia un aumento significativo de la velocidad de la comunicación.

```
C:/Documents and Settings/alumnos>ipconfig
Configuración IP de Windows
Adaptador Ethernet Conexión de área local :
        Sufijo de conexión específica DNS :
        Dirección IP. . . . . . . . . . . . : 192.168.11.5
        Máscara de subred . . . . . . . . . : 255.255.255.224
        Puerta de enlace predeterminada    : 192.168.11.1
```

Figura 5.4. Acceso mediante puerto Ethernet del módulo MPM-III-T

5.2 Comprobación DHCP

Para llevar a cabo la comprobación del funcionamiento del servidor DHCP, se observa la asignación de direcciones desde el propio servidor (ver figura 5.5) y desde un PC del laboratorio, utilizando Wireshark para analizar los paquetes intercambiados (ver figura 5.6) y se contrasta con la explicación teórica del apartado 3.2.7. En ambas figuras se ve que los paquetes 1 y 3 los envía el cliente y los paquetes 2 y 4 los envía el servidor. En el segundo mensaje el servidor le ofrece diferentes parámetros de red (dirección 192.168.4.3, máscara 255.255.255.0…) que posteriormente el cliente solicita en el tercer mensaje. El servidor DHCP guarda la MAC del equipo y le asigna unos parámetros de red la primera vez que los solicita para después entregarle los mismos parámetros en futuras peticiones.

```
Open DHCP Server Version 1.50 Windows Build 1027
Starting DHCP...
DHCP Range: 192.168.4.3-192.168.4.254/255.255.255.0
Server Name: jupiter
Detecting Static Interfaces..
Lease Status URL: http://127.0.0.1:6789
Listening On: 192.168.4.2
DHCP discover for 00:12:3f:ac:fc:63 (labpc8) from interface 192.168.4.2
received
Host 00:12:3f:ac:fc:63 (labpc8) offered 192.168.4.3
DHCP request for 00:12:3f:ac:fc:63 (labpc8) from interface 192.168.4.2
received
Host 00:12:3f:ac:fc:63 (labpc8) allotted 192.168.4.3 for 36000 seconds
```

Figura 5.5. Funcionamiento servidor DHCP

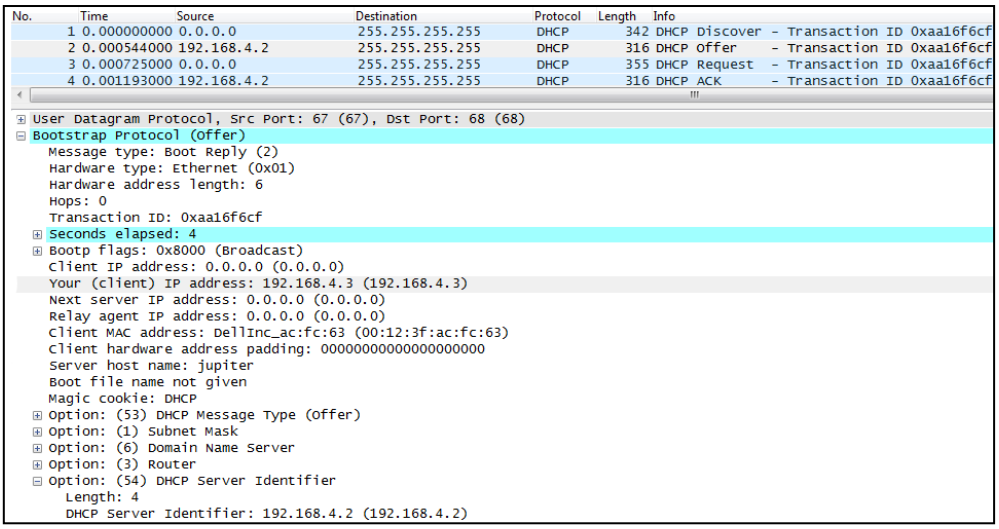


Figura 5.6. Intercambio de mensajes DHCP

5.3 Comprobación funcionamiento red troncal

Es posible visualizar estadísticas de ATM dentro de la propia interfaz de usuario del nodo ejecutando los comandos *"vls"*, para ver estadísticas de la capa ATM, y *"vcs"*, para ver estadísticas de las conexiones ATM. Para comprobar si la red troncal está configurada como se espera, es necesario analizar las celdas ATM que circulan por los enlaces troncales. Para ello, se utiliza el equipo ATM Advisor de HP disponible en el laboratorio de telemática.

Se ejecutan en el nodo de Enfermería los comandos *"vls"* y *"vcs"*. Mediante el primer comando y tal como aparece en la figura 5.7 se observan las estadísticas de envío y recepción de celdas en la capa ATM para todos los puertos (internos y físicos) que participan en el enlace troncal. Por otro lado, en la figura 5.8 aparecen las estadísticas de todas las conexiones virtuales ATM definidas en dichos puertos del enlace troncal.

```
$Enfermeria /Interface/ATM >vls
                          ATM Layer Statistics
Slot  Port   Rx SDUs     Tx SDUs     Rx Cells    Tx Cells   Rx Octets   Tx Octets
====  ====  ==========  ==========  ==========  ==========  ==========  ==========
2     1     84643       50222       135850      66382       6520800     3186336
2     2     56242       56455       63125       63676       3030000     3056448
                         CSM ATM Layer Statistics
Slot  Port     Received Cells     Received CLP=0 Cells Received CLP=1 Cells
====  ====  ====================  ====================  ====================
2     1                   66382                 66382                     0
2     2                   63676                 63676                     0
3     1                  138589                 62620                 75969
3     2                   40538                 38850                  1688
                        CSM ATM Layer Statistics
Slot  Port   Transmitted Cells      Mark EFCI Cells      Marked GCRA Cells
====  ====  ====================  ====================  ====================
2     1                  135912                     0                     0
2     2                   63125                     0                     0
3     1                   63698                     0                     0
3     2                   38925                     0                     0
```

Figura 5.7. Salida del comando *"vls"* (Enfermería)

```
$Enfermeria / >vcs
                        ATM Connection Statistics
Slot  Port VCI   Rx SDUs  Tx SDUs  Rx Cells  Tx Cells  Rx Octets  Tx Octets
==== ==== ==== ========= ========= ========= ========= ========== =========
2     1    5    4019      4031      4019      4031       192912     193488
2     1    16   20        22        40        44         1920       2112
2     1    202  453       1803      906       4495       43488      215760
2     1    404  6038      181       12076     362        579648     17376
2     2    1005 206       215       614       643        29472      30864
……
2     2    1013 4024      4020      4024      4020       193152     192960
                      CSM Connection Statistics
Slot Port VPI  VCI    Received Cells/    Transmitted Cells/
                    Received CLP=0 Cells Received CLP=1 Cells
==== ==== ==== ==== ==================== ====================
2    1    0    5                  4024                  4024
                                  4024                     0
2    1    0    16                   40                    40
                                    40                     0
2    1    0    18                    0                     0
                                     0                     0
2    1    0    202                4425                  4425
                                  4425                     0
2    1    0    404                 108                   108
                                   108                     0
2    2    0    1005                640                   640
                                   640                     0
……
2    2    0    1013               4021                  4021
                                  4021                     0
3    1    0    5                  1118                  1118
                                  1118                     0
3    1    0    16                    0                     0
                                     0                     0
3    1    0    18                  585                   585
                                   585                     0
3    1    0    32                12092                 12092
                                  4556                  7536
3    1    0    34                  924                   924
                                   235                   689
3    2    0    5                  1095                  1095
                                  1095                     0
3    2    0    16                    0                     0
                                     0                     0
3    2    0    18                  614                   614
                                   614                     0
```

Figura 5.8. Salida del comando *"vcs"* (Enfermería)

Con estas 2 figuras se comprueba que existe tráfico ATM en la red y que todas las conexiones definidas en el nodo envían y reciben celdas. En el apartado de recepción aparecen estadísticas de CLP=0 y CLP=1, que como se vio en el apartado 3.2.1 de teoría, indican si la celda debe ser descartada en caso de que haya congestión (1 indica que debe ser descartada y 0 que no), y si se suman ambos valores dan como resultado el total de celdas recibidas. Aparecen también estadísticas de conexiones en el puerto interno 2/2 (1005-1013), todas ellas son conexiones que se definen en el nodo para controlar los enlaces troncales.

ATM Advisor

Al intentar acoplar el analizador de ATM entre 2 nodos del anillo físico establecido, el sistema detecta que no se trata de un equipo perteneciente a dicho anillo y desvía las conexiones por la otra interfaz disponible, imposibilitando el análisis de las celdas ATM. El mensaje que aparece durante el proceso es "Duplicate node id detected on interface 3/1, 3/1 – PNNI hello frame ignored…" y por tanto, la única solución disponible es conectar las 2 interfaces de un mismo nodo al analizador, forzando que las celdas ATM vayan por esos enlaces. El analizador presenta las 2 interfaces que aparecen en la figura 5.9, y al igual que sucede con los nodos deben cruzarse los

pares de transmisión y recepción de cada interfaz para que funcione apropiadamente. Tras esto, debe accederse al analizador y configurarse de la siguiente forma:

Agilent Advisor – ATM Analysis – ATM Launch Current Interface → Run mode: Monitor y Framing: STS-3c.

Figura 5.9. Interfaces ATM Advisor

Usando el analizador se capturan varias celdas ATM que transportan diferentes protocolos. Las capturas realizadas se extraen a un documento .txt para que puedan ser analizadas sin usar el equipo ATM Advisor. En dichas capturas aparecen las conexiones de control y las conexiones virtuales definidas durante el desarrollo del proyecto en el enlace troncal ATM. Entre estas conexiones virtuales, hay unas sobre las que se define un servicio ATM punto a punto con encapsulamiento 802.2 LLC/SNAP (RFC1483) y otras sobre las que se definen los servicios de Trunking ATM y transportan las VLANs de los usuarios.

Análisis de una conexión virtual con servicio ATM punto a punto

```
(P2)174  18:03:50.7946990  0.33  5  ATM:CLP=High  PTI=SDU0  HEC=Good  AAL-5:
Type=NotEOM
 Record #174       (P2) Captured on 02.11.15 at 18:03:50.7946990 Length =
53
ATM:
 ATM Header = 0x00000210F
 0000 ....  .... .... .... ....  .... ....  .... .... Generic Flow Control =
0
 .... 0000  0000 ....  .... ....  .... ....  .... .... VPI = 0
 .... ....  .... 0000  0000 0010  0001 ....  .... .... VCI = 33
 .... ....  .... ....  .... ....  .... 000.  .... .... PTI = 0(User, no
cong, SDU 0)
 .... ....  .... ....  .... ....  .... ...0  .... .... Cell Loss Priority =
0 (High QoS)
 .... ....  .... ....  .... ....  .... ....  0000 1111 HEC = 0x0f (Good)

AAL-5:
  Type                  = Not End of Message
 Record #174       (P2) Captured on 02.11.15 at 18:03:50.7946990 Length =
53
      Cabecera ATM
     00 00 02 10 0f aa aa 03    00 80 c2 00 07 00 00 01    ........ ........
     80 c2 00 00 00 00 d0 95    6d ae b4 00 26 42 42 03    ........ ........
     00 00 00 00 01 80 00 00    d0 95 6d ae b4 00 00 00    ........ ........
     00 80 00 00 d0                                        .....
*************************************************************************
******
(P2) 175       18:03:50.7947017          0.33      5    ATM: CLP=Low   PTI=SDU1
HEC=Good AAL-5: Type=EOM    Len=70   CRC32=Good    RFC 1483: DSAP=aa SSAP=aa
Ctrl=UI SNAP: OUI=Bridged PID=802.3/Ethernet     MAC     src=00-D0-95-6D-AE-
B4 dst=01-80-C2-00-00-00 Len=38    LLC        Dsap=42   Ssap=42   C UF = UI
BPDU          Configuration  RPrio=32768  RADDr=0:d0:95:6d:ae:b4     RCost=0
BPrio=32768 RAddr=0:d0:95:6d:ae:b4  Port=802B
 Record #175       (P2) Captured on 02.11.15 at 18:03:50.7947017 Length =
53
ATM:
 ATM Header = 0x000002136
0000 ....  .... .... .... ....  .... ....  .... .... Generic Flow Control =
0
.... 0000  0000 ....  .... ....  .... ....  .... .... VPI = 0
.... ....  .... 0000  0000 0010  0001 ....  .... .... VCI = 33
```

```
.... ....  .... ....  .... ....  .... 001.  .... .... PTI = 1 (User, no
cong, SDU 1)
.... ....  .... ....  .... ....  .... ...1  .... .... Cell Loss Priority = 1
(Low QoS)
.... ....  .... ....  .... ....  .... ....  0000 0110 HEC = 0x06 (Good)
AAL-5: (reassembly complete: 2 cells)
  Type                    = End of Message
  User-User               = 00
  Common Part Indicator   = 00
  Length                  = 70
  CRC-32                  = 0xca-5d-8b-85 (Good)
RFC 1483:
  Destination SAP             = aa
  Source SAP                  = aa
  Control Byte                = 0x03 (UI)
SNAP:
  Organizationally Unique ID = 0x00-80-c2 (Bridged)
  Protocol ID                = 0x00-07 (802.3/Ethernet)
  Pad Bytes
------------  MAC Header  ------------
MAC: Destination: 01-80-C2-00-00-00
MAC: Source: 00-D0-95-6D-AE-B4
MAC: Length: 38
------------  LLC Header  ------------
LLC: Dsap: 0x42 (66)
LLC: Ssap: 0x42 (66) Command
LLC: Unnumbered frame: UI    (3)
------------  BPDU Header  ------------
BPDU: Protocol Identifier = 0
BPDU: Protocol Version = 0
BPDU: BPDU Type = Configuration (0x00)
BPDU: Flags = 0x01
BPDU:      0... .... Not Topology Change Acknowledgment
BPDU:      .... ...1 Topology change flag
BPDU: Root Identifier = 0x800000D0956DAEB4
BPDU:      Priority = 32768
BPDU:      MAC Address = 0:d0:95:6d:ae:b4
BPDU: Root Path Cost = 0
BPDU: Bridge Identifier = 0x800000D0956DAEB4
BPDU:      Priority = 32768
BPDU:      MAC Address = 0:d0:95:6d:ae:b4
BPDU: Port Identifier = 0x802B
BPDU: Message Age = 0 (Seconds)
BPDU: Max Age = 20 (Seconds)
BPDU: Hello Time = 2 (Seconds)
BPDU: Forward Delay = 15 (Seconds)

 Record #175       (P2) Captured on 02.11.15 at 18:03:50.7947017 Length =
53    Cabecera ATM
     00 00 02 13 06 95 6d ae    b4 80 2b 00 00 14 00 02    ........ ........
     00 0f 00 00 00 00 00 00    00 00 00 00 00 00 00 00    ........ ........
     00 00 00 00 00 00 00 00    00 00 00 00 00 00 00 00    ........ ........
     46 ca 5d 8b 85                                        .....
     (PDU length =    70 bytes)      PDU AAL5
     aa aa 03 00 80 c2 00 07    00 00 01 80 c2 00 00 00    ........ ........
     00 d0 95 6d ae b4 00 26    42 42 03 00 00 00 00 01    ........ ........
     80 00 00 d0 95 6d ae b4    00 00 00 00 80 00 00 d0    ........ ........
     95 6d ae b4 80 2b 00 00    14 00 02 00 0f 00 00 00    ........ ........
     00 00 00 00 00 00                                     ......
```

Figura 5.10. Captura conexión virtual con servicio ATM PTOP

En la figura 5.10 se observan los distintos campos que contiene una celda ATM que utiliza la capa AAL (AAL5) para adaptar los datos procedentes de capas superiores a un formato compatible con ATM. En este caso se trata de una celda perteneciente a la conexión 0/33, sobre la que se define un circuito punto a punto con encapsulación 802.2 LLC/SNAP (RFC1483). El paquete se divide en 2 celdas, ya que en la primera aparece “NotEOM” y en la segunda el “EOM”. La segunda celda agrega Bytes de relleno (Pad Bytes) para cumplir con el tamaño fijo de las celdas ATM, concretamente 27 Bytes. Esto se puede ver en la celda 175, donde los 8 últimos Bytes son el tráiler de AAL5, los 13 primeros son los datos de los protocolos de capa superior y los 27

restantes (48-13-8) son Bytes de relleno para cumplir con el tamaño fijo de las celdas ATM. Por tanto, 5 Bytes (Cabecera ATM #174) + 48 Bytes (PDU AAL5 #174)= 53 Bytes celda ATM y 5 Bytes (Cabecera ATM #175) + 13 Bytes (PDU AAL5 #175) + 8 Bytes (AAL5 Tráiler #175) + 27 Bytes (Pad Bytes #175) = 53 Bytes celda ATM.

En la cabecera ATM se puede comprobar que se trata de un tipo de interfaz UNI puesto que incluye el campo GFC (cuyo valor es siempre 0000), el campo PTI indica que se trata de una celda con datos de usuario que utiliza AAL5 en una red sin congestión. Respecto al encapsulamiento 802.2 LLC/SNAP, los resultados de la captura se corresponden también con la parte teórica explicada en el Capítulo 3, puesto que la celda #175 contiene una trama IEEE 802.3 con los mismos valores que aparecen en la figura 3.6. Como la trama IEEE 802.3 transporta una BPDU del STP, la MAC destino que aparece es multicast y aparece otra encapsulación LLC con los valores de DSAP y SSAP que identifican a este protocolo (0x42), concordando también con la teoría explicada sobre las BPDUs del STP en el apartado 3.2.3.

Análisis de una conexión virtual con servicio ATM de Trunking

```
(P2)  182  18:03:51.2945162   0.34   5 ATM:  CLP=Low  PTI=SDU0  HEC=Good  AAL-5:
Type=NotEOM
 Record #182       (P2) Captured on 02.11.15 at 18:03:51.2945162 Length =
53
ATM:
  ATM Header = 0x0000022198
……
*******************************************************************************
(P2) 183       18:03:51.2945216         0.34      5    ATM: CLP=Low   PTI=SDU1
HEC=Good AAL-5: Type=EOM     Len=68    CRC32=Good     MAC      src=00-D0-95-40-
D8-5F dst=01-80-C2-00-00-00 Len=38    LLC       Dsap=42   Ssap=42   C UF = UI
BPDU          Configuration   RPrio=32768   RADDr=0:d0:95:2a:cd:70     RCost=0
BPrio=32768 RAddr=0:d0:95:2a:cd:70  Port=8039
 Record #183       (P2) Captured on 02.11.15 at 18:03:51.2945216 Length =
53
ATM:
  ATM Header = 0x0000022396
0000 ....  .... ....  .... ....  .... ....  ....  .... Generic Flow Control
= 0
.... 0000  0000 ....  .... ....  .... ....  ....  .... VPI = 0
.... ....  .... 0000  0000 0010  0010 ....  ....  .... VCI = 34
.... .... ....  ....  .... ....  .... 001.  ....  .... PTI = 1 (User, no
cong, SDU 1)
.... ....  .... ....  .... ....  .... ...1  .... ....  Cell Loss Priority =
1 (Low QoS)
.... ....  .... ....  .... ....  .... ....  1001 0110 HEC = 0x96 (Good)
AAL-5: (reassembly complete: 2 cells)
  Type                  = End of Message
  User-User             = 00
  Common Part Indicator = 00
  Length                = 68
  CRC-32                = 0x68-d3-25-e6 (Good)
------------  MAC Header  ------------
MAC: Destination: 01-80-C2-00-00-00
MAC: Source: 00-D0-95-40-D8-5F
MAC: Length: 38
------------  LLC Header  ------------
LLC: Dsap: 0x42 (66)
LLC: Ssap: 0x42 (66) Command
LLC: Unnumbered frame: UI   (3)
------------  BPDU Header  ------------
……
 Record #183       (P2) Captured on 02.11.15 at 18:03:51.2945216 Length =
53
     Cabecera ATM
     00 00 02 23 96 02 00 0f    00 00 00 00 00 00 00 00    ........ ........
     00 00 0b 00 45 de ad be    ef 00 00 00 00 00 00 00    ........ ........
     00 00 00 00 00 00 00 00    00 00 00 00 00 00 00 00    ........ ........
     44 68 d3 25 e6                                        .....
```

```
                                                    PDU AAL5
   (PDU length =     68 bytes)
   01 80 c2 00 00 00 00 d0     95 40 d8 5f 00 26 42 42   ........ ........
   03 00 00 00 00 01 80 00     00 d0 95 2a cd 70 00 00   ........ ........
   00 00 80 00 00 d0 95 2a     cd 70 80 39 00 00 14 00   ........ ........
   02 00 0f 00 00 00 00 00     00 00 00 00 00 0b 00 45   ........ ........
   de ad be ef                                           ....
```

Figura 5.11. Captura conexión virtual con servicio ATM Trunking

La diferencia entre las celdas de la figura 5.11 y las de la figura 5.10, es que las celdas pertenecientes a las conexiones sobre las que están definidos los servicios de Trunking para el transporte de VLANs por la red troncal, no se encapsulan empleando 802.2 LLC/SNAP, sino que se definen directamente en la PDU de AAL5. Como ya se explicó en el Capítulo 3, los puertos de Trunk encapsulan las VLANs en tramas propietarias que contienen la información necesaria para reproducir la trama de origen en el extremo opuesto del Trunk.

Una vez explicadas estas capturas, se comprueban las conexiones detectadas (ver figura 5.12) y los filtros con las propiedades de estas conexiones que se crean en el analizador (ver figura 5.13).

0.5	0.16	0.18	0.37	0.36	0.38
0.32	0.39	0.40	0.34	0.33	

Figura 5.12. Conexiones detectadas por el analizador

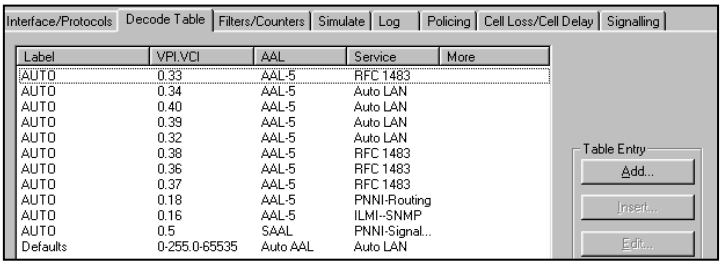


Figura 5.13. Filtros automáticos establecidos en el analizador

En este caso, sobre las conexiones 0/33, 0/36, 0/37 y 0/38, están definidos los servicios punto a punto y las celdas son como las de la figura 5.10. Sobre las conexiones 0/32, 0/34, 0/39 y 0/40, están definidos los servicios de trunking y las celdas son como las de la figura 5.11. Aparte de estas conexiones, el analizador detecta también las conexiones de gestión y señalización y son la 0/5 (ver figura 5.14), la 0/16 (ver figura 5.15) y la figura 0/18 (ver figura 5.16), todas ellas sobre AAL5 y explicadas de forma teórica en el apartado 3.2.1.

```
(P1) 238       18:03:53.7784573          0.5       5    ATM: CLP=High PTI=SDU1
HEC=Good  AAL-5:  Type=EOM        Len=8        CRC32=Good        SAAL:  POLL
N(PS)=000000c N(S)=0000002
 Record #238       (P1) Captured on 02.11.15 at 18:03:53.7784573 Length =
53
ATM:
  ATM Header = 0x00000052EC
0000 .... .... .... .... .... .... ....  .... .... Generic Flow Control = 0
.... 0000 0000 .... .... .... .... ....  .... .... VPI = 0
.... .... .... 0000 0000 0000 0101 ....  .... .... VCI = 5
.... .... .... .... .... .... .... 001.  .... .... PTI = 1 (User, no cong,
SDU 1)
.... .... .... .... .... .... .... ...0  .... .... Cell Loss Priority = 0
(High QoS)
.... .... .... .... .... .... .... ....  1110 1100 HEC = 0xec (Good)
AAL-5:
  Type                    = End of Message
  User-User               = 00
  Common Part Indicator   = 00
  Length                  = 8
```

```
  CRC-32                = 0x86-52-99-cd (Good)
SAAL:
  PDUType/PadLen = 0x0A
    .... 1010 PDU Type = Poll (POLL)
  N(PS)           = 0x00000c
  N(S)            = 0x000002
 Record #238       (P1) Captured on 02.11.15 at 18:03:53.7784573 Length =
53
    00 00 00 52 ec 00 00 00    0c 0a 00 00 02 00 00 00    ........ ........
    00 00 00 00 00 00 00 00    00 00 00 00 00 00 00 00    ........ ........
    00 00 00 00 00 00 00 00    00 00 00 00 00 00 00 00    ........ ........
    08 86 52 99 cd                                        .....
    (PDU length =     8 bytes)
    00 00 00 0c 0a 00 00 02                               ......
```

Figura 5.14. UNI Call Signaling (0/5)

La particularidad de la conexión 0/5 es que transporta la información de señalización sobre SAAL (ATM Adaptation Layer for Signaling).

```
(P1) 461       18:04:03.3133846         0.16      5    ATM: CLP=High PTI=SDU1
HEC=Good AAL-5: Type=EOM      Len=39     CRC32=Good      SNMP      GetRequest
0x4
 Record #461       (P1) Captured on 02.11.15 at 18:04:03.3133846 Length =
53
ATM:
  ATM Header = 0x000001024E
0000 .... .... .... .... .... .... ....  .... .... Generic Flow Control = 0
.... 0000 0000 .... .... .... .... ....  .... .... VPI = 0
.... .... .... 0000 0000 0001 0000 ....  .... .... VCI = 16
.... .... .... .... .... .... .... 001.  .... .... PTI = 1 (User, no cong,
SDU 1)
.... .... .... .... .... .... .... ...0  .... .... Cell Loss Priority = 0
(High QoS)
.... .... .... .... .... .... .... ....  0100 1110 HEC = 0x4e (Good)
AAL-5:
  Type                  = End of Message
  User-User             = 00
  Common Part Indicator = 00
  Length                = 39
  CRC-32                = 0xf4-8e-06-fc (Good)
------------  SNMP Header  ------------
SNMP: Version = 0
SNMP: Community = ILMI
SNMP: PDU = GetRequest
SNMP: Request identifier = 0x4 (4)
SNMP: Error status = noError (0)
SNMP: Error index = 0
SNMP: Object = 1.3.6.1.2.1.system.sysUpTime.0
 Record #461       (P1) Captured on 02.11.15 at 18:04:03.3133846 Length =
53
    00 00 01 02 4e 30 25 02    01 00 04 04 49 4c 4d 49    ........ ........
    a0 1a 02 01 04 02 01 00    02 01 00 30 0f 30 0d 06    ........ ........
    08 2b 06 01 02 01 01 03    00 02 01 00 00 00 00 00    ........ ........
    27 f4 8e 06 fc                                        .....
    (PDU length =    39 bytes)
    30 25 02 01 00 04 04 49    4c 4d 49 a0 1a 02 01 04    ........ ........
    02 01 00 02 01 00 30 0f    30 0d 06 08 2b 06 01 02    ........ ........
1 03 00 02 01 00                                        ......
```

Figura 5.15. ILMI Get Request (0/16)

Como se explicó en el apartado teórico, ILMI utiliza mensajes SNMP (sin UDP ni IP) y, en este caso, aparece la captura de un mensaje tipo GetRequest (sysUpTime).

```
(P2) 550       18:04:08.5480967         0.18      5    ATM: CLP=High PTI=SDU0
HEC=Good AAL-5: Type=NotEOM
 Record #550       (P2) Captured on 02.11.15 at 18:04:08.5480967 Length =
53
……
(P2) 551       18:04:08.5480995         0.18      5    ATM: CLP=High PTI=SDU0
HEC=Good AAL-5: Type=NotEOM
……
(P2) 552       18:04:08.5481027         0.18      5    ATM: CLP=High PTI=SDU1
HEC=Good AAL-5: Type=EOM    Len=100  CRC32=Good    PNNI: Type=Hello
 Record #552       (P2) Captured on 02.11.15 at 18:04:08.5481027 Length =
```

```
53
ATM:
  ATM Header = 0x00000122AE
0000 .... .... .... .... ....  .... .... .... .... Generic Flow Control = 0
.... 0000 0000 .... .... ....  .... .... .... .... VPI = 0
.... .... .... 0000 0000 0001  0010 .... .... .... VCI = 18
.... .... .... .... .... ....  .... 001. .... .... PTI = 1 (User, no cong,
SDU 1)
.... .... .... .... .... ....  .... ...0 .... .... Cell Loss Priority = 0
(High QoS)
.... .... .... .... .... ....  .... .... 1010 1110 HEC = 0xae (Good)
AAL-5: (reassembly complete: 3 cells)
  Type                   = End of Message
  User-User              = 00
  Common Part Indicator = 00
  Length                 = 100
  CRC-32                 = 0xb0-f9-d9-27 (Good)
PNNI:
  Packet Type     = Hello (1)
  Packet Length   = 100 Bytes
  Protocol Version= 1
  Newest Version  = 1
  Oldest Version  = 1
  Reserved        = 0x00
  Flags           = 0x0000
  Node ID         = 0x50A03903488001BC90000101DBE2A00020DADBE2A000
  ATM        ES        Addr                                                =
57.3.72.128.1.188.144.0.1.1.219.226.160.0.32.218.219.226.160.0
  Peer Group ID            = 0x503903488001BC90000101000000
  Remote Node ID           = 0x00000000000000000000000000000000000000000000000000
  Port ID                  = 0x00000080
  Remote Port ID           = 0x00000000
  Hello Interval           = 15 Seconds
  Reserved                 = 0x0000
 Record #552       (P2) Captured on 02.11.15 at 18:04:08.5481027 Length =
53
……
```

Figura 5.16. PNNI Hello (0/18)

IP sobre ATM

```
……(6 celdas anteriores)
(P1) 259       18:11:16.0246323         0.32      5    ATM: CLP=High PTI=SDU1
HEC=Good  AAL-5:  Type=EOM      Len=312    CRC32=Good       RFC  1483:  DSAP=aa
SSAP=aa Ctrl=UI SNAP: OUI=Bridged PID=802.3/Ethernet      ETHER    00-00-00-
00-00-00  ->  00-00-00-00-00-00  Proto=IP        IP            192.168.2.5  ->
192.168.2.1 Id=0004 ICMP    Echo request
 Record #259       (P1) Captured on 02.11.15 at 18:11:16.0246323 Length =
53
ATM:
  ATM Header = 0x0000020271
0000 .... .... .... .... .... .... ....  .... .... Generic Flow Control = 0
.... 0000 0000 .... .... .... .... ....  .... .... VPI = 0
.... .... .... 0000 0000 0010 0000 ....  .... .... VCI = 32
.... .... .... .... .... .... .... 001.  .... .... PTI = 1 (User, no cong,
SDU 1)
.... .... .... .... .... .... .... ...0  .... .... Cell Loss Priority = 0
(High QoS)
.... .... .... .... .... .... .... ....  0111 0001 HEC = 0x71 (Good)
AAL-5: (reassembly complete: 7 cells)
  Type                   = End of Message
  User-User              = 00
  Common Part Indicator = 00
  Length                 = 312
  CRC-32                 = 0xf3-d5-ed-d2 (Good)
RFC 1483:
  Destination SAP            = aa
  Source SAP                 = aa
  Control Byte               = 0x03 (UI)
SNAP:
  Organizationally Unique ID = 0x00-80-c2 (Bridged)
  Protocol ID                = 0x00-01 (802.3/Ethernet)
  Pad Bytes
```

```
------------  ETHER Header  ------------
ETHER: Destination: 00-00-00-00-00-00
ETHER: Source: 00-00-00-00-00-00
ETHER: Protocol: IP
------------  IP Header  ------------
IP: Version = 4
IP: Header length = 20
IP: Differentiated Services (DS) Field = 0x00
IP:     0000 00.. DS Codepoint = Default PHB (0)
IP:     .... ..00 Unused
IP: Packet length = 284
IP: Id = 4
IP: Fragmentation Info = 0x0000
IP:     .0.. ....  .... .... Don't Fragment Bit = FALSE
IP:     ..0. ....  .... .... More Fragments Bit = FALSE
IP:     ...0 0000  0000 0000 Fragment offset = 0
IP: Time to live = 255
IP: Protocol = ICMP (1)
IP: Header checksum = 3586
IP: Source address = 192.168.2.5
IP: Destination address = 192.168.2.1
------------  ICMP Header  ------------
ICMP: Type = Echo request (8)
ICMP: Code = 0
ICMP: Checksum = 9D1B
ICMP: Identifier = 0 (0x0)
ICMP: Sequence Number = 0 (0x0)
ICMP: 256 bytes of data
 Record #259       (P1) Captured on 02.11.15 at 18:11:16.0246323 Length =
53
……
```

Figura 5.17. Captura IP sobre ATM

Por las dificultades de introducir el nodo en el anillo físico del laboratorio comentadas anteriormente, no es posible ver mensajes de Echo Reply, pero la encapsulación es la misma que en el mensaje de la figura 5.17. En ella se ve que el datagrama IP se encapsula en una trama Ethernet cuyo campo Tipo toma el valor de 0x0800 y esta trama se encapsula siguiendo el RFC 1483 en celdas con 802.2 LLC/SNAP.

5.4 Comprobación funcionamiento red de acceso de usuarios

Para comprobar el funcionamiento de las VLANs creadas en esta red, se utiliza el analizador de protocolos Wireshark y el analizador LAN Advisor de HP. Con el primero se analizan capturas de tráfico entre VLANs y se estudian los mensajes que aparecen entre equipos configurados en distintas VLANs. Con el LAN Advisor se muestran 2 partes de una captura realizada en el puerto de Trunking de un nodo para ver el etiquetado de las VLANs y el formato de paquetes que viajan por la red.

Para analizar los mensajes de distintas VLANs se configuran 3 PC del laboratorio con el direccionamiento que aparece en la figura 5.18:

```
C:/Documents and Settings/alumnos>ipconfig/all
Configuración IP de Windows
        Nombre del host . . . . . . . . . . : labpc3
        Dirección física. . . . . . . . . . : 00-12-3F-AC-FC-FE
        Dirección IP. . . . . . . . . . . . : 192.168.2.40
        Máscara de subred . . . . . . . . . : 255.255.255.224
        Puerta de enlace predeterminada   : 192.168.2.33
        Servidores DNS . . . . . . . . . . .: 192.168.110.11
C:/Documents and Settings/alumnos>ipconfig/all
Configuración IP de Windows
        Nombre del host . . . . . . . . . . : labpc4
        Dirección física. . . . . . . . . . : 00-12-3F-AD-30-8A
        Dirección IP. . . . . . . . . . . . : 192.168.3.100
        Máscara de subred . . . . . . . . . : 255.255.255.224
        Puerta de enlace predeterminada   : 192.168.3.97
        Servidores DNS . . . . . . . . . . .: 192.168.110.11
```

VLAN 11 (Náutica)

VLAN 12 (Medicina)

```
C:/Documents and Settings/alumnos>ipconfig/all
Configuración IP de Windows
        Nombre del host . . . . . . . . . . : labpc5
        Dirección física. . . . . . . . . . : 00-12-3F-AC-FC-8C
        Dirección IP. . . . . . . . . . . . : 192.168.3.130
        Máscara de subred . . . . . . . . . : 255.255.255.224
        Puerta de enlace predeterminada     : 192.168.3.129
        Servidores DNS . . . . . . . . . . .: 192.168.110.11
```

VLAN 12 (Enfermería)

Figura 5.18. Direccionamiento PCs laboratorio (1)

El equipo labpc4 envía un ping a los otros 2 equipos, y ambos responden. En el primer ping a labpc3, únicamente comparten los echo request-reply, pero en el segundo ping a labpc5, se ven los ARP de broadcast enviados, tanto en labpc4 como en labpc5, además de los echo request-reply entre los 2 dispositivos. En estos mensajes de echo, las MAC de origen y destino cambian porque cambia la subred.

En la figura 5.19 se muestra la captura de labpc3 (192.168.2.40), en la figura 5.20 la de labpc4 (192.168.3.100) y en la figura 5.21 la de labpc5 (192.168.3.130).

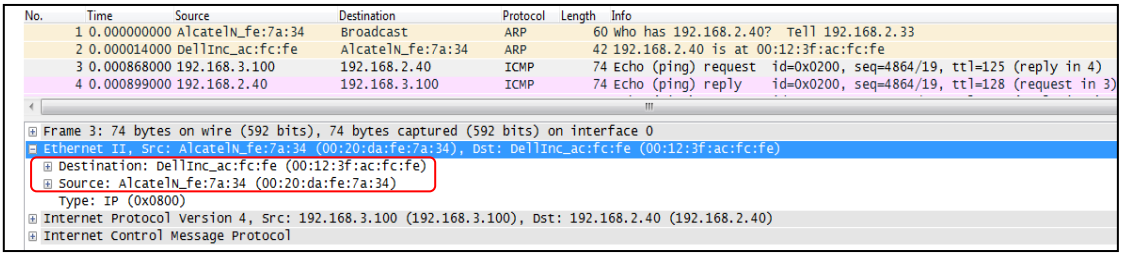


Figura 5.19. Captura labpc3 (1)

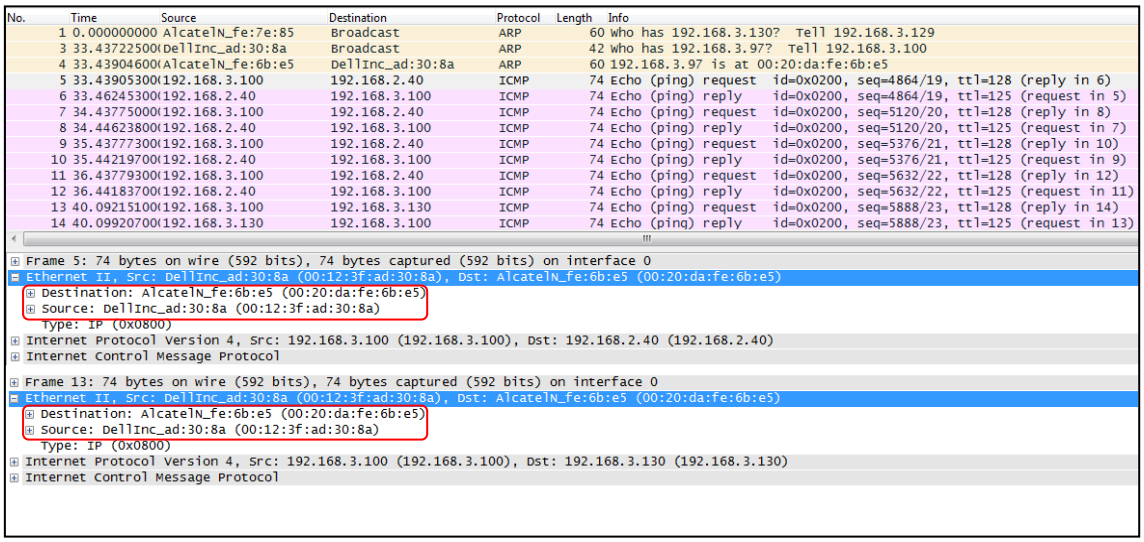


Figura 5.20. Captura labpc4 (1)

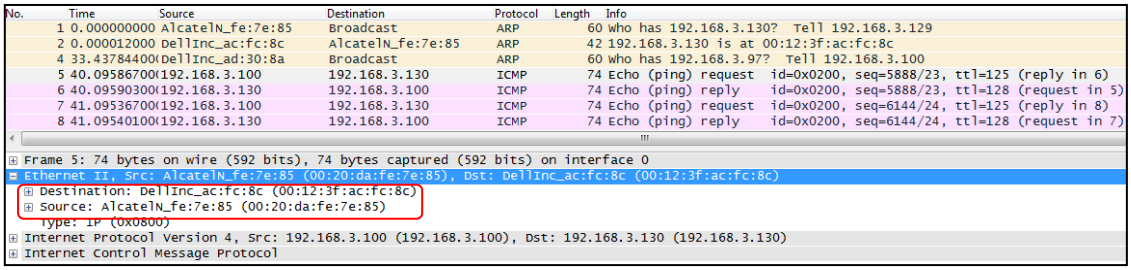


Figura 5.21. Captura labpc5 (1)

En la figura 5.19 se ven los ARP de la red a la que pertenece el equipo, y aunque el primer mensaje es de broadcast, no aparece en las otras capturas al estar en una red

diferente. En el segundo mensaje el equipo responde al nodo cual es su dirección MAC, esta vez en mensaje unicast. En las figuras 5.20 y 5.21, pueden verse los mensajes de broadcast ARP solicitando las direcciones MAC de capa 2, pero los dispositivos ignoran el mensaje ARP Request puesto que no va destinado a ellos. Después, al igual que en el caso anterior, la respuesta es unicast.

Al estar en subredes diferentes, en los mensajes de echo que intercambian los equipos se puede ver que cambian la MACs de la estación que envía o recibe los paquetes y se sustituye por la del nodo (SVI). En el caso de los paquetes que llegan a labpc3 y labpc5, el campo Source es el de la interfaz del router virtual por el que se enruta el paquete de entrada, y en el caso de la figura 5.20, el campo Destination es el de la interfaz del router virtual por el que se enrutan los paquetes de salida. Por tanto, al cambiar las MACs de origen/destino por la de un dispositivo con funciones de Capa 3, quiere decir que es necesario enrutamiento y por tanto las VLANs son distintas.

Por último, se ejecuta un *"traceroute"*, que se observa en la figura 5.22, desde labpc4 para ver la ruta que siguen los paquetes hasta llegar a su destino.

```
C:/Documents and Settings/alumnos>tracert 192.168.2.40
Traza a la dirección [192.168.2.40] (labpc3) sobre un máximo de 30 saltos:
  1     2 ms     3 ms     4 ms  [192.168.3.97] (Router VLAN 12 Medicina)
  2     1 ms     1 ms     1 ms  [192.168.0.5]  (Interfaz SdeI-Medicina)
  3     4 ms     3 ms     3 ms  [192.168.0.2]  (Interfaz Náutica-SdeI)
  4     2 ms     2 ms     1 ms  [192.168.2.40] (labpc3)
Traza completa.
C:/Documents and Settings/alumnos>tracert 192.168.3.130
Traza a 192.168.3.130 (labpc5) sobre caminos de 30 saltos como máximo.
  1     2 ms     3 ms     3 ms  [192.168.3.97]  (Router VLAN 12 Medicina)
  2     4 ms     1 ms     1 ms  [192.168.0.5]   (Interfaz SdeI-Medicina)
  3    10 ms     6 ms     3 ms  [192.168.0.10]  (Interfaz Enfermería-SdeI)
  4    13 ms     2 ms     2 ms  [192.168.3.130] (labpc5)
Traza completa.
```

Figura 5.22. Traceroute (1)

Se comprueba que para llegar a su destino, el paquete necesita ser enrutado, y por tanto, los equipos están en diferentes VLANs.

Tras realizar las pruebas descritas anteriormente, se cambia el direccionamiento de labpc5, el PC sigue estando conectado al nodo de Enfermería, pero ahora su direccionamiento es el de un PC conectado al nodo de Medicina (ver figura 5.23)

```
labpc3 y labpc4 mantienen la misma configuración que en la figura 5.18
C:/Documents and Settings/alumnos>ipconfig/all
Configuración IP de Windows
        Nombre del host . . . . . . . . . . : labpc5
        Dirección física. . . . . . . . . . : 00-12-3F-AC-FC-8C
        Dirección IP. . . . . . . . . . . . : 192.168.3.110
        Máscara de subred . . . . . . . . . : 255.255.255.224
        Puerta de enlace predeterminada   : 192.168.3.97
        Servidores DNS . . . . . . . . . . .: 192.168.110.11
```

VLAN 12 (Medicina) Equipo conectado a Enfermería

Figura 5.23. Direccionamiento PCs laboratorio (2)

El equipo labpc4 envía un ping a los otros 2 equipos, y ambos responden. En el primer ping a labpc3, únicamente comparten los echo request-reply (MAC de origen y destino cambian porque cambia la subred), pero en el segundo ping a labpc5, se ven los ARP de broadcast enviados, tanto en labpc4 como en labpc5, además de los echo request-reply entre los 2 dispositivos. En estos mensajes de echo, las MACs de origen y destino no cambian porque se envían por la misma subred.

En la figura 5.24 se muestra la captura de labpc3 (192.168.2.40), en la figura 5.25 la de labpc4 (192.168.3.100) y en la figura 5.26 la de labpc5 (192.168.3.110).

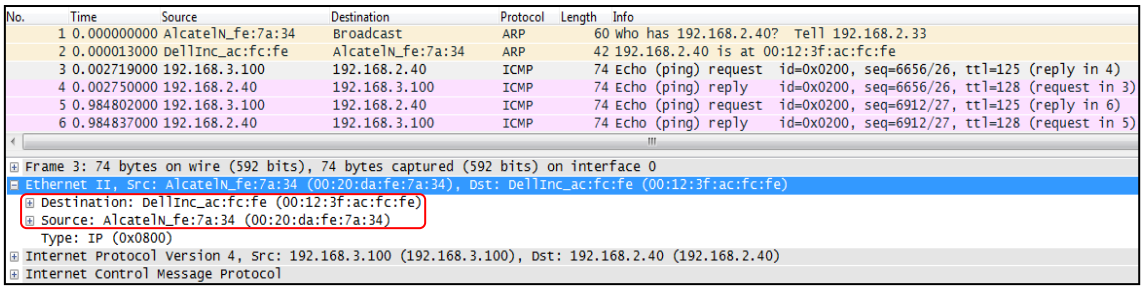


Figura 5.24. Captura labpc3 (2)

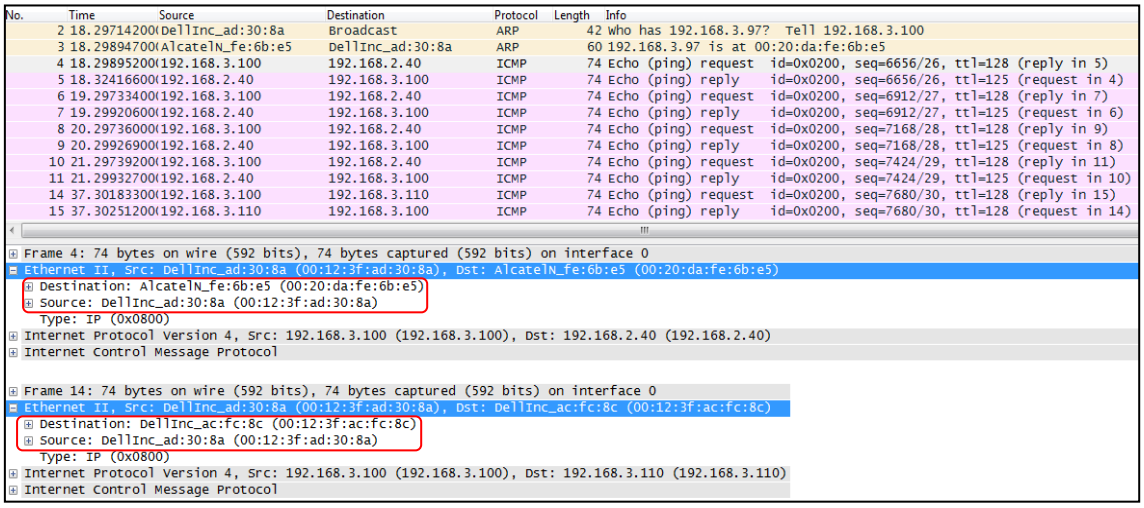


Figura 5.25. Captura labpc4 (2)

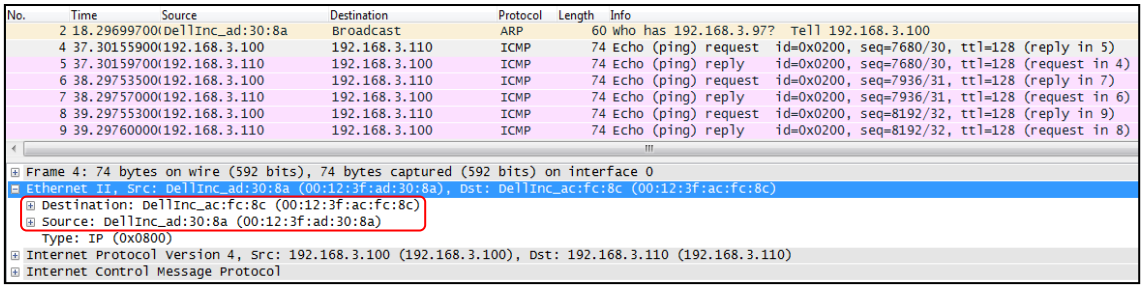


Figura 5.26. Captura labpc5 (2)

En la figura 5.24 se ven los ARP de la red a la que pertenece el equipo, y aunque el primer mensaje es de broadcast, no aparece en las otras capturas al estar en una red diferente. En el segundo mensaje el equipo responde al nodo cual es su dirección MAC, esta vez en mensaje unicast. En las figuras 5.25 y 5.26, pueden verse los mensajes de broadcast ARP solicitando las direcciones MAC de capa 2 en la subred. Después, al igual que en el caso anterior, la respuesta es unicast.

Al estar en subredes diferentes, en los mensajes de echo que intercambian labpc3 y labpc4 (figura 5.24 y primer ICMP figura 5.25) se puede ver que cambian la MACs de la estación que envía o recibe los paquetes y se sustituye por la del nodo (SVI). En el caso de los paquetes entre labpc4 y labpc5 (figura 5.26 y segundo ICMP figura 5.25), se observa que al haber cambiado el direccionamiento de labpc5, las MAC de origen y destino se corresponden con las de los PC. Por tanto, los PC labpc4 y labpc5 se encuentran ahora en una misma subred (VLAN) y el PC labpc3 está situado en otra subred diferente.

Por último, se ejecuta un *"traceroute"*, que se observa en la figura 5.27, desde labpc4 para ver la ruta que siguen los paquetes hasta llegar a su destino.

```
C:/Documents and Settings/alumnos>tracert 192.168.2.40
Traza a la dirección [192.168.2.40] (labpc3)
sobre un máximo de 30 saltos:
  1     2 ms     3 ms     3 ms  [192.168.3.97] (Router VLAN 12 Medicina)
  2     5 ms     2 ms     1 ms  [192.168.0.5]  (Interfaz SdeI-Medicina)
  3     8 ms     3 ms     3 ms  [192.168.0.2]  (Interfaz Náutica-SdeI)
  4    11 ms     2 ms     1 ms  [192.168.2.40] (labpc3)
Traza completa.
C:/Documents and Settings/alumnos>tracert 192.168.3.110
Traza a la dirección [192.168.3.110] (labpc5) sobre un máximo de 30 saltos:
  1     1 ms    <1 ms    <1 ms  [192.168.3.110] (labpc5)
Traza completa.
```

Figura 5.27. Traceroute (2)

Se comprueba que para llegar a labpc3 el paquete tiene que ser enrutado y por tanto el PC no está en la misma subred que labpc4, pero en este caso, el paquete con destino lapc5 llega de un solo salto entre 2 equipos de la misma subred, estando por tanto labpc4 y lapc5 en la misma VLAN. Además de esto, se probó también que 2 equipos sin salida a Internet estando en la misma VLAN, pueden comunicarse.

LAN Advisor

Para capturar con este analizador debe accederse a: Agilent Advisor – LAN Analysis – Ethernet undercradle y configurar el analizador en modo internal AUI. Debe conectarse por cable Ethernet el PC al puerto "To Hub / Switch" del analizador (ver figura 5.28).

Figura 5.28. Interfaces LAN Advisor

Se utiliza el analizador para capturar en el puerto de Trunking configurado en los nodos y se muestran 2 tramas extraídas de un archivo .txt. La figura 5.29 muestra una trama en la que se integra el MSTP (puesto que cada VLAN utiliza el STP de forma independiente) y mediante el envío de BPDUs buscan cual es el switch raíz. La figura 5.30 muestra un paquete IP con dirección destino la dirección de broadcast de una subred (que corresponde a la VLAN 12 de Enfermería).

```
    2    68  16:09:04.367231   00-D0-95-2A-CD-6F            01-80-C2-00-00-00
VLAN      00-D0-95-2A-CD-6F  ->  01-80-C2-00-00-00  VID=10  LLC        Dsap=42
Ssap=42     C   UF   =   UI          BPDU          Configuration   RPrio=32768
RADDr=0:20:da:de:42:13   RCost=7          BPrio=32768  RAddr=0:d0:95:2a:cd:6f
Port=8026
 Record  #2              (From  Hub  To  Node)  Captured  on  02.05.15  at
16:09:04.367231200 Length =    68
 Runtime Frame# 2
------------  VLAN Header  ------------
VLAN: VLAN Tagged Frame Media Type = 802.3/Ether
VLAN: Destination Address = 01-80-C2-00-00-00
VLAN: Source Address = 00-D0-95-2A-CD-6F
VLAN: VLAN Tag Type = 0x8100
VLAN: Tag Control Information (TCI) = 0x000A
VLAN:  000. ....  .... .... User Priority = 0
VLAN:  ...0 ....  .... .... CFI = E-RIF Absent, MAC Format Is Canonical (0)
VLAN:      .... 0000  0000 1010 VLAN ID = 10
VLAN: Length = 38
VLAN: FCS = E14456FD
------------  LLC Header  ------------
LLC: Dsap: 0x42 (66)
LLC: Ssap: 0x42 (66) Command
LLC: Unnumbered frame: UI   (3)
------------  BPDU Header  ------------
```

```
BPDU: Protocol Identifier = 0
BPDU: Protocol Version = 0
BPDU: BPDU Type = Configuration (0x00)
BPDU: Flags = 0x00
BPDU:     0... .... Not Topology Change Acknowledgment
BPDU:     .... ...0 Not Topology change
BPDU: Root Identifier = 0x80000020DADE4213
BPDU:     Priority = 32768
BPDU:     MAC Address = 0:20:da:de:42:13
BPDU: Root Path Cost = 7
BPDU: Bridge Identifier = 0x800000D0952ACD6F
BPDU:     Priority = 32768
BPDU:     MAC Address = 0:d0:95:2a:cd:6f
BPDU: Port Identifier = 0x8026
BPDU: Message Age = 0 (Seconds)
BPDU: Max Age = 20 (Seconds)
BPDU: Hello Time = 2 (Seconds)
BPDU: Forward Delay = 15 (Seconds)
BPDU: 8 bytes of padding
 Record  #2              (From  Hub  To  Node)  Captured  on  02.05.15  at
16:09:04.367231200 Length =    68
    01 80 c2 00 00 00 00 d0    95 2a cd 6f 81 00 00 0a    ........ ........
    00 26 42 42 03 00 00 00    00 00 80 00 00 20 da de    ........ ........
    42 13 00 00 00 07 80 00    00 d0 95 2a cd 6f 80 26    ........ ........
    00 20 14 00 02 00 0f 00    00 00 00 00 00 00 00 00    ........ ........
    e1 44 56 fd                                           ....
```

Figura 5.29. VLAN STP (MSTP)

En esta trama se observa que la VLAN 10 utiliza el protocolo ST para buscar cual es el switch raíz. La cabecera inicial que aparece es IEEE 802.3 (campo Length) y al usar el campo TPID 0x8100 quiere decir que la trama transporta una VLAN (en este caso el ID de la VLAN es 10). La MAC destino es multicast (propia del protocolo ST) y la BPDU se encapsula en LLC con DSAP y SSAP igual a 0x42 que indica que el protocolo que transportan es ST.

```
115     82  16:10:06.679072   192.168.3.130                    192.168.3.159
VLAN       00-12-3F-AC-FC-8C  ->  Broadcast  VID=12  EncapsProto=IP       IP
192.168.3.130 -> 192.168.3.159 Id=6fe8 ICMP    Echo request
 Record  #115           (From  Hub  To  Node)  Captured  on  02.05.15  at
16:10:06.679072600 Length =    82
 Runtime Frame# 115
------------  VLAN Header  ------------
VLAN: VLAN Tagged Frame Media Type = 802.3/Ether
VLAN: Destination Address = Broadcast
VLAN: Source Address = 00-12-3F-AC-FC-8C
VLAN: VLAN Tag Type = 0x8100
VLAN: Tag Control Information (TCI) = 0x000C
VLAN:  000. ....  .... .... User Priority = 0
VLAN:  ...0 ....  .... .... CFI = E-RIF Absent, MAC Format Is Canonical (0)
VLAN:     .... 0000  0000 1100 VLAN ID = 12
VLAN: Encapsulated Protocol = IP (0x0800)
VLAN: FCS = 41C0736B
------------  IP Header  ------------
IP: Version = 4
IP: Header length = 20
IP: Differentiated Services (DS) Field = 0x00
IP:     0000 00.. DS Codepoint = Default PHB (0)
IP:     .... ..00 Unused
IP: Packet length = 60
IP: Id = 6fe8
IP: Fragmentation Info = 0x0000
IP:     .0.. ....  .... .... Don't Fragment Bit = FALSE
IP:     ..0. ....  .... .... More Fragments Bit = FALSE
IP:     ...0 0000  0000 0000 Fragment offset = 0
IP: Time to live = 128
IP: Protocol = ICMP (1)
IP: Header checksum = 4267
IP: Source address = 192.168.3.130
IP: Destination address = 192.168.3.159
------------  ICMP Header  ------------
ICMP: Type = Echo request (8)
ICMP: Code = 0
ICMP: Checksum = 475C
```

```
ICMP: Identifier = 512 (0x200)
ICMP: Sequence Number = 1024 (0x400)
ICMP: 32 bytes of data
 Record  #115            (From  Hub  To  Node)  Captured  on  02.05.15  at
16:10:06.679072600 Length =    82
    ff ff ff ff ff ff 00 12    3f ac fc 8c 81 00 00 0c    ........ ........
    08 00 45 00 00 3c 6f e8    00 00 80 01 42 67 c0 a8    ........ ........
    03 82 c0 a8 03 9f 08 00    47 5c 02 00 04 00 61 62    ........ ........
    63 64 65 66 67 68 69 6a    6b 6c 6d 6e 6f 70 71 72    ........ ........
    73 74 75 76 77 61 62 63    64 65 66 67 68 69 41 c0    ........ ........
    73 6b                                                 ..
```

Figura 5.30. IP broadcast puerto trunking

La estructura de la trama coincide con la que se presentó en el apartado teórico (figura 3.15). La MAC de origen que aparece en la de un PC del laboratorio configurado en la VLAN 12 de Enfermería, que ejecuta un ping a la dirección de broadcast de su subred. El datagrama IP se encapsula directamente en el campo de Datos de Ethernet, que al ser formato Ethernet II no necesita usar la cabecera LLC/SNAP, indicando en su campo Tipo que se encapsula IP con el valor 0x0800.

5.5 Gestión de red SNMP

En este apartado se exponen las capturas de pantalla realizadas en el gestor de red que utiliza el software MIB Browser para comprobar el estado de las interfaces y ver información de gestión en el nodo de Paraninfo. Las MIBs que se utilizan son (figura 5.31), por una parte, la MIB-2 estándar (iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).) y por otro las MIB privadas del fabricante XYLAN tras haber sido compiladas usando el MIB compiler que incorpora el software.

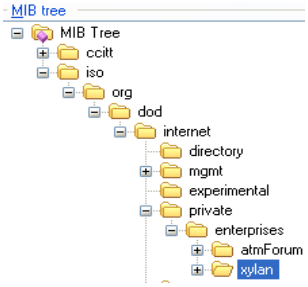


Figura 5.31. MIB Tree

Antes de poder visualizar la información de gestión, se configura el software con las comunidades apropiadas, como aparece en la figura 5.32 y se comprueba que los agentes de los nodos están activos, tal y como se ve en la figura 5.33 [28].

Figura 5.32. Configuración software MIB Browser

```
Remote address: 192.168.0.1  port: 161 transport: IP/UDP          (SdeI)
Local address: 192.168.4.3  port: 3837 transport: IP/UDP
Protocol version: SNMPv1
1: sysUpTimeInstance (timeticks) 0 days 05h:41m:32s.00th (2049200)
Remote address: 192.168.0.2  port: 161 transport: IP/UDP         (Náutica)
Local address: 192.168.4.3  port: 3839 transport: IP/UDP
Protocol version: SNMPv1
1: sysUpTimeInstance (timeticks) 0 days 05h:41m:41s.74th (2050174)
Remote address: 192.168.0.6  port: 161 transport: IP/UDP         (Medicina)
Local address: 192.168.4.3  port: 3843 transport: IP/UDP
Protocol version: SNMPv1
1: sysUpTimeInstance (timeticks) 0 days 05h:42m:11s.53th (2053153)
Remote address: 192.168.0.10  port: 161 transport: IP/UDP       (Enfermería)
Local address: 192.168.4.3  port: 3845 transport: IP/UDP
Protocol version: SNMPv1
1: sysUpTimeInstance (timeticks) 0 days 05h:42m:16s.79th (2053679)
Remote address: 192.168.0.14  port: 161 transport: IP/UDP        (Paraninfo)
Local address: 192.168.4.3  port: 3847 transport: IP/UDP
Protocol version: SNMPv1
1: sysUpTimeInstance (timeticks) 0 days 05h:42m:08s.38th (2052838)
```

Figura 5.33. Comprobaciones agentes

Por último, se muestran las siguientes capturas que contienen información de gestión del nodo Paraninfo: La figura 5.34 muestra estadísticas de la capa ATM, celdas transmitidas, recibidas… en las interfaces 2/1 (servicios ATM) y 2/2 (control). En la figura 5.35 aparecen los servicios ATM creados en el nodo, el primero un servicio punto a punto con encapsulamiento RFC1483 y el segundo un servicio ATM de Trunking. Con la figura 5.36 se comprueba que tanto las interfaces internas (ATM) como las interfaces físicas (CSM) están activas. Mediante la figura 5.37 se pueden consultar las estadísticas (celdas enviadas, recibidas…) de las conexiones virtuales ATM (de control y las definidas para soportar los servicios ATM creados) tanto en la interfaz interna (slot 2) como en la interfaz física (slot 3), en este caso los circuitos 201 y 403 definidos en la interfaz 2/1 salen por la interfaz 3/1 con las etiquetas 41 y 42. En la figura 5.38 se muestran los routers virtuales del nodo y en la figura 5.39 se muestra la tabla de rutas del Paraninfo. Por último en la figura 5.40 aparecen las VLANs creadas en el nodo.

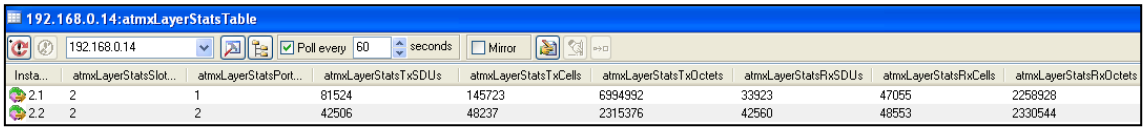


Figura 5.34. Estadísticas capa ATM (SNMP)

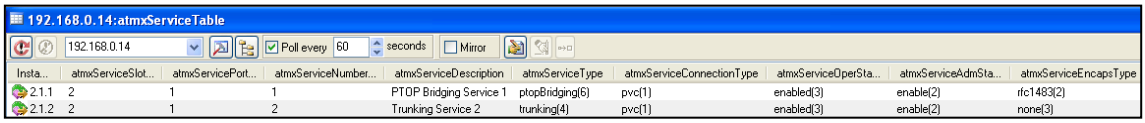


Figura 5.35. Servicios ATM (SNMP)

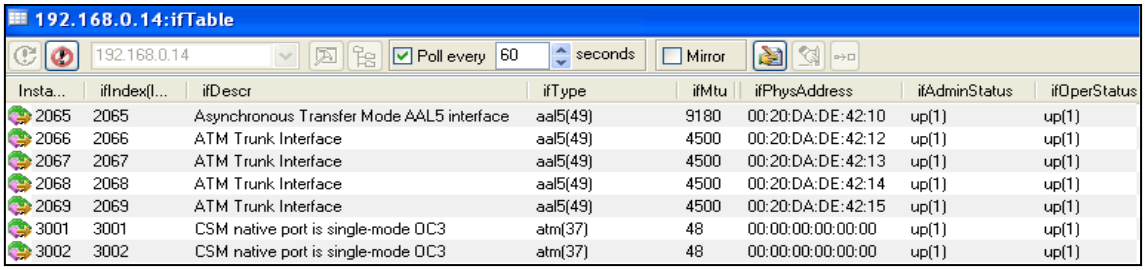


Figura 5.36. Comprobación de interfaces (SNMP)

192.168.0.14:xylnatmVclStatTable

192.168.0.14 | Poll every 60 seconds | Mirror

Instance	xylnatmVclStatSlot...	xylnatmVclStatPort...	xylnatmVclStatVpi...	xylnatmVclStatVci...	xylnatmVclStatRxCells	xylnatmVclStatTxCells	xylnatmVclStatRxClp0Cells
2.1.0.5	2	1	0	5	26509	26511	26511
2.1.0.16	2	1	0	16	4002	4002	4002
2.1.0.18	2	1	0	18	0	0	0
2.1.0.201	2	1	0	201	20546	20629	20710
2.1.0.403	2	1	0	403	8123	8127	8131
2.2.0.1005	2	2	0	1005	4081	4081	4081
2.2.0.1006	2	2	0	1006	0	0	0
2.2.0.1007	2	2	0	1007	7400	7400	7401
2.2.0.1008	2	2	0	1008	2686	2686	2686
2.2.0.1009	2	2	0	1009	0	0	0
2.2.0.1010	2	2	0	1010	4646	4646	4646
2.2.0.1011	2	2	0	1011	0	0	0
2.2.0.1012	2	2	0	1012	4002	4002	4002
2.2.0.1013	2	2	0	1013	26513	26513	26513
3.1.0.5	3	1	0	5	4653	4653	4653
3.1.0.16	3	1	0	16	0	0	0
3.1.0.18	3	1	0	18	2542	2542	2542
3.1.0.41	3	1	0	41	355	355	355
3.1.0.42	3	1	0	42	8	8	8
3.2.0.5	3	2	0	5	7529	7530	7530
3.2.0.16	3	2	0	16	0	0	0
3.2.0.18	3	2	0	18	4416	4416	4416

Figura 5.37. Estadísticas conexiones ATM (SNMP)

192.168.0.14:vIPRouterTable

192.168.0.14 | Poll every 60 seconds | Mirror

Insta...	vIPRouterVLan...	vIPRouterProto...	vIPRouterNetAddr...	vIPRouterSubNetMask	vIPRouterBcastAddress	vIPRouterDescript...	vIPRouterAdmSta...	vIPRouterOperSta...
3	3	00.02 (hex)	192.168.0.14	255.255.255.252	192.168.0.15	Enlace Paraninfo SI	enable(2)	active(2)
10	10	00.02 (hex)	192.168.1.65	255.255.255.224	192.168.1.95	(zero-length)	enable(2)	active(2)
11	11	00.02 (hex)	192.168.2.65	255.255.255.224	192.168.2.95	(zero-length)	enable(2)	active(2)
12	12	00.02 (hex)	192.168.3.65	255.255.255.224	192.168.3.95	(zero-length)	enable(2)	active(2)

Figura 5.38. Routers virtuales (SNMP)

192.168.0.14:ipRouteTable

192.168.0.14 | Poll every 60 seconds | Mirror

Instance	ipRouteDest(IDX)	ipRouteIfIn...	ipRouteMetr...	ipRouteMetr...	ipRouteMetr...	ipRouteMetr...	ipRouteNext...	ipRouteT...
0.0.0.0	0.0.0.0	4	1	-1	-1	-1	192.168.0.13	indirect(4)
192.168.0.12	192.168.0.12	4	1	-1	-1	-1	192.168.0.14	direct(3)
192.168.1.64	192.168.1.64	3	1	-1	-1	-1	192.168.1.65	direct(3)
192.168.2.64	192.168.2.64	2	1	-1	-1	-1	192.168.2.65	direct(3)
192.168.3.64	192.168.3.64	1	1	-1	-1	-1	192.168.3.65	direct(3)

Figura 5.39. Tabla de rutas Paraninfo (SNMP)

192.168.0.14:vLanTable

192.168.0.14 | Poll every 60 seconds | Mirror

Insta...	vLanNumber(I...	vLanBridgeAddress	vLanDescription	vLanAdmStatus	vLanOperStatus	vLanMode	vLanFloodOverride	vLanMobileGroup	vLanAuthGr...	vLanStpStatus
1	1	00:20:DA:DE:42:12	Default GROUP (#1)	enable(2)	active(2)	standard(3)	-1	disabled(2)	disabled(2)	on(2)
2	2	00:00:00:00:00:00	Paraninfo	disable(1)	inactive(1)	standard(3)	-1	disabled(2)	disabled(2)	on(2)
3	3	00:20:DA:DE:42:10	Enlace Paraninfo-SI	enable(2)	active(2)	standard(3)	-1	disabled(2)	disabled(2)	on(2)
10	10	00:20:DA:DE:42:13	VLAN P	enable(2)	active(2)	standard(3)	-1	enabled(1)	disabled(2)	on(2)
11	11	00:20:DA:DE:42:14	VLAN A	enable(2)	active(2)	standard(3)	-1	enabled(1)	disabled(2)	on(2)
12	12	00:20:DA:DE:42:15	VLAN ALUMNOS	enable(2)	active(2)	standard(3)	-1	enabled(1)	disabled(2)	on(2)
99	99	00:20:DA:FF:88:9E	802.1Q	enable(2)	inactive(1)	standard(3)	999999999	disabled(2)	disabled(2)	on(2)

Figura 5.40. VLANs nodo Paraninfo (SNMP)

También se ha probado el funcionamiento de las sondas RMON. Estas sondas muestran estadísticas acerca de los paquetes enviados (número de paquetes, dirección destino broadcast, multicast…).

Para finalizar, se comprueba el funcionamiento de los traps que envía el agente al gestor cuando ocurre algún evento de los indicados a partir de la máscara que aparece en la figura 4.56. Por ejemplo, si se desconecta un enlace de la red troncal, el agente detecta la trap “Link down” y envía el mensaje de la figura 5.41 al gestor.

```
…
<pdu_type>v1_trap</pdu_type>/par
<v1_trap_agent_address>192.168.0.14</v1_trap_agent_address>/par
<v1_trap_generic_type name="linkDown">2</v1_trap_generic_type>/par
<v1_trap_specific_type>0</v1_trap_specific_type>/par
<v1_trap_time_stamp name="0 days
…
```

Figura 5.41. Trap “Link down” (SNMP)

Capítulo 6. Desarrollo de una práctica para laboratorio

En este apartado se propone un guión para una práctica de laboratorio que concentre las distintas partes explicadas en el presente documento y permita a los alumnos poner en práctica los conceptos adquiridos en la parte teórica de la asignatura de Redes Troncales. En este capítulo únicamente se redacta el guión de la parte de simulación, dejando relegada la parte correspondiente a medidas reales sobre la red al Anexo IV. La primera parte de la práctica se centra en el simulador de redes Cisco Packet Tracer y la segunda parte en la verificación de los resultados de simulación en el entorno real de los nodos de comunicaciones. Las tecnologías más relevantes con las que se trabaja en la práctica son ATM y VLAN.

6.1 Guión de la práctica

OBJETIVOS

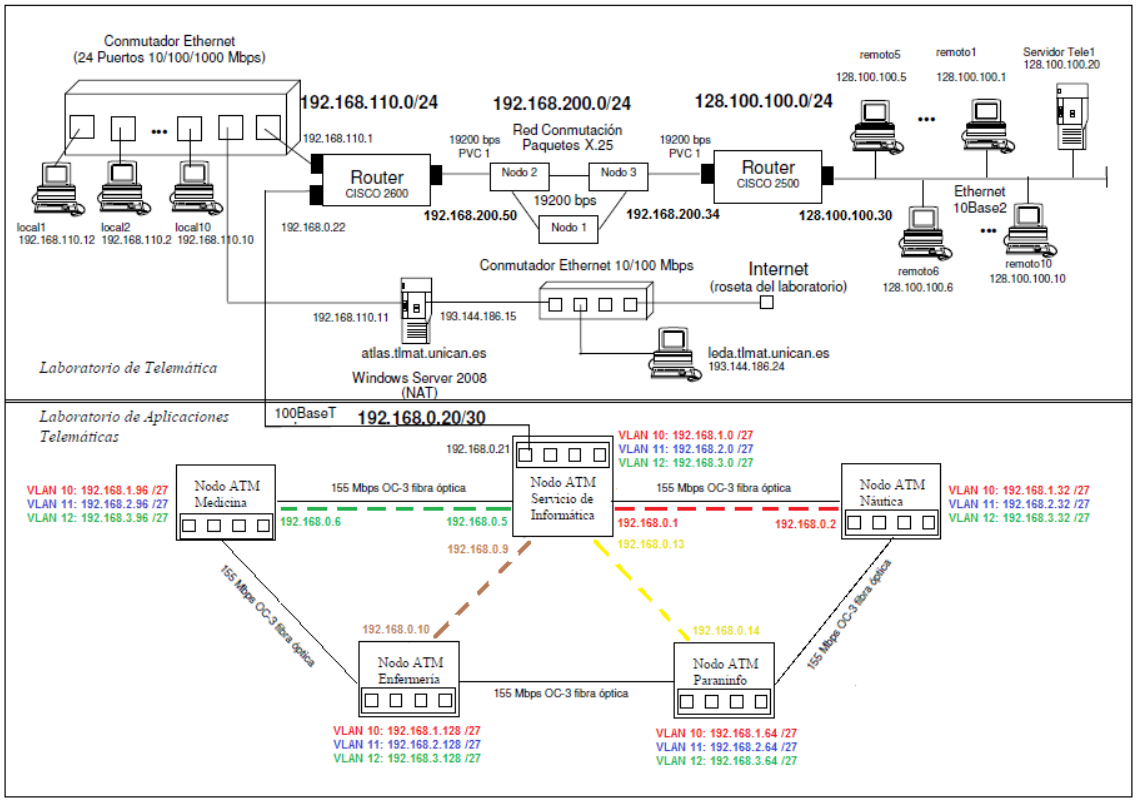
Esta práctica refuerza los conocimientos adquiridos por los alumnos en las clases de teoría acerca de las tecnologías de comunicaciones ATM y VLAN. Para ello, se van a realizar las siguientes acciones:

- Diseñar y configurar, mediante el simulador Packet Tracer de Cisco, la red de acceso Ethernet que se implementa sobre la red dorsal ATM del Laboratorio de Aplicaciones telemáticas.
- Observar los protocolos que participan en la comunicación y verificar el funcionamiento de las distintas VLANS configuradas en la red de acceso.
- Comprobar mediante la interfaz de usuario de los nodos las configuraciones de las VLANs y los servicios ATM definidos en los enlaces.
- Contrastar los resultados obtenidos en el simulador con los análisis realizados sobre el entorno real.
- Observar y capturar el tráfico ATM por la red dorsal.

INTRODUCCIÓN

La red sobre la que se desarrolla esta práctica está físicamente instalada en el Laboratorio de Aplicaciones Telemáticas y se integra dentro del conjunto de redes existentes en el Laboratorio de Telemática mediante una conexión directa entre la interfaz 5/1 del nodo SdeI (192.168.0.21) y el router Cisco2600 (192.168.0.22) que enlaza ambos laboratorios. Este hecho, unido a que el propio router y el servidor Atlas tienen configuradas en su tabla de rutas ciertas entradas de enrutamiento, posibilita que la red del Laboratorio de Aplicaciones Telemáticas se integre con el resto de redes existentes, y además presente una salida a Internet por la interfaz 192.168.110.11. En la parte dorsal de la red, los nodos forman un anillo físico mediante enlaces de fibra óptica a 155 Mbps sobre tecnología ATM. En esta parte de la red el tráfico entre nodos va sobre los circuitos ATM definidos. Los circuitos son de tipo SoftPVC, esto quiere decir que se crea un PVC entre el SdeI y el resto de nodos y que en el interior de la red se establecen circuitos SVC, lo que provoca que aunque la configuración física de

la red sea un anillo, la configuración lógica toma forma de estrella, con el nodo SdeI ejerciendo de nodo central de comunicaciones. Sobre estos circuitos, se define, por un lado, un servicio ATM punto a punto que transporta determinados circuitos de datos, y por otro, un servicio de Trunking ATM que transporta a través de la red dorsal las VLANs configuradas en los nodos. En la parte de acceso de usuario se utiliza tecnología Ethernet conmutada con cable de par trenzado a 100 Mbps. En esta parte de la red se definen 3 VLANs (10, 11, 12), en base a reglas de puertos y direccionamiento IP, que permiten establecer dominios de difusión independientes sin importar la localización de los usuarios en la red. El dimensionado completo de los Laboratorios de Telemática aparece en la siguiente figura:

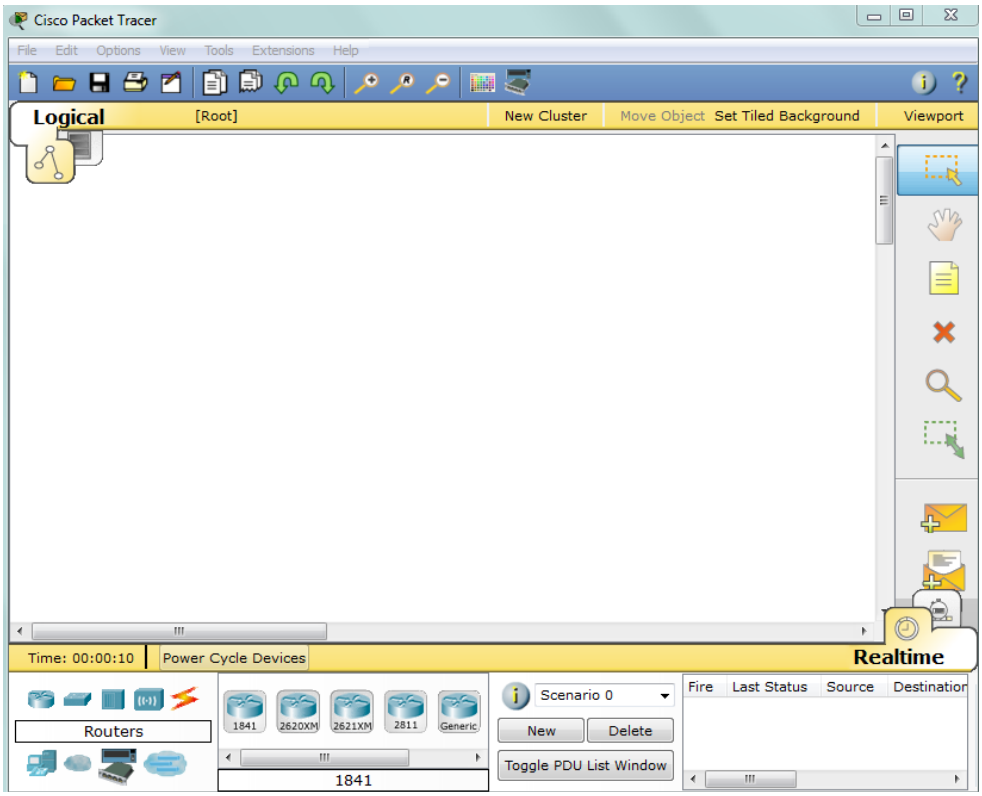


1 Diseño de la red de acceso mediante simulador Packet Tracer de Cisco

Para poder estudiar la red del Laboratorio de Aplicaciones Telemáticas se va a hacer uso del simulador de redes Packet Tracer, desarrollado por Cisco Systems, que permite recrear dicha red, analizar la configuración de la parte de acceso de usuarios y capturar los paquetes que se envían para analizar los protocolos en las distintas capas de la red.

1.1 Ejecutar el programa Cisco Packet Tracer 

Así, se accede a la interfaz gráfica mostrada a continuación:

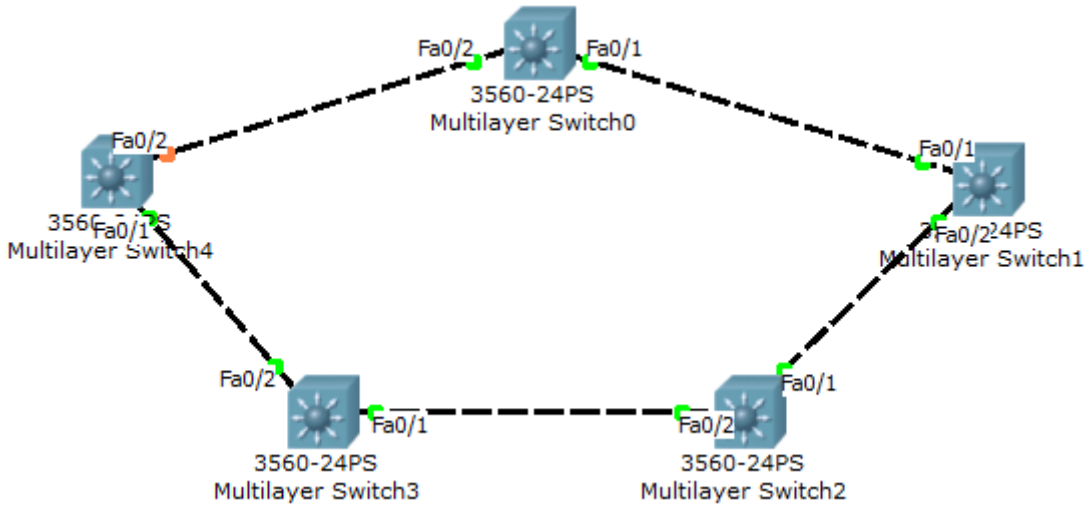


Para llevar a cabo el diseño de la red, es necesario seleccionar los dispositivos de comunicaciones que la forman. En la parte inferior izquierda, aparecen una serie de grupos con equipos y herramientas necesarios para el diseño de redes (*Routers, Switches, Hubs, Wireless Devices, Connections, End Devices, Wan Emulation, Custom Made Devices y Multiuser Connection*) entre los que se tendrá que realizar la selección anteriormente comentada.

Para simular los nodos existentes en el laboratorio, en el apartado Switches seleccionaremos el dispositivo 3560-24PS dado que se trata de un Switch multicapa con 24 puertos Fast Ethernet y 2 puertos Gigabit Ethernet que nos va a permitir enrutar entre las distintas VLANs que se configuren en la red.

1.2 Arrastrar 5 dispositivos al fondo principal y enlazarlos utilizando el cable "*Copper Cross-Over*" que aparece en el apartado *Connections*. Este cable se utiliza en este tipo de enlaces para cruzar los cables de transmisión de un extremo con los de recepción del otro.

1.3 Pinchar sobre un nodo, seleccionar Fa0/1 y lo unirlo con el nodo posterior en el anillo físico en su interfaz Fa0/1. Del mismo modo, uniremos éste último con el posterior utilizando las interfaces más bajas disponibles, creando una topología física como la que se muestra a continuación.



Para poder configurar la red, es necesario acceder a la interfaz de línea de comandos (CLI) de los nodos, e ir configurando en cada uno de ellos el direccionamiento y las propiedades de cada interfaz (*"trunk"* o *"access"*) adecuadamente según la figura de la red expuesta en el apartado introductorio.

1.4 Comenzar accediendo al nodo SdeI. Seleccionar *"CLI"*, y escribir *#enable* para entrar en el modo privilegiado. Después, seguir los pasos de configuración presentes para los nodos de SdeI, Náutica y Paraninfo y, posteriormente, configurar los nodos restantes del anillo (Enfermería y Medicina).

```
SDEI

RENOMBRAR NODO
Switch>enable
Switch#configure terminal
Switch(config)#hostname SdeI
SdeI(config)#exit

CREAR LAS VLANs
SdeI#vlan database
SdeI(vlan)#vlan 3 name VLAN_NAUTICA
SdeI(vlan)#vlan 4 name VLAN_MEDICINA
SdeI(vlan)#vlan 6 name VLAN_ENFERMERIA
SdeI(vlan)#vlan 7 name VLAN_PARANINFO
SdeI(vlan)#vlan 10 name VLAN_PDI
SdeI(vlan)#vlan 11 name VLAN_PAS
SdeI(vlan)#vlan 12 name VLAN_ALUMNOS
SdeI(vlan)#exit

DIRECCIONAR TODAS LAS INTERFACES
SdeI#configure terminal
SdeI(config)#interface vlan 3
SdeI(config-if)#ip address 192.168.0.1 255.255.255.252
SdeI(config-if)#no shutdown
SdeI(config-if)#end
SdeI(config)#interface vlan 4
SdeI(config-if)#ip address 192.168.0.5 255.255.255.252
SdeI(config-if)#no shutdown
SdeI(config-if)#exit
SdeI(config)#interface vlan 6
SdeI(config-if)#ip address 192.168.0.9 255.255.255.252
SdeI(config-if)#no shutdown
SdeI(config-if)#exit
SdeI(config)#interface vlan 7
SdeI(config-if)#ip address 192.168.0.13 255.255.255.252
SdeI(config-if)#no shutdown
SdeI(config-if)#exit
```

```
SdeI(config)#interface vlan 10
SdeI(config-if)#ip address 192.168.1.1 255.255.255.224
SdeI(config-if)#no shutdown
SdeI(config-if)#exit
SdeI(config)#interface vlan 11
SdeI(config-if)#ip address 192.168.2.1 255.255.255.224
SdeI(config-if)#no shutdown
SdeI(config-if)#exit
SdeI(config)#interface vlan 12
SdeI(config-if)#ip address 192.168.3.1 255.255.255.224
SdeI(config-if)#no shutdown
SdeI(config-if)#exit

HABILITAR EL TRUNK EN EL ENLACE TRONCAL (ENCAPSULACIÓN 802.1Q)
SdeI(config)#interface fa0/1
SdeI(config-if)#switchport trunk encapsulation dot1q
SdeI(config-if)#switchport trunk allowed vlan 1-99
SdeI(config-if)#switchport mode trunk
SdeI(config-if)#no shutdown
SdeI(config-if)#exit

CREAR ENTRADAS PARA LA TABLA DE RUTAS
SdeI(config)#ip route 192.168.1.32 255.255.255.224 192.168.0.2
SdeI(config)#ip route 192.168.2.32 255.255.255.224 192.168.0.2
SdeI(config)#ip route 192.168.3.32 255.255.255.224 192.168.0.2
SdeI(config)#ip route 192.168.1.96 255.255.255.224 192.168.0.6
SdeI(config)#ip route 192.168.2.96 255.255.255.224 192.168.0.6
SdeI(config)#ip route 192.168.3.96 255.255.255.224 192.168.0.6
SdeI(config)#ip route 192.168.1.128 255.255.255.224 192.168.0.10
SdeI(config)#ip route 192.168.2.128 255.255.255.224 192.168.0.10
SdeI(config)#ip route 192.168.3.128 255.255.255.224 192.168.0.10
SdeI(config)#ip route 192.168.1.64 255.255.255.224 192.168.0.14
SdeI(config)#ip route 192.168.2.64 255.255.255.224 192.168.0.14
SdeI(config)#ip route 192.168.3.64 255.255.255.224 192.168.0.14
SdeI(config)#exit
```

```
NAUTICA

RENOMBRAR NODO
Switch>enable
Switch#configure terminal
Switch(config)#hostname Nautica
Nautica(config)#exit

CREAR LAS VLANs (TODAS LAS QUE VAYAN A PASAR POR EL NODO)
Nautica(vlan)#vlan 3 name VLAN_NAUTICA
Nautica(vlan)#vlan 4 name VLAN_MEDICINA
Nautica(vlan)#vlan 6 name VLAN_ENFERMERIA
Nautica(vlan)#vlan 7 name VLAN_PARANINFO
Nautica(vlan)#vlan 10 name PDI
Nautica(vlan)#vlan 11 name PAS
Nautica(vlan)#vlan 12 name ALUMNOS
Nautica(vlan)#exit

DIRECCIONAR LAS INTERFACES (Y ACTIVAR LAS DE NODOS POSTERIORES)
Nautica(config)#interface vlan 3
Nautica(config-if)#ip address 192.168.0.2 255.255.255.252
Nautica(config-if)#no shutdown
Nautica(config-if)#exit
Nautica(config)#interface vlan 4
Nautica(config-if)#exit
Nautica(config)#interface vlan 6
Nautica(config-if)#exit
Nautica(config)#interface vlan 7
Nautica(config-if)#exit
Nautica(config)#interface vlan 10
Nautica(config-if)#ip address 192.168.1.33 255.255.255.224
Nautica(config-if)#no shutdown
Nautica(config-if)#exit
Nautica(config)#interface vlan 11
Nautica(config-if)#ip address 192.168.2.33 255.255.255.224
Nautica(config-if)#no shutdown
Nautica(config-if)#exit
Nautica(config)#interface vlan 12
```

```
Nautica(config-if)#ip address 192.168.3.33 255.255.255.224
Nautica(config-if)#no shutdown
Nautica(config-if)#exit

HABILITAR EL TRUNK EN LOS ENLACES TRONCALES (ENCAPSULACIÓN 802.1Q)
Nautica(config)#interface fa0/1
Nautica(config-if)#switchport trunk encapsulation dot1q
Nautica(config-if)#switchport trunk allowed vlan 1-99
Nautica(config-if)#switchport mode trunk
Nautica(config-if)#no shutdown
Nautica(config-if)#exit
Nautica(config)#interface fa0/2
Nautica(config-if)#switchport trunk encapsulation dot1q
Nautica(config-if)#switchport trunk allowed vlan 1-99
Nautica(config-if)#switchport mode trunk
Nautica(config-if)#no shutdown
Nautica(config-if)#exit

AÑADIR RUTA POR DEFECTO AL SDEI
Nautica(config)#ip route 0.0.0.0 0.0.0.0 192.168.0.1
Nautica(config)#exit
```

```
PARANINFO

RENOMBRAR NODO
Switch>enable
Switch#configure terminal
Switch(config)#hostname Paraninfo
Paraninfo(config)#exit

CREAR LAS VLANs (TODAS LAS QUE VAYAN A PASAR POR EL NODO)
Paraninfo(vlan)#vlan 4 name VLAN_MEDICINA
Paraninfo(vlan)#vlan 6 name VLAN_ENFERMERIA
Paraninfo(vlan)#vlan 7 name VLAN_PARANINFO
Paraninfo(vlan)#vlan 10 name VLAN_PDI
Paraninfo(vlan)#vlan 11 name VLAN_PAS
Paraninfo(vlan)#vlan 12 name VLAN_ALUMNOS
DIRECCIONAR LAS INTERFACES (Y ACTIVAR LAS DE NODOS POSTERIORES)
Paraninfo(config)#interface vlan 4
Paraninfo(config-if)#exit
Paraninfo(config)#interface vlan 6
Paraninfo(config-if)#exit
Paraninfo(config)#interface vlan 7
Paraninfo(config-if)#ip address 192.168.0.14 255.255.255.252
Paraninfo(config-if)#no shutdown
Paraninfo(config-if)#exit
Paraninfo(config)#interface vlan 10
Paraninfo(config-if)#ip address 192.168.1.65 255.255.255.224
Paraninfo(config-if)#no shutdown
Paraninfo(config-if)#exit
Paraninfo(config)#interface vlan 11
Paraninfo(config-if)#ip address 192.168.2.65 255.255.255.224
Paraninfo(config-if)#no shutdown
Paraninfo(config-if)#exit
Paraninfo(config)#interface vlan 12
Paraninfo(config-if)#ip address 192.168.3.65 255.255.255.224
Paraninfo(config-if)#no shutdown
Paraninfo(config-if)#exit
Paraninfo#configure terminal

HABILITAR EL TRUNK EN LOS ENLACES TRONCALES (ENCAPSULACIÓN 802.1Q)
Paraninfo(config)#interface fa0/1
Paraninfo(config-if)#switchport trunk encapsulation dot1q
Paraninfo(config-if)#switchport trunk allowed vlan 1-99
Paraninfo(config-if)#switchport mode trunk
Paraninfo(config-if)#no shutdown
Paraninfo(config-if)#exit
Paraninfo(config-if)#interface fa0/2
Paraninfo(config-if)#switchport trunk encapsulation dot1q
Paraninfo(config-if)#switchport trunk allowed vlan 1-99
Paraninfo(config-if)#switchport mode trunk
Paraninfo(config-if)#no shutdown
Paraninfo(config-if)#exit
```

```
AÑADIR RUTA POR DEFECTO AL SDEI
Paraninfo(config)#ip route 0.0.0.0 0.0.0.0 192.168.0.13
Paraninfo(config)#exit
```

```
ENFERMERIA

RENOMBRAR NODO
Switch>enable
Switch#configure terminal
Switch(config)#hostname Enfermeria
Enfermeria(config)#exit

CREAR LAS VLANs (TODAS LAS QUE VAYAN A PASAR POR EL NODO)
Enfermeria#vlan database
Enfermeria(vlan)#vlan 4 name VLAN_MEDICINA
Enfermeria(vlan)#vlan 6 name VLAN_ENFERMERIA
Enfermeria(vlan)#vlan 10 name VLAN_PDI
Enfermeria(vlan)#vlan 11 name VLAN_PAS
Enfermeria(vlan)#vlan 12 name VLAN_ALUMNOS
Enfermeria(vlan)#exit

DIRECCIONAR LAS INTERFACES (Y ACTIVAR LAS DE NODOS POSTERIORES)
Enfermeria#configure terminal
Enfermeria(config)#interface vlan 4
Enfermeria(config-if)#exit
Enfermeria(config)#interface vlan 6
Enfermeria(config-if)#ip address 192.168.0.10 255.255.255.252
Enfermeria(config-if)#no shutdown
Enfermeria(config-if)#exit
Enfermeria(config)#interface vlan 10
Enfermeria(config-if)#ip address 192.168.1.129 255.255.255.224
Enfermeria(config-if)#no shutdown
Enfermeria(config-if)#exit
Enfermeria(config)#interface vlan 11
Enfermeria(config-if)#ip address 192.168.2.129 255.255.255.224
Enfermeria(config-if)#no shutdown
Enfermeria(config-if)#exit
Enfermeria(config)#interface vlan 12
Enfermeria(config-if)#ip address 192.168.3.129 255.255.255.224
Enfermeria(config-if)#no shutdown
Enfermeria(config-if)#exit

HABILITAR EL TRUNK EN LOS ENLACES TRONCALES (ENCAPSULACIÓN 802.1Q)
Enfermeria(config)#interface fa0/1
Enfermeria(config-if)#switchport trunk encapsulation dot1q
Enfermeria(config-if)#switchport trunk allowed vlan 1-99
Enfermeria(config-if)#switchport mode trunk
Enfermeria(config-if)#no shutdown
Enfermeria(config-if)#exit
Enfermeria(config)#interface fa0/2
Enfermeria(config-if)#switchport trunk encapsulation dot1q
Enfermeria(config-if)#switchport trunk allowed vlan 1-99
Enfermeria(config-if)#switchport mode trunk
Enfermeria(config-if)#no shutdown
Enfermeria(config-if)#exit

AÑADIR RUTA POR DEFECTO AL SDEI
Enfermeria(config)#ip route 0.0.0.0 0.0.0.0 192.168.0.9
Enfermeria(config)#exit
```

```
MEDICINA

RENOMBRAR NODO
Switch>enable
Switch#configure terminal
Switch(config)#hostname Medicina
Medicina(config)#exit

CREAR LAS VLANs
Medicina#Medicina#vlan database
Medicina(vlan)#vlan 4 name VLAN_MEDICINA
Medicina(vlan)#vlan 10 name VLAN_PDI
```

```
Medicina(vlan)#vlan 11 name VLAN_PAS
Medicina(vlan)#vlan 12 name VLAN_ALUMNOS
Medicina(vlan)#exit

DIRECCIONAR LAS INTERFACES
Medicina#configure terminal
Medicina(config)#interface vlan 4
Medicina(config-if)#ip address 192.168.0.6 255.255.255.252
Medicina(config-if)#no shutdown
Medicina(config-if)#exit
Medicina(config)#interface vlan 10
Medicina(config-if)#ip address 192.168.1.97 255.255.255.224
Medicina(config-if)#no shutdown
Medicina(config-if)#exit
Medicina(config)#interface vlan 11
Medicina(config-if)#ip address 192.168.2.97 255.255.255.224
Medicina(config-if)#no shutdown
Medicina(config-if)#exit
Medicina(config)#interface vlan 12
Medicina(config-if)#ip address 192.168.3.97 255.255.255.224
Medicina(config-if)#no shutdown
Medicina(config-if)#exit

HABILITAR EL TRUNK EN EL ENLACE TRONCAL (ENCAPSULACIÓN 802.1Q)
Medicina(config)#interface fa0/1
Medicina(config-if)#switchport trunk encapsulation dot1q
Medicina(config-if)#switchport trunk allowed vlan 1-99
Medicina(config-if)#switchport mode trunk
Medicina(config-if)#no shutdown
Medicina(config-if)#exit

AÑADIR RUTA POR DEFECTO AL SDEI
Medicina(config)#ip route 0.0.0.0 0.0.0.0 192.168.0.5
Medicina(config)#exit
```

2 Comprobación del funcionamiento de la red (parte de acceso de usuario) según los resultados de la simulación.

Una vez configurada la red, se realizan las pruebas de funcionamiento apropiadas para comprobar que todo funciona según lo esperado.

2.1 Acceder a la línea de comandos (CLI) del nodo SdeI y escribir *#enable*.

2.2 Consultar qué VLANs hay creadas mediante el comando *#show vlan brief*.

```
SdeI#show vlan brief
VLAN Name                Status              Ports
---- ----------------  ---------  -------------------------------
1    default             active      Fa0/2, Fa0/3, Fa0/4, Fa0/5 Fa0/6,
                                     Fa0/7, Fa0/8, Fa0/9 Fa0/10,
                                     Fa0/11, Fa0/12, Fa0/13, Fa0/14,
                                     Fa0/15, Fa0/16, Fa0/17, Fa0/18,
                                     Fa0/19, Fa0/20, Fa0/21, Fa0/22,
                                     Fa0/23, Fa0/24, Gig0/1, Gig0/2.

3    VLAN_NAUTICA        active
4    VLAN_MEDICINA       active
6    VLAN_ENFERMERIA     active
7    VLAN_PARANINFO      active
10   VLAN_PDI            active
11   VLAN_PAS            active
12   VLAN_ALUMNOS        active
1002 fddi-default        active
1003 token-ring-default  active
1004 fddinet-default     active
1005 trnet-default       active
```

2.3 Visualizar la información del protocolo Spanning Tree ejecutando el comando *#show spanning-tree*.

```
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0005.5E89.8EDA
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     0005.5E89.8EDA
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
-------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p

VLAN0003
  Spanning tree enabled protocol ieee
  Root ID     Priority    32771
              Address     0005.5E89.8EDA
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32771  (priority 32768 sys-id-ext 3)
              Address     0005.5E89.8EDA
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
-------
Fa0/1            Desg FWD 19        128.1    P2p

.....
```

a) ¿Qué variante del protocolo Spanning Tree se está ejecutando en la red?

(MSTP, cada VLAN ejecuta el STP de forma independiente y selecciona su bridge raíz.)

b) ¿Qué criterio se sigue para establecer el bridge raíz?

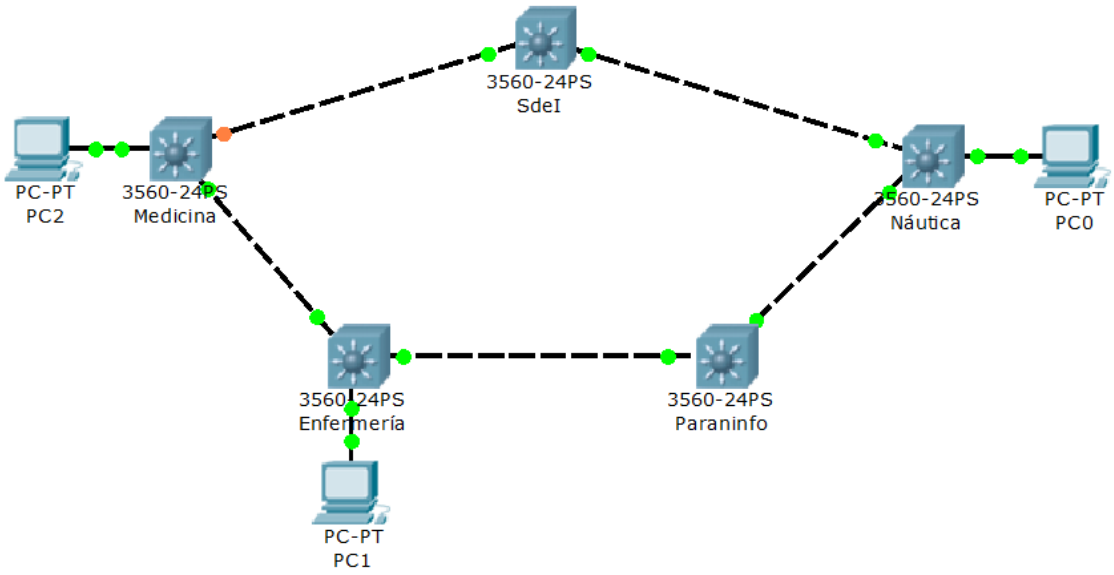
(Cada VLAN envía BPDUs para establecer el switch raíz que se asigna al que tiene el ID más bajo. El ID tiene en cuenta los campos: Brige Priority, que por defecto es 32768, el ID de la VLAN y la dirección MAC del Switch).

2.4 Comprobar que interfaces tienen habilitado el trunking y qué tipo de encapsulamiento está establecido mediante el comando *#show interface trunk*.

```
SdeI#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking           1

Port        Vlans allowed on trunk
Fa0/1       1-99

Port        Vlans allowed and active in management domain
Fa0/1       1,3,4,6,7,10,11,12

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,3,4,6,7,10,11,12
```

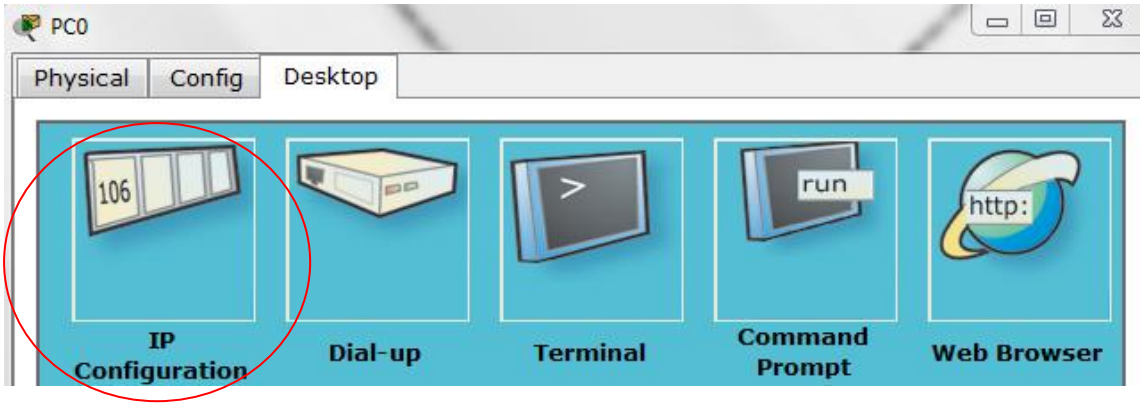
Llegados a este punto, vamos a configurar 3 PC conectándolos a distintos nodos para verificar el funcionamiento de las VLANs. Los terminales se seleccionan en el apartado de End Devices.

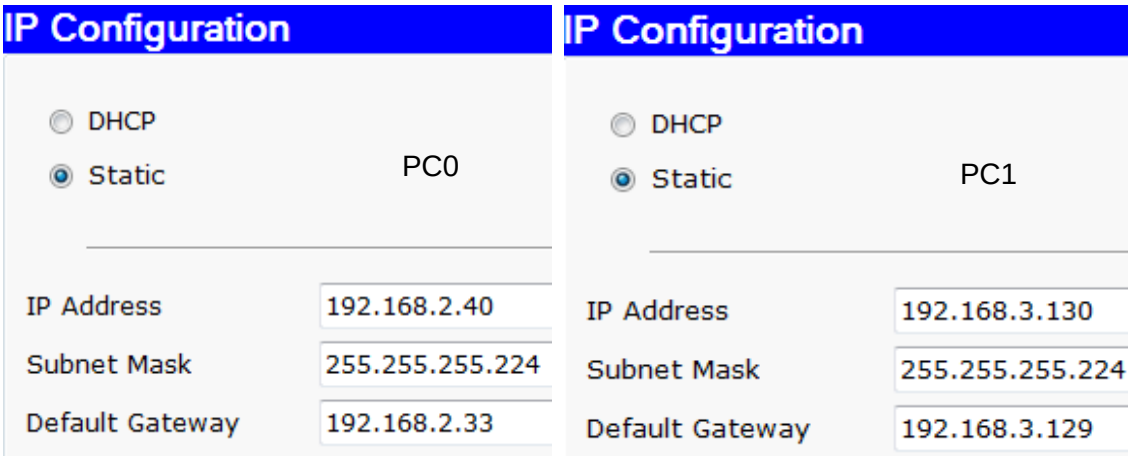
2.5 Conectar los equipos a los nodos utilizando el cable “Copper Straight-Through”, habitual en redes de área local. Conectaremos un PC (interfaz Fast Ethernet) a la interfaz Fa0/3 de Náutica, otro PC a la interfaz Fa0/3 de Enfermería y otro PC a la interfaz Fa0/3 de Medicina.

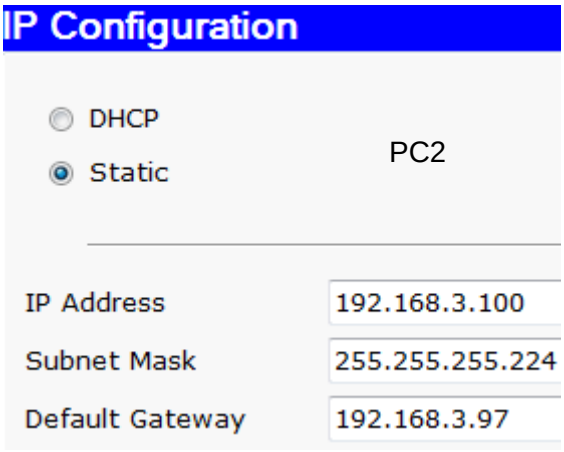


Vamos a configurar los PCs con el siguiente direccionamiento: PC0 en la VLAN 11 de Náutica (192.168.2.40 /27), PC1 en la VLAN 12 de Enfermería (192.168.3.130 /27) y PC2 en la VLAN 12 de Medicina (192.168.3.100).

2.6 Haciendo doble clic sobre un terminal, accedemos a la ventana que posibilita su configuración. Seleccionamos Desktop y entramos en “IP Configuration” para configurar el direccionamiento de los equipos.







2.7 Acceder al nodo de Náutica y habilitar el modo privilegiado ejecutando *#enable*. Posteriormente acceder al modo de configuración global y configurar la interfaz Fa0/3:

```
PC0

Nautica>enable
Nautica#configure terminal
Nautica(config)#interface fa0/3
Nautica(config-if)#switchport mode access
Nautica(config-if)#switchport access vlan 11
Nautica(config-if)#no shutdown
Nautica(config-if)#exit
Nautica(config)#exit
```

Hacer lo mismo para los otros 2 nodos.

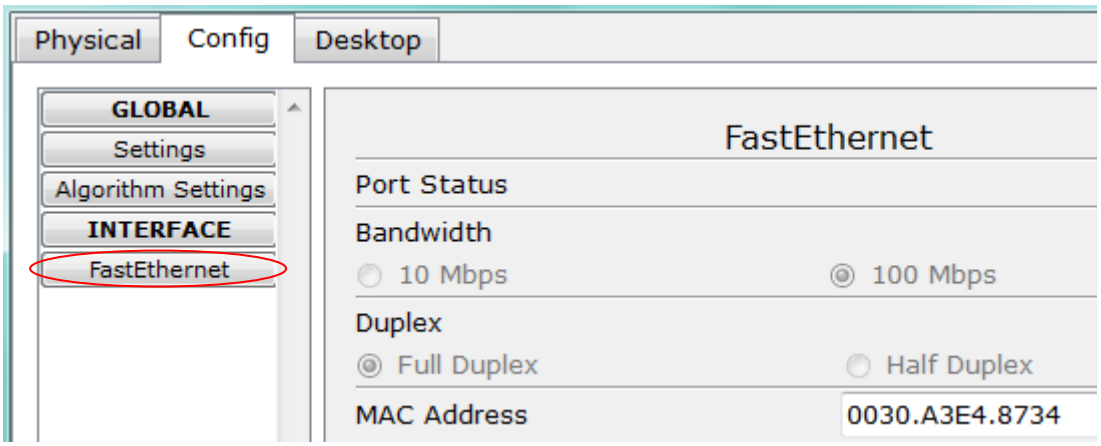
```
PC1

Enfermeria>enable
Enfermeria#configure terminal
Enfermeria(config)#interface fa0/3
Enfermeria(config-if)#switchport mode access
Enfermeria(config-if)#switchport access vlan 12
Enfermeria(config-if)#no shutdown
Enfermeria(config-if)#exit
Enfermeria(config)#exit
```

```
PC2

Medicina>enable
Medicina#configure terminal
Medicina(config)#interface fa0/3
Medicina(config-if)#switchport mode access
Medicina(config-if)#switchport access vlan 12
Medicina(config-if)#no shutdown
Medicina(config-if)#exit
Medicina(config)#exit
```

2.8 Comprobar haciendo un ping desde el símbolo del sistema *"Command Prompt"* del PC de Medicina a los otros 2 que existe conectividad en la red.

```
PC>ping 192.168.2.40
Pinging 192.168.2.40 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Reply from 192.168.2.40: bytes=32 time=138ms TTL=125
Ping statistics for 192.168.2.40:
    Packets: Sent = 4, Received = 1, Lost = 3 (75% loss),
Approximate round trip times in milli-seconds:
    Minimum = 138ms, Maximum = 138ms, Average = 138ms

PC>ping 192.168.3.130
Pinging 192.168.3.130 with 32 bytes of data:
Request timed out.
Request timed out.
Reply from 192.168.3.130: bytes=32 time=250ms TTL=125
Reply from 192.168.3.130: bytes=32 time=265ms TTL=125
Ping statistics for 192.168.3.130:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
Approximate round trip times in milli-seconds:
    Minimum = 250ms, Maximum = 265ms, Average = 257ms
```

2.9 Anotar la dirección MAC de los switches SdeI, Náutica, Enfermería y Medicina ejecutando *#show versión* y la de los PCs configurados anteriormente accediendo al menú *"Config"* y seleccionando *"Fast Ethernet"*.




```
SdeI>enable
SdeI#show version
Base ethernet MAC Address: 0005.5E89.8EDA
Nautica>enable
Nautica#show version
Base ethernet MAC Address : 00E0.A322.CD05
Enfermeria>enable
Enfermeria#show version
Base ethernet MAC Address : 00E0.8F19.7757
```

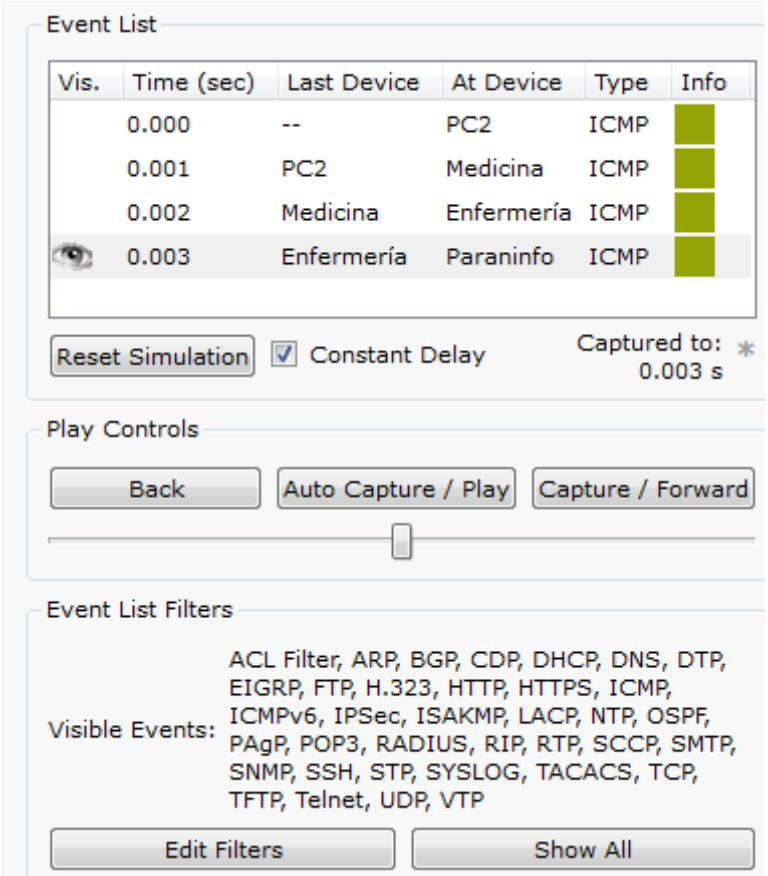
```
Medicina>enable
Medicina#show version
Base ethernet MAC Address : 00E0.8F80.0AD9
PC0 MAC Address: 0001.6436.9AC2
PC1 MAC Address: 0060.4737.85CA
PC2 MAC Address: 0030.A3E4.8734
```

Para analizar los protocolos que intervienen en la comunicación, el simulador incorpora la opción de hacer que los paquetes sean visibles en todos los puntos de la red. En la parte inferior derecha aparecen 2 iconos como los que se muestran a continuación:

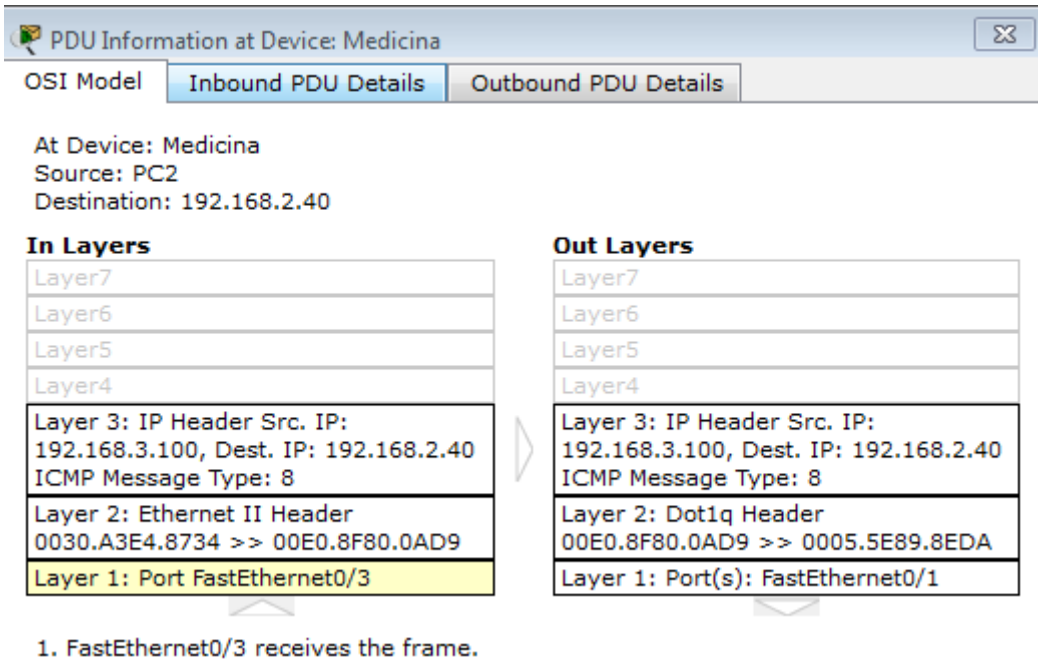
El icono de la izquierda indica simulación en tiempo real.

El icono de la derecha indica modo simulación.

A la hora de capturar los protocolos, aparece la siguiente ventana en la que va apareciendo cada transición de los mensajes dentro de la red y, pinchando cada uno de ellos, podemos ver las distintas capas que los conforman.



Por ejemplo, si analizamos el segundo mensaje de la ventana anterior, nos aparecen los protocolos (según la capa del modelo OSI en la que se integran) que intervienen en el mensaje.



Si cambiamos de pestaña, veremos con más detalle la PDU entrante y la PDU saliente.

2.10 Analizar los paquetes ARP e ICMP que aparecen al ejecutar los ping anteriores. (Tras entrar en *Simulation* volvemos a ejecutar los ping anteriores y analizamos los mensajes ARP e ICMP).

c) ¿Qué saltos tiene que dar el mensaje ICMP para llegar al nodo de Náutica?

```
Medicina → Enfermería → Paraninfo → Náutica → SdeI → Náutica
```

2.11 Realizar un *tracert* de PC2 a PC0 y PC1 y analizar los resultados obtenidos.

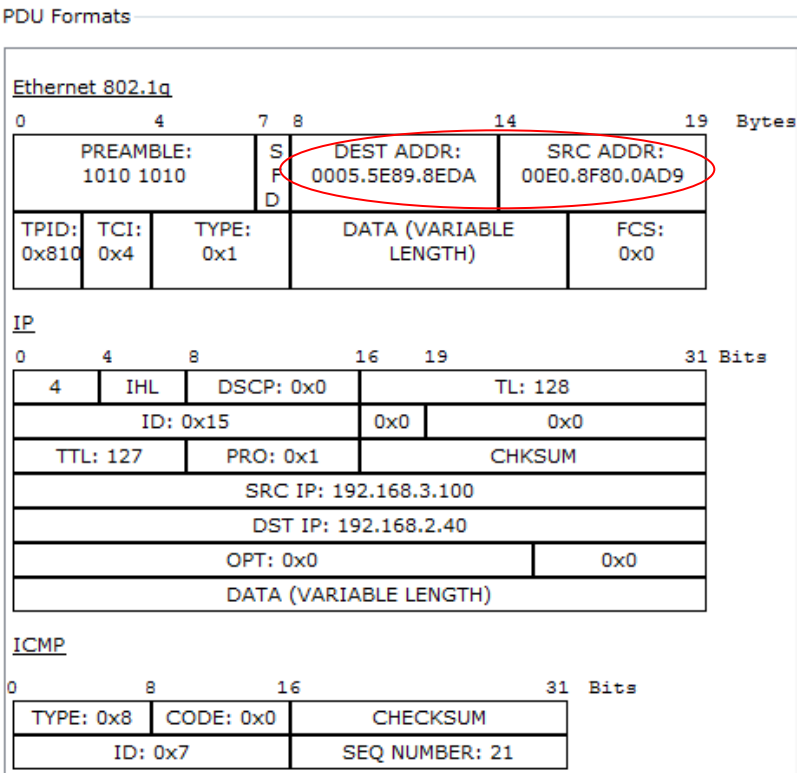
```
PC>tracert 192.168.2.40
Tracing route to 192.168.2.40 over a maximum of 30 hops:
  1   31 ms    31 ms    31 ms   192.168.3.97 (Router VLAN12 Medicina)
  2   140 ms   156 ms   140 ms  192.168.0.5  (Interfaz SdeI-Medicina)
  3   156 ms   156 ms   187 ms  192.168.0.2  (Interfaz Náutica-SdeI)
  4   203 ms   141 ms   203 ms  192.168.2.40 (PC0)
Trace complete.

PC>tracert 192.168.3.130
Tracing route to 192.168.3.130 over a maximum of 30 hops:
  1   32 ms    18 ms    31 ms   192.168.3.97 (Router VLAN12 Medicina)
  2   156 ms   156 ms   96 ms   192.168.0.5  (Interfaz SdeI-Medicina)
  3   187 ms   234 ms   218 ms  192.168.0.10 (Interfaz Enfermería-SdeI)
  4   219 ms   281 ms   250 ms  192.168.3.130 (PC1)
Trace complete.
```

d) ¿Están los equipos en la misma VLAN? ¿Por qué?

Los equipos están en distintas VLANs. Aunque haya 2 equipos que tengan configurada una VLAN 12, cada VLAN debe corresponder a una subred única y una vez que el paquete es enrutado (se puede ver en el traceroute) significa que se cambia de VLAN. Si analizamos un ICMP de Medicina a Enfermería por el enlace de trunk, vemos como la MAC origen se corresponde con la MAC del nodo Medicina y la MAC

destino se corresponde con la MAC del nodo SdeI (que enviará el paquete al destino original de Náutica).

En Ethernet 802.1q el TPID (Tag Protocol ID) es 0x8100 (por eso es 802.1q) y el TCI (Tag Control Information) indica que la VLAN a la que corresponde el mensaje es la 4, definida en el enlace Sdei – Medicina. Como la dirección destino es la de un equipo de Náutica, el mensaje irá al SdeI a través identificado con esta VLAN, y desde el SdeI a Náutica, irá identificado con la VLAN propia del enlace SdeI – Náutica (VLAN 3).



2.12 Cambiar ahora el direccionamiento del PC de Enfermería. Volver a entrar en *"IP Configuration"* de PC1 y configurar:

```
Dirección IP. . . . . . . . . . . . : 192.168.3.110
Máscara de subred . . . . . . . . . : 255.255.255.224
Puerta de enlace predeterminada     : 192.168.3.97
```

2.13 Entrar de nuevo en *Simulation* y volver a analizar los paquetes ARP e ICMP que aparecen tras ejecutar los ping desde PC0.

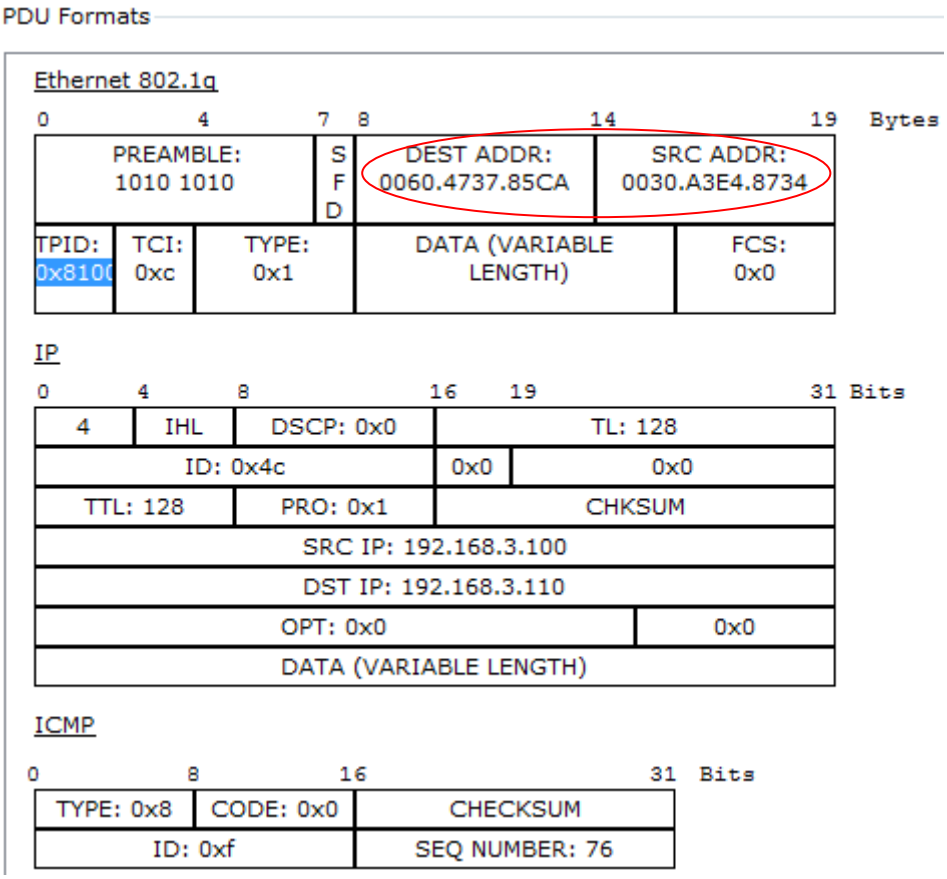
2.14 Realizar un *tracert* de PC2 a PC0 y PC1 y analizar los resultados obtenidos.

```
PC>tracert 192.168.2.40
Tracing route to 192.168.2.40 over a maximum of 30 hops:
  1   31 ms    16 ms    31 ms    192.168.3.97 (Router VLAN12 Medicina)
  2   109 ms   156 ms   140 ms   192.168.0.5  (Interfaz SdeI-Medicina)
  3   172 ms   187 ms   187 ms   192.168.0.2  (Interfaz Náutica-SdeI)
  4   218 ms   156 ms   203 ms   192.168.2.40 (PC0)
Trace complete.
PC>tracert 192.168.3.110
Tracing route to 192.168.3.110 over a maximum of 30 hops:
```

```
  1   124 ms    34 ms     78 ms     192.168.3.110 (PC1)
Trace complete.
```

e) ¿Están los equipos en la misma VLAN? ¿Por qué?

En esta ocasión, los equipos PC1 y PC2 si que están configurados en la misma VLAN. Aparte de que en el traceroute se observa que con un salto (sin enrutar) se llega al equipo, si analizamos el mismo mensaje que en la ocasión anterior en el enlace troncal de Medicina y Enfermería, vemos como las MACs origen y destino se corresponden con las de los PCs, indicando que se encuentran en la misma subred.

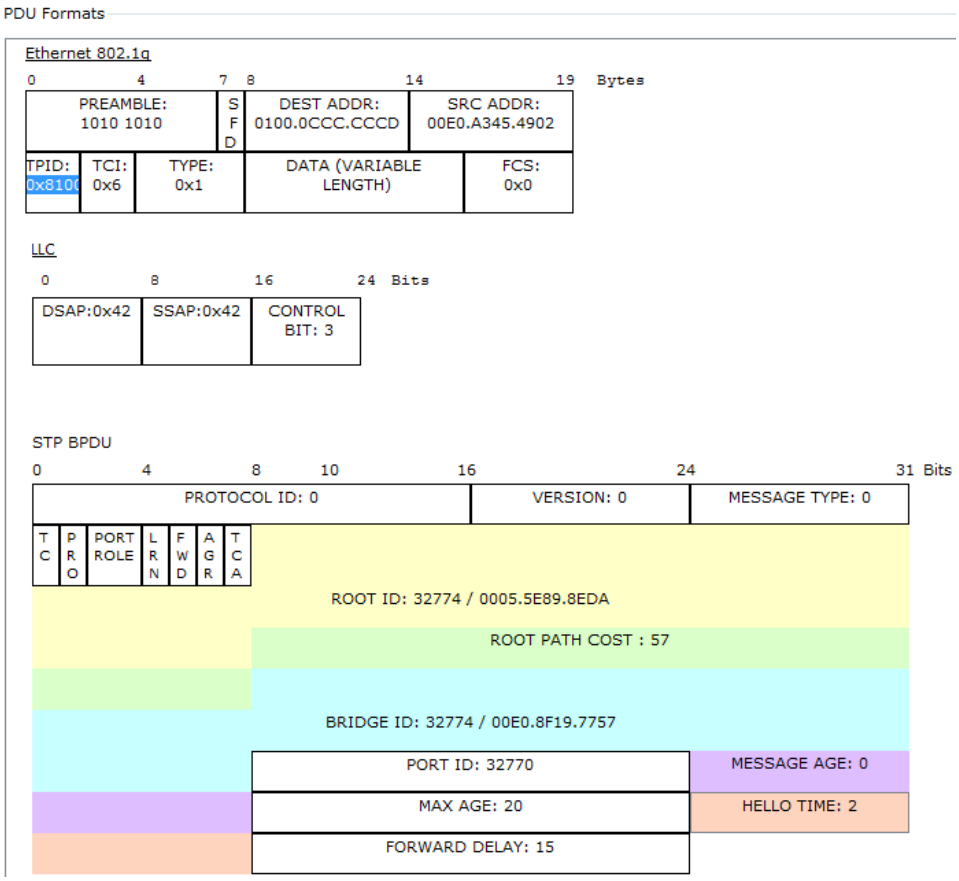


En Ethernet 802.1q el TPID (Tag Protocol ID) es 0x8100 (por eso es 802.1q) y el TCI (Tag Control Information) indica que la VLAN a la que corresponde el mensaje es la 12 (0xc), hecho que confirma que ambos equipos se encuentran en la misma VLAN.

2.15 Analizar también una trama Spanning-Tree por los enlaces de trunk.

f) ¿Cómo se encapsula la trama?

El protocolo Spanning-Tree se encapsula en LLC con los valores DSAP y SSAP igual a 0x42.



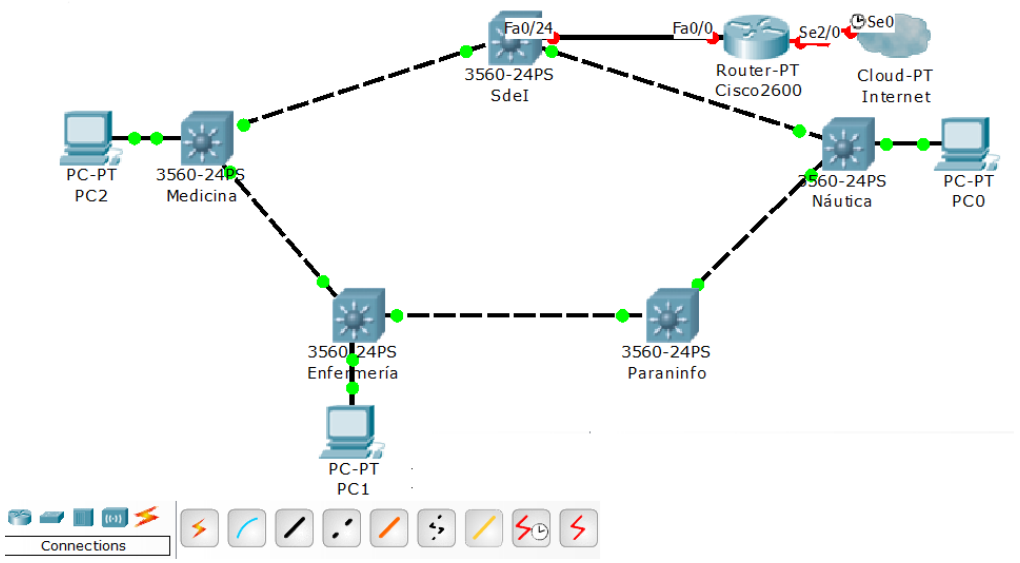
2.16 Comprobar que existe una ruta (en el SdeI) para enviar paquetes a otras redes (por ejemplo, hacer un ping desde PC0 a 192.168.110.11).

```
PC>ping 192.168.110.11
Pinging 192.168.110.11 with 32 bytes of data:
Reply from 192.168.0.1: Destination host unreachable.
Reply from 192.168.0.1: Destination host unreachable.
Reply from 192.168.0.1: Destination host unreachable.
Reply from 192.168.0.1: Destination host unreachable.
Ping statistics for 192.168.110.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

2.17 Mediante el comando *#show ip route*, verificar en el SdeI si existe una ruta por defecto, en caso contrario, crearla de la siguiente forma.

No existe una ruta por defecto, por lo que hay que configurarla y hacer que cualquier paquete que llegue sea respondido (simular Internet).

Seleccionar un Router Genérico que simulará al Router Cisco2600 del Laboratorio de Telemática. Unir mediante el cable “Copper Straight-Through” la interfaz fa0/24 del SdeI con la interfaz fa0/0 del router. Posteriormente seleccionar de *“WAN Emulation”* una nube (*“Cloud-PT”*) y conectarla por la interfaz Serial0 (mediante una conexión serie) a la interfaz Serial2/0 del Router Cisco2600.



Configuración Cisco2600 y SdeI:

```
CISCO2600

Router>enable
Router#configure terminal
Router(config)#hostname Cisco2600
Cisco2600(config)#interface fa0/0
Cisco2600(config-if)#ip address 192.168.0.22 255.255.255.252
Cisco2600(config-if)#no shutdown
Cisco2600(config-if)#exit
Cisco2600(config)#ip route 192.168.1.0 255.255.255.0 192.168.0.21
Cisco2600(config)#ip route 192.168.2.0 255.255.255.0 192.168.0.21
Cisco2600(config)#ip route 192.168.3.0 255.255.255.0 192.168.0.21
Cisco2600(config)#exit
```

```
SDEI

SdeI>enable
SdeI#vlan database
SdeI(vlan)#vlan 8 name VLAN_CISCO2600
SdeI(vlan)#exit
SdeI#configure terminal
SdeI(config)#interface vlan 8
SdeI(config-if)#ip address 192.168.0.21 255.255.255.252
SdeI(config-if)#no shutdown
SdeI(config-if)#exit
SdeI(config)#interface fa0/24
SdeI(config-if)#switchport mode access
SdeI(config-if)#switchport access vlan 8
SdeI(config-if)#no shutdown
SdeI(config-if)#exit
SdeI(config)#ip route 0.0.0.0 0.0.0.0 192.168.0.22
SdeI(config)#exit
```

2.18 Volver a realizar el ping desde PC0 a 192.168.110.11 y comprobar que la configuración se ha realizado correctamente.

```
PC>ping 192.168.110.11
Pinging 192.168.110.11 with 32 bytes of data:
Request timed out.
Request timed out.
Reply from 192.168.0.22: Destination host unreachable.
Reply from 192.168.0.22: Destination host unreachable.
Ping statistics for 192.168.110.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)
```

Aunque salga *Destination host unreachable*, la red está bien configurada, puesto que el mensaje sale del anillo físico al router Cisco2600, que tendría una entrada por defecto a Atlas (192.168.110.11). Atlas enrutaría el mensaje hacia Internet o, en este caso, respondería al ping.

OPCIONALES

1- Cambiar la configuración de la red de tal forma que los mensajes con destino Náutica o Paraninfo salgan por la interfaz fa0/1 del SdeI y los mensajes con destino Medicina o Enfermería salgan por la interfaz fa0/2 del SdeI.

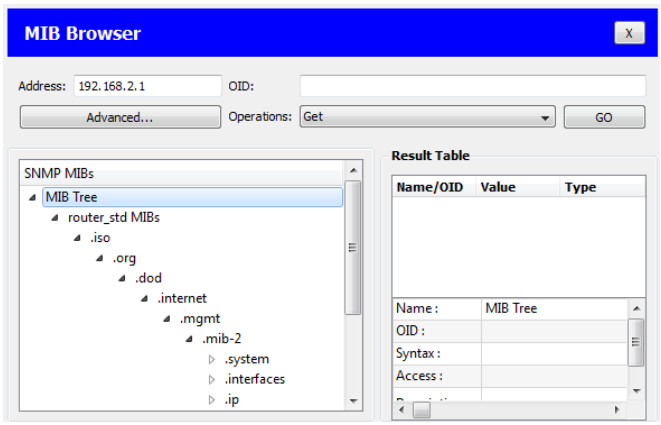
2- Habilitar la gestión SNMP en el nodo SdeI y analizar un mensaje GetRequest.

Conectar un equipo Gestor al nodo SdeI (interfaz fa0/3) y configurar el nodo SdeI y el equipo gestor:

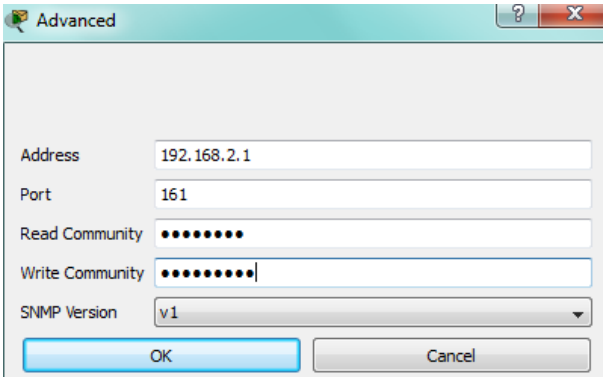
```
SdeI>enable
SdeI#configure terminal
SdeI(config)#snmp-server community solomira ro
SdeI(config)#snmp-server community miramucho rw
SdeI(config)#exit

EQUIPO GESTOR
SdeI(config)#interface fa0/3
SdeI(config-if)#switchport mode access
SdeI(config-if)#switchport access vlan 11
SdeI(config-if)#no shutdown
SdeI(config-if)#exit
```

```
EQUIPO GESTOR

Dirección IP. . . . . . . . . . . : 192.168.2.5
Máscara de subred . . . . . . . . : 255.255.255.224
Puerta de enlace predeterminada   : 192.168.2.1
```

Acceder al software *MIB Browser* integrado en el *Desktop* del PC (Debajo de la interfaz de línea de comandos)



Entrar en *Advanced* y configurar: La dirección del agente, el puerto por el que se envían las peticiones SNMP al agente, las comunidades de lectura y escritura y la versión del protocolo SNMP.



Por ejemplo, seleccionar .interfaces – if.Number y ver el mensaje enviado hacia el agente 192.168.2.1 del nodo SdeI.

g) ¿Qué protocolo de transporte utiliza SNMP?

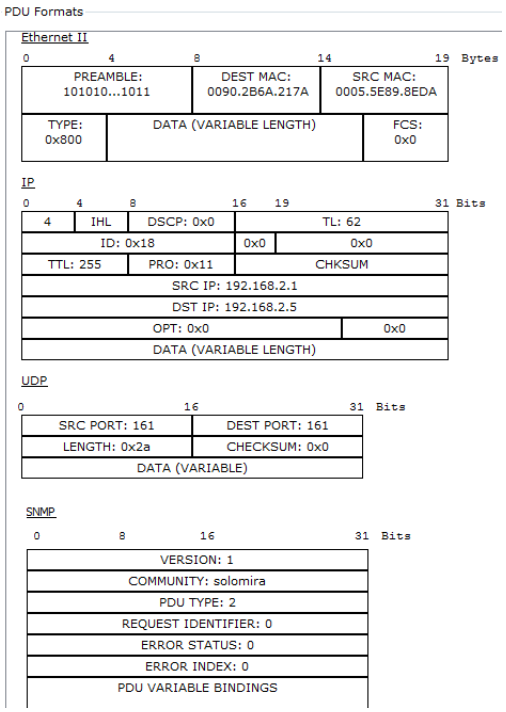
El protocolo UDP, el mensaje se envía por el puerto 161 (puerto en el que escuchan los agentes).

h) ¿Cuál es el resultado de la petición? Interpretarlo

Result Table

Name/OID	Value	Type
.1.3.6.1.2.1.2.1.0 (.iso.org.dod.internet.mgmt.mib-2.interfaces.ifNumber.0)	35	Integer

El número de interfaces del SdeI (independientemente de si están activas o no). Son las interfaces fa0/1-fa0/24, ge0/1-ge0/2, VLANs: 1,3, 4, 6, 7, 8, 10, 11 y 12.



Capítulo 7. Conclusiones y líneas futuras

La elaboración de este proyecto ha supuesto la configuración de los 5 nodos trocales Alcatel que aparecen en el Anexo y su correspondiente red de acceso, así como la elaboración de unas prácticas de laboratorio que permitan a los estudiantes poner en práctica los conocimientos teóricos recogidos en la asignatura de Redes Troncales.

En el proceso de configuración, se ha establecido, por una parte, la red troncal (comunicación entre los nodos) basada en tecnología ATM y, por otra, la red de acceso de usuario (comunicación nodos – usuarios) basada en tecnología VLAN Ethernet, ejerciendo los nodos como conmutadores entre las tramas procedentes de Ethernet y las celdas propias de la tecnología ATM. En la red troncal, el tráfico de usuarios se transporta sobre los servicios ATM definidos en los nodos, y las celdas son encaminadas siguiendo las tablas de enrutamiento establecidas. En la red de acceso, se ha comprobado que gracias a las VLANs configuradas se pueden establecer dominios de difusión independientes sin importar a que nodo estén conectados los usuarios de la red. La integración de esta red dentro del conjunto de redes existentes en el Laboratorio de Telemática se ha llevado a cabo enlazando el nodo SdeI y una interfaz disponible del router Cisco2600 del Laboratorio de Telemática y añadiendo las rutas necesarias en el router Cisco2600 y el Servidor Atlas para posibilitar la comunicación entre redes y dar salida a Internet al Laboratorio de Aplicaciones Telemáticas.

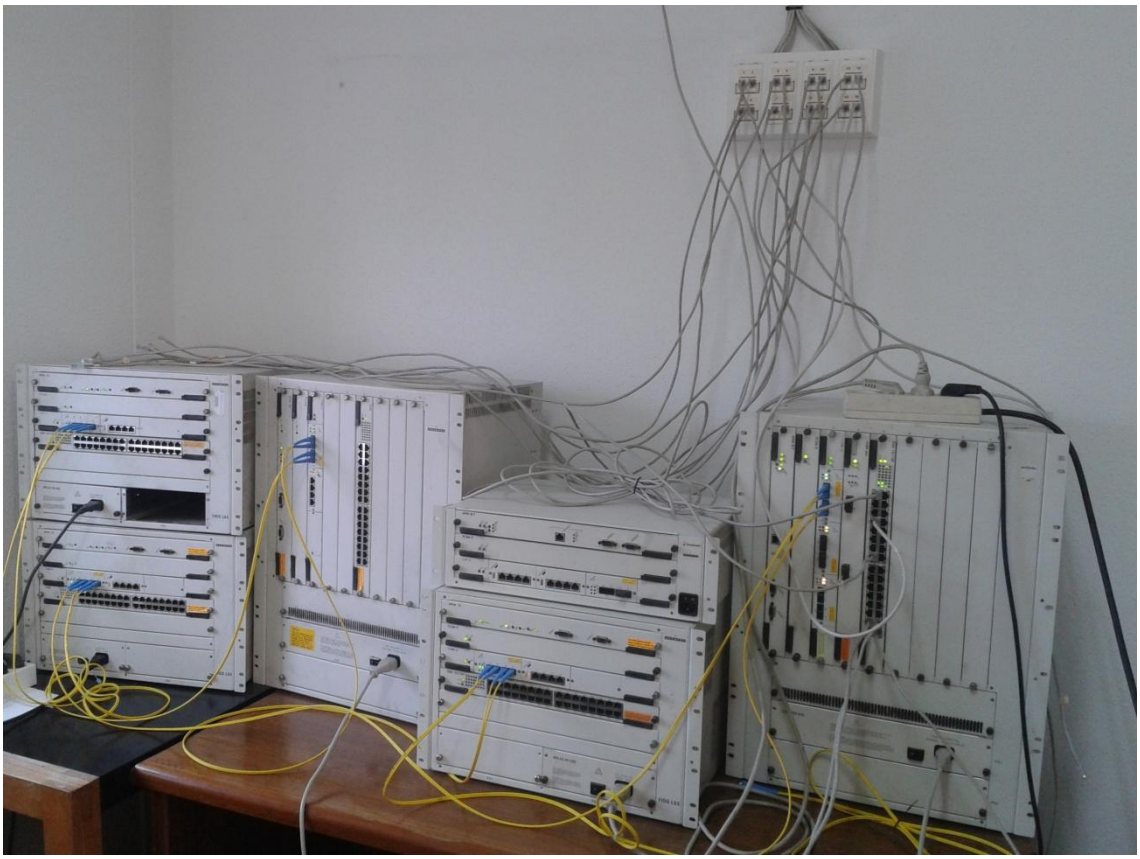
Tras finalizar el proceso de configuración, se ha comprobado el correcto funcionamiento de la red empleando diferentes analizadores de protocolos y contrastando los resultados con la parte teórica explicada en el Capítulo 3 del proyecto y con los resultados obtenidos en la implementación de la red de acceso a usuario en el simulador Cisco Packet Tracer.

Por último se ha redactado un guión para la impartición de una práctica de laboratorio enfocada para alumnos de Redes Troncales, asignatura impartida en el 4º curso de los estudios de Grado en Ingeniería de Tecnologías de Telecomunicación.

Por ello, puede decirse que los objetivos planteados al inicio se han visto cumplidos.

De cara al futuro, se plantea la migración de los nodos Alcatel actuales por otros de nueva generación dado que el Servicio de Informática ha cedido al Grupo de Ingeniería Telemática los equipos JUNIPER M120 (Multiservice Edge Router) tras haber sido reemplazados en la red troncal de la universidad. Estos equipos presentan un software más moderno y mejores prestaciones en cuanto a capacidad y velocidad en la comunicación. El M120 es una plataforma altamente redundante de 120 Gbps, perfecta para admitir aplicaciones de enrutamiento periférico convergentes de ancho de banda elevado. Esta plataforma utilizar tecnología Gigabit Ethernet tanto en la red de acceso como en la red dorsal, permitiendo realizar ingeniería de tráfico y diferenciar perfiles de calidad de servicio gracias a la tecnología MPLS sobre IP. Otra de las ventajas de estos nuevos nodos es que presenta una interfaz de configuración más evolucionada y más sencilla que facilita la gestión de la red [29].

Anexo I. Imagen nodos Alcatel



Anexo II. Hojas de características de los equipos

OmniS/R-5 Technical Specifications	
Total Module Slots	5
Total Slots for Switching Modules	4
Physical Dimensions	12.25" (31.12 cm) high, 17.14" (43.54 cm) wide, 13" (33.02 cm) deep
Weight	approximately 55 lb. (24.09 kg), fully populated with modules and power supplies.
Switching Backplane	Up to 12 Gbps (aggregate) switching fabric capacity
Voltage Range	90-265 VAC, 47 to 63 Hz auto-ranging and auto-sensing.
Current Draw	6 Amps at 100/115 VAC; 3 Amps at 230 VAC
Watts (Output)	375
Current Provided	60 Amps at 5 Volts (V1) 5 Amps at 12 Volts (V2) 3 Amps at 3.3 Volts (V3) 5.1 Amps at 1.5 Volts (V4)
Temperature Operating Range	0 to 45 degrees Celsius 32 to 113 degrees Fahrenheit
Humidity	Relative humidity operating range from 0 to 95 percent non-condensing.
Altitude	Sea level to 10,000 feet (3 km)
Heat Generation	1280 BTUs per hour (one power supply)
Agency Listings	UL 1950; CSA-C22.2; EN60950; FCC Part 15, Subpart B (Class A); EN55022, 1987/EN50081; FCC Class B; C.I.S.P.R. 22: 1985; EN50082-1, 1992; IEC 801-2, 1991; IEC 801-3, 1984; IEC 801-4, 1988

OmniS/R-9 Technical Specifications	
Total Module Slots	9
Total Slots for Switching Modules	8
Physical Dimensions	24.50" (62.23 cm) high, 16.60" (42.16 cm) wide, 13.25" (36.66 cm) deep
Weight	96 lb. (43.55 kg), fully populated with modules and power supplies.
Switching Backplane	Up to 22 Gbps (aggregate) switching fabric capacity
Voltage Range	90-264 VAC, 47 to 63 Hz
Current Draw	12 Amps at 100/115 VAC; 6 Amps at 230 VAC
Watts (Output)	650
Current Provided	120 Amps at 5 Volts 4 Amps at 12 Volts 6 Amps at 3.3 Volts 8 Amps at 1.5 Volts
Temperature Operating Range	0 to 45 degrees Celsius 32 to 113 degrees Fahrenheit
Humidity	Relative humidity operating range from 0 to 95 percent non-condensing
Altitude	Sea level to 10,000 feet (3 km)
Heat Generation	2219 BTUs per hour (one power supply)
Agency Listings	UL 1950; CSA-C22.2; EN60950; EN55022, 1987/EN50081; C.I.S.P.R. 22: 1985; EN50082-1, 1992; IEC 801-2, 1991; IEC 801-3, 1984; IEC 801-4, 1988; VCCI V-3/94.04 (Class 1); FCC Part 15, Subpart B (Class A); FCC Class B

CSM-AB-155F Technical Specifications	
Number of ports	2 SONET/SDH
Connector Type	SC
Standards Supported	ATM Forum User-to-Network Interface 4.0, 3.1, and 3.0 ITU-T I.432 and G.957 ANSI T1.105 Bellcore TR-NWT-000253 ATM Forum Traffic Management 4.0 Private Network-to-Network Interface (PNNI) 1.0 Interim Interswitch Protocol (IISP)
Data Rate	155 Mbps
Virtual Circuits Supported	4096 point-to-point per port; 2048 point-to-multipoint per CSM-155
Cell Buffer Size	8192 per port
Connections Supported	OC-3c/STM-1 connections to ATM stations, backbones.
Optical output power	Multimode: -19 to -14 dBm Single mode intermediate reach: -15 to -8 dBm Single mode long reach: -5 to 0 dBm
Optical receiver sensitivity	Multimode: -30 to -14 dBm Single mode intermediate reach: -31 to -8 dBm Single mode long reach: -34 to -10 dBm
Cable Supported	Multimode: 62.5 micron multimode fiber Single mode intermediate reach: intermediate-reach single-mode fiber Single mode long reach: long-reach single-mode fiber
Cable Distance	Multimode: 4 km Single mode intermediate reach: 24 km Single mode long reach: 40 km

CSM-AB-DS1/E1 Technical Specifications	
Number of ports	4 DS1 (T1) or E1
Connector Type	RJ-48C
Standards Supported	RFC 1406
Frame Formats	DS1: Superframe, Extended Superframe, Unframed E1: E1, E1-CRC, E1-MF, E1-CRC-MF, Unframed
Line Type	DS1: B8ZS or AMI E1: HDB3 or AMI
Data Rates Supported	DS1: 1.544 Mbps E1: 2.048 Mbps
Facility Datalink Protocol	ANSI T1.403 and AT&T 54016
Connections Supported	Physical Data Terminal Equipment (DTE) or Data Communication Equipment (DCE)
Cable Distance	DS1/E1 (short haul): 200 meters DS1/E1 (long haul): 1829 meters

ESM-100C-32W Technical Specifications	
Ports	(32) 10BaseT/100BaseTx Ethernet ports
Connector Type	RJ-45
Standards Supported	IEEE 802.3; IAB RFCs 826, 894, IEEE 10BaseT, 100BaseTx
Data Rate	10 or 100 Mbps (auto-sensing)
Maximum Frame Size	1,518 bytes
MAC Addresses Supported	1,024 (2,048 with CAM upgrade option)
Connections Supported	10BaseT hub or device; 100BaseTx hub or device
Cables Supported	Unshielded twisted-pair (UTP)—100 ohms (Category 5, EIA/TIA 568); Shielded twisted-pair (STP)—100 ohms (Category 5)
Current Draw	5.75 amps
Cable Distance	100 m

FCSM II Technical Specifications	
Standards Supported	ATM Forum User-to-Network Interface 4.0, 3.1, and 3.0 ISO Q.2931 ATM LAN Emulation Client V1.0 ITU-T I.432 and G.957 Bellcore TR-NWT-000253 Private Network-to-Network Interface (PNNI) 1.0 Interim Interswitch Protocol (IISP)
Data Rate	Up to 500 Mbps
Maximum Frame Size	8,000 bytes (ASM half)

Anexo III. Ejemplo fichero de configuración final

Fichero de configuración final correspondiente al nodo de Paraninfo:

```
! Version "4.1.3 GA"
! chassis type "9-slot 1100 LSS - Series 500"


!
! CHASSIS SLOT INFO
slot  1  "MPM 1G"
slot  2  "FCSM"
slot  3  "CSM_U"
slot  4  "Empty"
slot  5  "Empty"
slot  6  "ESM 100C 32"
slot  7  "Empty"
slot  8  "Empty"
slot  9  "Empty"


!
!System
! system date 01/27/2015
! system time 09:56:13
system timezone 1:00
system daylight savings start last sunday in march at 2:00
system daylight savings end last sunday in october at 3:00
system description "Nodo ATM Paraninfo"
system admin-contact "Jose Angel Irastorza"
system location "V-Pino"
system name Paraninfo

! VLAN group/VLAN info:
group 1 no router ip
group 2
group 2 description "Paraninfo"
group 3
group 3 router ip 192.168.0.14 255.255.255.252 192.168.0.15 inactive
group 3 description "Enlace Paraninfo-SI"
group 10
group 10 mobility on
group 10 router ip 192.168.1.65 255.255.255.224 192.168.1.95
group 10 description "VLAN PDI"
group 11
group 11 mobility on
group 11 router ip 192.168.2.65 255.255.255.224 192.168.2.95
group 11 description "VLAN PAS"
group 12
group 12 mobility on
group 12 router ip 192.168.3.65 255.255.255.224 192.168.3.95
group 12 description "VLAN ALUMNOS"
group 99
group 99 description "802.1Q"
! VLAN group/VLAN qgp info
group 10 802.1q 6/15 multi 10 0 "Vlan 10"
group 11 802.1q 6/15 multi 11 0 "Vlan 11"
group 12 802.1q 6/15 multi 12 0 "Vlan 12"
! VLAN group/VLAN stp info
! VLAN group/vlan rules info:

!
!HRE-X Filtering

!
!IP
!
! IP static routes
ip route 0.0.0.0          0.0.0.0          192.168.0.13

!
!IPX
```

```
! ATM Services:
atm service 2/1 "PTOP Bridging Service 1" PTOP 3    201
atm service 2/1 "PTOP Bridging Service 1" encapsulation RFC1483
atm service 2/1 "Trunking Service 2" TRUNKING 10  403
atm service 2/1 "Trunking Service 2" member 11
atm service 2/1 "Trunking Service 2" member 1
atm service 2/1 "Trunking Service 2" member 12
no default lane service 2/1

! ATM Connection:
atm connection 2/1 201   maximum tx frame size 2048
atm connection 2/1 201   maximum rx frame size 2048
atm connection 2/1 403   maximum tx frame size 2048
atm connection 2/1 403   maximum rx frame size 2048

! ATM Port:
atm port 2/1  tx SAR buffer 2048
atm port 2/1  rx SAR buffer 2048
atm port 2/1  tx frame buffer 4600
atm port 2/1  rx frame buffer 4600


! CSM Port:
csm port 2/1 ilmi polling ENABLE
csm port 2/1 auto configuration ENABLE
csm port 2/2 auto configuration ENABLE
csm port 3/1 interface type PNNI
csm port 3/2 interface type PNNI
csm port 3/3 ilmi DISABLE
csm port 3/4 ilmi DISABLE
csm port 3/5 ilmi DISABLE
csm port 3/6 ilmi DISABLE

! CSM SPVC:
csm spvc 3/3 0   289  3903488001bc900001014e4a0000d09500008002 0   289
csm spvc 3/3 0   289  transport priority CBR
csm spvc 3/3 0   289  pcr Clp01 tx 5991
csm spvc 3/3 0   289  aal5 discard status DISABLE
csm spvc 3/3 0   289  cell delay variation 10000
csm spvc 3/3 0   289  broadband bearer traffic CBR
csm spvc 3/3 0   289  broadband bearer timing end to end
csm spvc 3/3 0   289  broadband bearer clipping OFF

! PNNI configuration:

! PNNI Node:
pnni node  changes apply DISABLE
pnni node  changes apply ENABLE

! PNNI:
pnni  changes apply DISABLE
pnni  changes apply ENABLE

! PNNI Port:

! PNNI Route properties:

! PNNI Routes:
! VLAN interfaces info:
group 10 interface 6/3
group 10 interface 6/4
group 10 interface 6/5
group 10 interface 6/6
group 11 interface 6/7
group 11 interface 6/8
group 11 interface 6/9
group 11 interface 6/10
group 12 interface 6/11
group 12 interface 6/12
group 12 interface 6/13
group 12 interface 6/14
group 99 interface 6/15
group 99 vport 6/15 flood limit 0
group 10 vport 6/15 description "Vlan 10"
group 10 vport 6/15 bridge mode bridged
group 10 vport 6/15 flood limit 0
```

```
group 11 vport 6/15 description "Vlan 11"
group 11 vport 6/15 bridge mode bridged
group 11 vport 6/15 flood limit 0
group 12 vport 6/15 description "Vlan 12"
group 12 vport 6/15 bridge mode bridged
group 12 vport 6/15 flood limit 0

! 10/100 Interface info:

! Slip info:

!
!Bridging
bridge 11 6/8 path cost 10
bridge 99 flood limit   99

! SNMP General info:
!snmp community read-only ********
!snmp community read-write *********
snmp trap unicast
! SNMP Traps info:
snmp station 192.168.4.3 8000000d:2000f c:0 on 162 on



!
! Configuration dump successful for: atm bridging filter interface ip ipx
snmp system vlan
```

Anexo IV. Práctica (Trabajo en el laboratorio)

A continuación se expone la parte del guión de la práctica correspondiente al trabajo en el laboratorio, que no se incluye con la parte de simulación debido a que las pruebas que se hacen en el laboratorio son las mismas que en el Capítulo 5.

3. Comprobación del funcionamiento de la red (parte dorsal y parte de acceso de usuario) con herramientas y aplicaciones de comunicaciones.

Para comprobar el funcionamiento de la red en el entorno real, se va a hacer uso de las herramientas de comunicaciones LAN Advisor y ATM Advisor, del analizador de protocolos Wireshark, y de la propia interfaz de usuario que incorporan los nodos.

Para acceder a la interfaz de configuración de los nodos tenemos la opción de conectar directamente un PC mediante cable RS-232 a la interfaz serie (Console) que incorporan los equipos en su módulo de gestión o hacer un telnet desde el *cmd* a cualquier interfaz con dirección IP configurada en el nodo. Tal y como se ha visto en el apartado de simulación estas interfaces son:

SdeI

192.168.0.1 – 192.168.0.5 – 192.168.0.9 – 192.168.0.13 – 192.168.0.21 – 192.168.1.1 – 192.168.2.1 y 192.168.3.1.

Náutica

192.168.0.2 – 192.168.1.33 – 192.168.2.33 y 192.168.3.33.

Paraninfo

192.168.0.14 – 192.168.1.65 – 192.168.2.65 y 192.168.3.65.

Enfermería

192.168.0.10 – 192.168.1.129 – 192.168.2.129 y 192.168.3.129.

Medicina

192.168.0.6 – 192.168.1.97 -192.168.2.97 y 192.168.3.97.

Además al nodo SdeI se puede acceder conectando un PC mediante un cable RJ-45 a una interfaz Ethernet disponible en su módulo de gestión. El PC tiene que estar configurado en la red 192.168.11.0 /24.

3.1 Conectarse al nodo SdeI mediante una de las opciones anteriores (Máximo 2 usuarios vía telnet, 1 usuario por conexión serie y 1 usuario por cable Ethernet)

Una vez hemos accedido, el sistema requiere usuario y contraseña. Accederemos con usuario: Alumnos Telematica y contraseña: telematica.

En el menú principal se muestran los menús de configuración disponibles, dentro de cada uno de ellos encontraremos comandos para visualizar diferentes estadísticas o configuraciones del nodo. Como se explicó en el apartado introductorio, sobre las conexiones virtuales que transitan por la red se definen una serie de servicios ATM punto a punto y de Trunking.

3.2 Ejecutar el comando *"vas"*.

(Para ver los servicios ATM configurados, ver figura 4.34)

3.3 Ejecutar el comando *"vvc"*.

(Para ver las conmutaciones de los circuitos al pasar de los módulos internos a las interfaces de salida, ver figura 4.35)

3.4 Ejecutar el comando *"gp"*.

(Para ver las VLANs configuradas en el nodo y su direccionamiento, ver figuras 4.39 y 4.49)

3.5 Ejecutar el comando *"ipr"*.

(Para ver la tabla de rutas del nodo, ver figura 4.51)

3.6 Ejecutar los comandos *"vcs"* y *"vls"* para comprobar que existe tráfico ATM por la red e identificar los circuitos que se vieron al ejecutar *"vas"*.

(Para el caso del nodo de Enfermería los comandos aparecen en 5.7 y 5.8)

ATM Advisor

En este punto vamos a analizar el tráfico que pasa a través de la red dorsal (como celdas ATM) utilizando el analizador ATM Advisor.

Conectar los 2 pares de cables de fibra óptica del slot 3 del SdeI a los puertos 1 y 2 del analizador (asegurarse que Tx-Rx y Rx-Tx). Ejecutar el programa Agilent Advisor – ATM Analysis – ATM Launch Current Interface y configurar Run mode: Monitor y Framing: STS-3c.

3.7 Empezar a capturar y observar los mensajes que aparecen en el analizador. Localizar mensajes correspondientes a los circuitos de gestión y señalización.

0/5 (ver figura 5.14), 0/16 (ver figura 5.15) y 0/18 (ver figura 5.16).

3.8 Localizar también mensajes correspondientes a servicios punto a punto y a servicios de trunking.

(ver figuras 5.10 y 5.11)

i) ¿Qué tamaño tienen las celdas ATM? ¿Qué diferencia significativa hay entre las capturas de los 2 tipos de servicios ATM?
   Celdas de 53 Bytes (5 de cabecera y 48 de datos)
   Ambos mensajes utilizan una PDU de AAL5 para transportar el protocolo de capa superior (BPDUs de STP), pero los servicios punto a punto tienen definida

la encapsulación RFC1483 con LLC/SNAP, mientras que los servicios de trunking se encapsulan directamente en la PDU de AAL5.

OPCIONAL

Generar un ping desde el analizador y observar el mensaje que contiene IP sobre ATM

(ver figura 5.17)

VLANs

Para analizar la red de acceso de usuario, vamos a realizar las mismas pruebas que en el apartado de simulación. Las VLANs se establecen en el laboratorio en base a puertos y direccionamiento IP. El direccionamiento ya es conocido por el apartado de simulación (también aparece en la figura de la red de telemática), pero los puertos asignados a cada VLAN en los distintos nodos aparecen en la siguiente figura.

(Ver figura 4.55)

3.9 Conectar un PC del laboratorio a la VLAN 11 de Náutica (puertos 7, 8, 9 y10), otro a la VLAN 12 de Enfermería (puertos 11, 12, 13 y 14) y otro a la VLAN 12 de Medicina (puertos 11, 12, 13 y 14) y configurarles de la siguiente forma: (Ver figura 5.18)

3.10 Ejecutar Wireshark en los 3 equipos y enviar un ping desde el PC de Medicina a cada equipo. Analizar los mensajes ARP e ICMP que aparecen.

(Ver figuras 5.19, 5.20 y 5.21)

3.11 Ejecutar un *traceroute* desde el PC de Medicina a los otros 2 equipos.

(Ver figura 5.22)

j) ¿Están los equipos en la misma VLAN? ¿Por qué?

No, misma respuesta que la pregunta d).

3.12 Cambiar el direccionamiento del PC de Enfermería para que, aunque esté conectado a este nodo, tenga el direccionamiento de la VLAN de Medicina:

(Ver figura 5.23)

3.13 Ejecutar Wireshark en los 3 equipos y enviar un ping desde el PC de Medicina a cada equipo. Analizar los mensajes ARP e ICMP que aparecen.

(Ver figuras 5.24, 5.25 y 5.26)

3.14 Ejecutar un *traceroute* desde el PC de Medicina a los otros 2 equipos.

(Ver figura 5.27)

k) ¿Están los equipos en la misma VLAN? ¿Por qué?

PC de Medicina y PC de Enfermería si, misma respuesta que la pregunta e).

LAN ADVISOR

Para finalizar la práctica, vamos a analizar las tramas que aparecen en el puerto de trunking configurado en los nodos (puerto 15) utilizando LAN Advisor. Para capturar con este analizador debe accederse a: Agilent Advisor – LAN Analysis – Ethernet undercradle y configurar el analizador en modo internal AUI. Debe conectarse por cable Ethernet el PC al puerto "To Hub / Switch" del analizador.

3.15 Poner a capturar el analizador y ejecutar un ping desde el PC de Medicina a la dirección 192.168.3.127 (broadcast de subred).

3.16 Analizar las tramas BPDUs y el mensaje ICMP que aparece tras la ejecución del ping anterior.

(Ver figuras 5.29 y 5.30)

OPCIONAL

- Establecer un equipo del laboratorio como gestor de red direccionándole correctamente según la configuración de SNMP del nodo SdeI, que se puede consultar ejecutando el comando *"snmpc"*. Ejecutar el software MIB Browser y acceder a SNMP Protocol Preferences para configurar los parámetros SNMP. (Ver figuras 4.56 y 5.32)

- Analizar las estadísticas de gestión SNMP en el nodo SdeI.

Bibliografía y Referencias

[1] Página Web Servicio de Informática de la UC: https://sdei.unican.es

[2] Documentación facilitada por el Servicio de Informática de la UC.

[3] Manual de usuario de los equipos OmniSwitch de Alcatel.

[4] Apuntes de la asignatura Redes y Servicios Telemáticos, Universidad de Cantabria.

[5] ATM (Asyncronous Transfer Mode): http://www.ramonmillan.com/tutoriales/atm.php

[6] Multiprotocol encapsulation over AAL5: https://tools.ietf.org/html/rfc1483

[7] Redes convergentes ATM-IP: *www.uv.es/~montanan/iir/iir99.ppt*

[8] IP sobre ATM: http://www.rediris.es/difusion/publicaciones/boletin/53/enfoque1.html

[9] ATM: https://www.tlm.unavarra.es/~daniel/docencia/arss_itt/arss_itt12_13/slides/Tema3-6-ATM.pdf

[10] ATM Signaling Support for IP over ATM: https://tools.ietf.org/html/rfc1755

[11] Understanding ILMI on ATM Interfaces: http://www.cisco.com/c/en/us/support/docs/asynchronous-transfer-mode-atm/atm-signaling/10449-ilmi.html

[12] PNNI Overview: http://www.cisco.com/c/en/us/td/docs/switches/wan/mgx/ses/software/ses_pnni_controller/r1-0-11/reference/guide/pnni_con/overvw.html

[13] Apuntes de la asignatura Transmisión de Datos, Universidad de Cantabria.

[14] Understanding and Configuring STP: http://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/5234-5.html

[15] VLANs: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/vlans.html

[16] VLAN: *www.suarezdefigueroa.es/manuel/PAR/TEMAS/VLAN.doc*

[17] Marina Smith: *"Virtual LANs: A Guide to Construction, Operation and Utilization"*. Mc Graw Hill Computer Communications Series, 1997.

[18] How Bridging of VLAN Traffic Works: http://www.juniper.net/documentation/en_US/junos13.2/topics/concept/bridging-ex-series-understanding.html

[19] Proxy ARP: http://www.cisco.com/cisco/web/support/LA/102/1025/1025364_5.html

[20] Conceptos básicos DHCP: https://support.microsoft.com/es-es/kb/169289

[21] DHCP: https://www.ietf.org/rfc/rfc2131.txt

[22] Apuntes de la asignatura Gestión de Red, Universidad de Cantabria.

[23] LAN Advisor: http://www.keysight.com/en/pd-32661-pn-J3446E/agilent-advisor-lan-fast-ethernet?cc=ES&lc=eng

[24] ATM Advisor: http://www.keysight.com/en/pd-31012-pn-J2300E/agilent-advisor-wan?cc=ES&lc=eng

[25] Wireshark: https://www.wireshark.org/about.html

[26] MG-SOFT MIB Browser: http://www.mg-soft.si/mgMibBrowserPE.html

[27] Packet Tracer: https://www.netacad.com/es/web/about-us/cisco-packet-tracer

[28] Manual de usuario del programa MIB Browser, MG-SOFT.

[29] M120 Multiservice Edge Router: http://www.juniper.net/us/en/products-services/routing/m-series/m120/]