Diseño y Administración de Redes

Práctica 3.1

Diseño y Gestión de Tecnologías LANC

Dpto. Ingeniería Electrónica y Comunicaciones
Área de Ingeniería Telemática

Departamento de
Ingeniería Electrónica
y Comunicaciones
Universidad Zaragoza

Autores:
Profesores del área de Ingeniería Telemática

1. Introducción

1.1. Objetivos

Tras la realización de esta práctica, el alumno deberá ser capaz de:
-Configurar y monitorizar equipos basados en tecnología LAN Conmutada
-Administrar o gestionar características propias de LANC como son las tablas de conmutación o la creación de LAN virtuales.

1.2. Contenidos

Los objetivos propuestos en esta práctica pretenden afianzar y complementar los **contenidos teóricos vistos en clase**. Por lo tanto, será necesario un estudio previo de los mismos, así como la utilización de los apuntes de clase (y cualquier material adicional que el alumno considere oportuno) como apoyo a la realización práctica.

A modo de orientación se enumeran aquellos aspectos de LAN Conmutadas que se consideran más relevantes:

Ethernet.
Switch Ethernet.
Definición y funcionamiento.
Características de interconexión.

Del mismo modo se recomienda, en caso necesario, consultar cualquier ayuda online, así como 'man' de Linux y el manual de configuración (*Quick reference guide*) de los equipos *hub* 3Com SSII PS40 y *switch* 3Com Superstack 4500.

1.3. Equipos, tecnologías y herramientas

La práctica propuesta consiste en la configuración, monitorización y análisis de un escenario de interconexión de redes IP mediante las tecnologías LAN conmutada. Para ello, se contará con los siguientes equipos y tecnologías de interconexión:

Equipos: máquinas reales con sistema operativo Windows XP en los que se podrá ejecutar una máquina virtual mediante virtualbox. Habrá una máquina real para gestión, otra virtual para captura y dos virtuales para host. Las máquinas virtuales tendrán sistema operativo Linux (CentOS).

Tecnología de conexión: será Ethernet mediante tarjetas internas con una velocidad de 10/100 Mbps. El equipo de captura consta de dos tarjetas, identificadas en Linux como eth0 y eth1, correspondientes respectivamente a las tarjetas superior e inferior. En el equipo de gestión y los host se utilizará únicamente la tarjeta superior.

Elementos de interconexión de la red LAN del laboratorio (dos *hub* 3Com SSII PS40 y un *switch* 3Com SSII 4500); que disponen de las siguientes posibilidades de gestión:
Gestión a través del puerto de consola.
Gestión a través del servidor *telnet* que implementa el conmutador.
Control rápido del funcionamiento del conmutador a través de los LED en el panel frontal.
Gestión basada en web a través del servidor HTTP que implementa el conmutador.
Gestión basada en el protocolo SNMP.

En cuanto a las **herramientas** necesarias para la verificación y el análisis de los escenarios, utilizaremos el software de captura ***tcpdump*** y el analizador de protocolos ***Wireshark***.

1.4. Escenarios

A continuación, se muestra la disposición de los escenarios con los que se trabajará a lo largo de toda la práctica.

En la figura 1.1 se muestran todas las interfaces de conexión, así como los equipos de interconexión asociados.

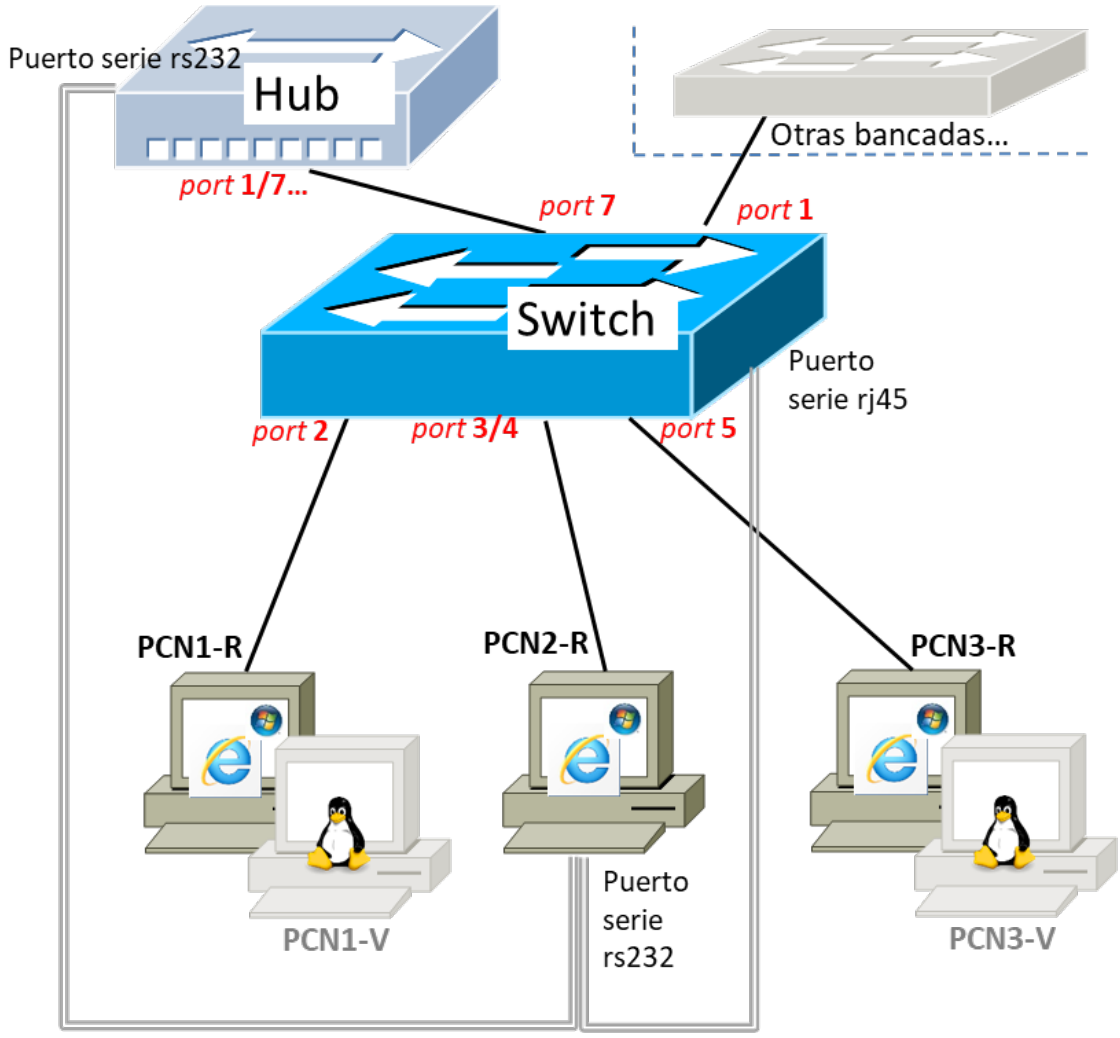


Figura 1.1: Escenario de interconexión de redes para la bancada N.

La Figura 1.2 nos muestra la conexión entre los *switch* de las diferentes bancadas.

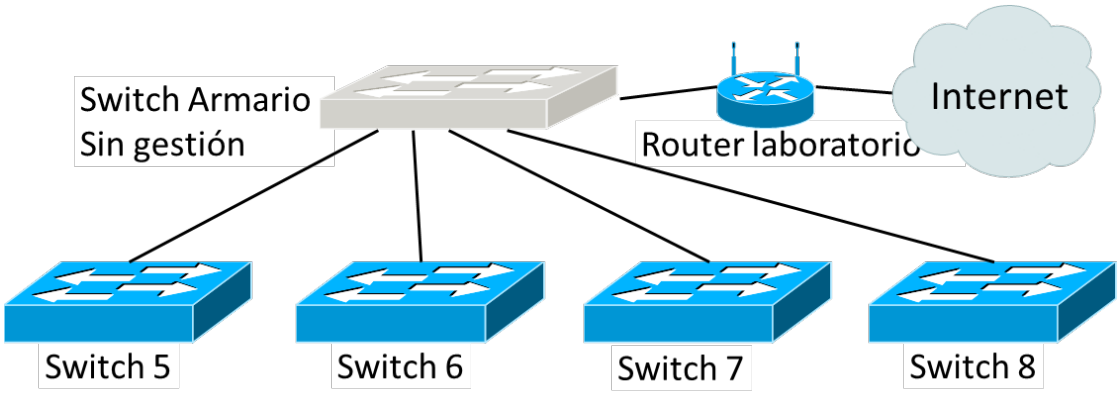


Figura 1.2: Escenario de interconexión del laboratorio.

La Figura 1.3 nos muestra cuál debe ser la configuración del escenario que probaremos sobre GNS3.

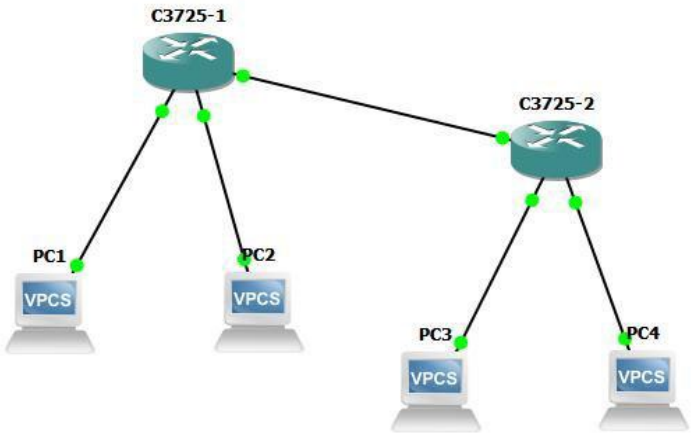


Figura 1.3: Escenario virtual para GNS3.

2. Realización práctica en el laboratorio

Como se ha comentado anteriormente, para la realización de esta práctica se utilizarán equipos reales con SO Windows y máquinas virtuales con SO Linux (CentOS).

En el caso de no poder acceder presencialmente al laboratorio, este capítulo 2 no se ejecuta tal y como aparece, sino que se hará solamente el capítulo 3.

**** El entregable sirve de guía para el seguimiento de la práctica. Completar todas las cuestiones implica alcanzar todos los resultados de aprendizaje requeridos ****

**** La evaluación al final de la práctica supondrá la discusión con el profesor de los apartados propuestos y la entrega de cuestiones del entregable ****

**** Las cuestiones marcadas como E se resolverán antes del comienzo de la práctica y se entregarán individualmente ****

**** Comentar con el profesor o contestar en el entregable, según se indique. Las preguntas marcadas como P. Se entregarán por grupos ****

**** Habrá cuestiones marcadas como E y P simultáneamente. Esto significa que hay que resolverlas antes de la práctica y también comprobar el grado de acierto en el transcurso de la misma. La E se entrega individualmente y la P por grupos ****

Configuración previa

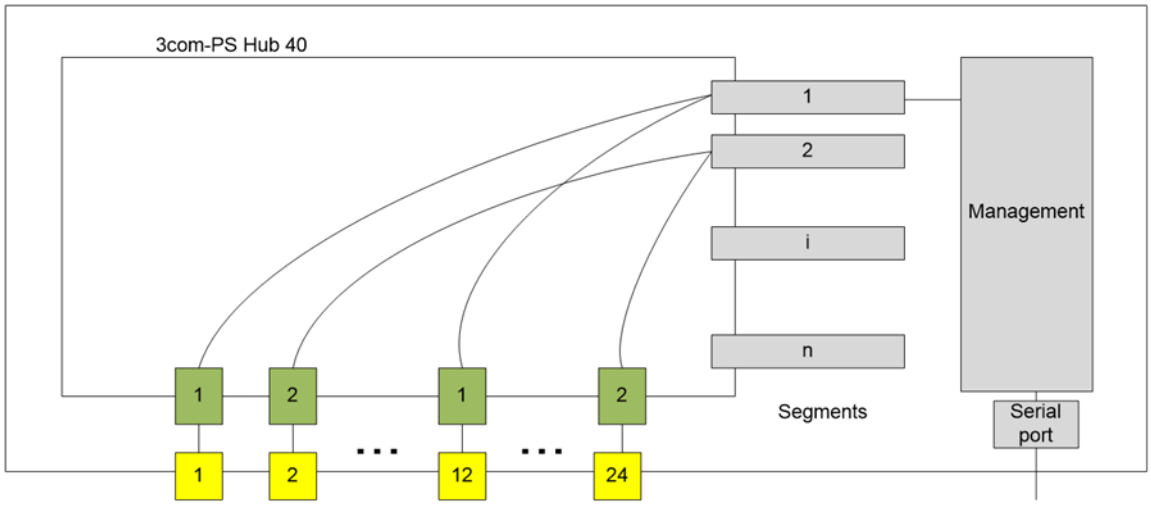
Para configurar correctamente el escenario a lo largo de la práctica, tal y como se va indicando, asegurarse inicialmente de que **son correctas las conexiones indicadas** en la figura 1.1.

Inicialmente, se configurará el direccionamiento IP manteniendo los datos de los equipos en la red del laboratorio. En PCN1 y PCN3 trabajaremos tanto con la máquina real como la máquina virtual de linux. En PCN2 sólo con la real. En PCN1-virtual y PCN3-virtual configuraremos la dirección IP **155.210.157.Y**, siendo Y = X + 4, siendo X el último byte de la dirección IP de la máquina real (etiqueta frontal).

2.1. Configuración y Gestión del hub.

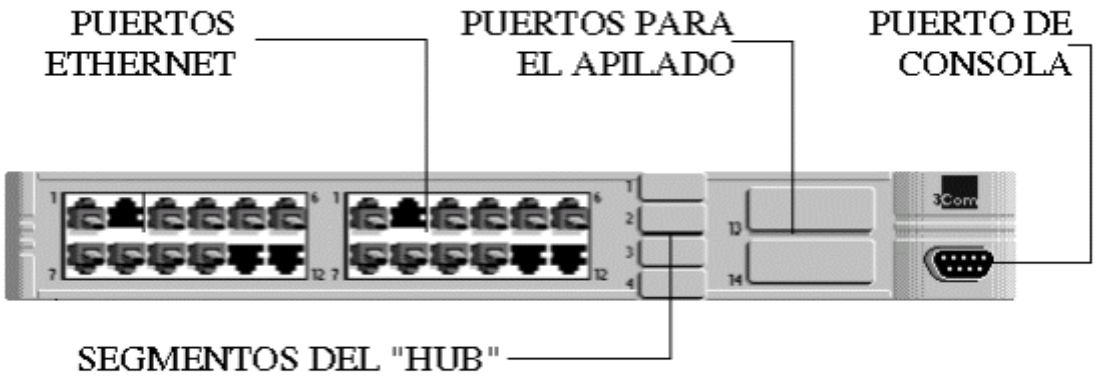
Para este apartado de la práctica, no será necesario entregar ningún documento, sino que haremos una serie de ejemplos que serán utilizados para la realización del trabajo final de gestión.

Recordemos el esquema del *hub* que hemos visto en la teoría:



Este *hub* dispone de 24 puertos l0BaseT RJ45 y con la posibilidad de generar 4 segmentos. Estos puertos pueden estar conectados a la tarjeta Ethernet de un ordenador mediante un cable directo, o conectado a otro *hub* o *switch* a través de un cable cruzado. Además dispone de un puerto de consola DB9, con los parámetros siguientes: 9600 kbps, 8 bits de datos y 1 bit de parada. Por último existen dos puertos en la parte de atrás (25 y 26) para apilar varios *hub*, permitiendo de esta forma el crecimiento de la red.

Estos puertos vienen representados en la siguiente figura, junto con la posibilidad de utilizar hasta 4 segmentos como si fueran 4 *hub* aislados entre sí.



El estado de funcionamiento del *hub* se indica en un conjunto de led, cuyo código de colores es el siguiente:

Para los puertos:

el led está verde si el puerto está habilitado
el led está verde parpadeando si está inhabilitado
el led está apagado si no hay nada conectado.

Para los segmentos:

el led está apagado si no hay tráfico
el led está verde si hay tráfico y amarillo si hay colisión.

Vamos a establecer dos clasificaciones posibles para la gestión del *hub*:

A.-La primera de ellas se basa en el tipo de puerto al cual se conecta el equipo de gestión:

1.-Puerto de consola: Utilizado como tal o conectado a un modem

2.-Puerto Ethernet.: Situado comúnmente en el segmento 1 del *hub*, con una dirección IP asignada.

B.-La segunda clasificación está en función del servidor utilizado para la gestión:

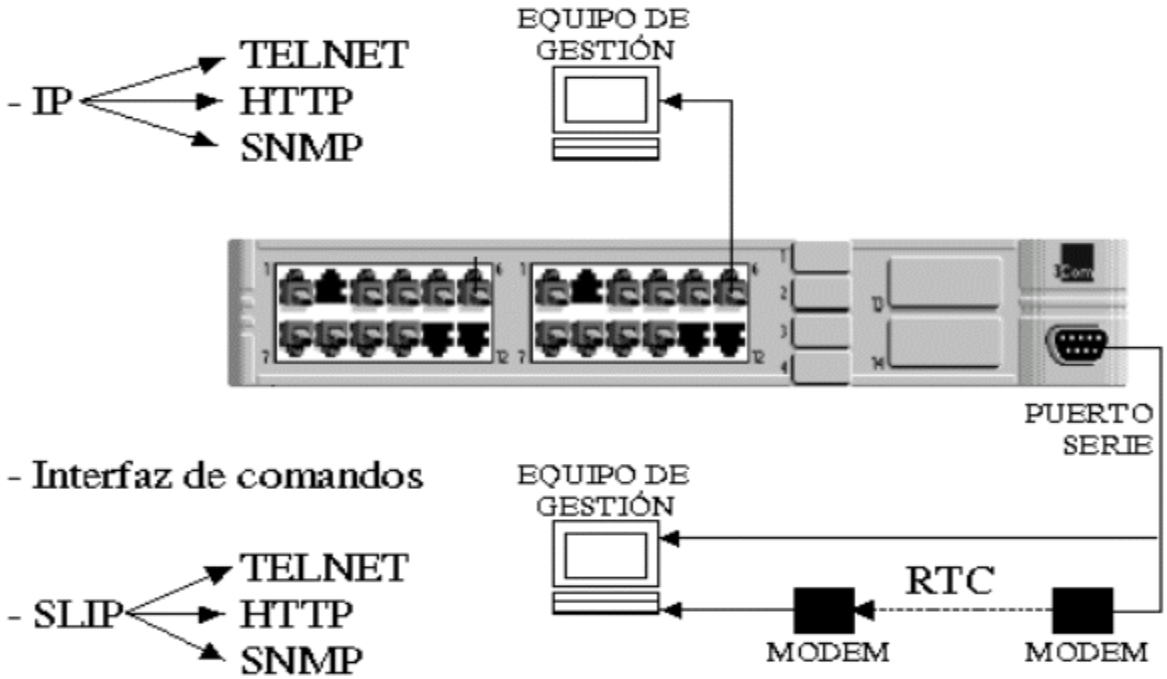
1.-Interfaz línea de comandos: Directamente sobre una consola.

2.-*TELNET*. Conectándonos a un servidor *telnet* situado en el *hub*, con una presentación similar a la interfaz línea de comandos.

3.-HTTP. Utilizando el protocolo http, conectándonos a un servidor web residente en el propio *hub*. Siendo necesario el uso de un navegador.

4.-SNMP/RMON. Donde el *hub* actúa como agente SNMP/RMON, siendo necesario un gestor externo.

Hay que indicar que en el caso de usar el puerto de consola son posibles todos los servidores. Sin embargo, si se usa un puerto Ethernet, la interfaz línea de comandos no está habilitada.



2.1.2.- Ejemplos de métodos de gestión del hub

Llegados a este punto vamos a poner en práctica cuatro métodos de gestión: Interfaz de comandos, servidor *TELNET*, servidor HTTP y servidor SNMP/RMON.

Por motivos de seguridad, para poder acceder al *hub* será necesario introducir un login de usuario y su clave correspondiente. Existen varios usuarios posibles, de los cuales comentaremos dos, cuyos *login* son *security* y *monitor*, cada uno con unos privilegios asignados diferentes. El usuario *security* tiene asignados todos los privilegios, lo que permite realizar cambios en la configuración. El usuario monitor únicamente puede ver el estado del *hub*, sin modificarlo. El usuario que utilizaremos será security y la clave se facilitará en la propia sesión de prácticas.

A continuación, lo que haremos será conectarnos a los diferentes servidores de administración del *hub* y realizar una serie de acciones de configuración sobre los mismos.

2.1.3.- Gestión a través del puerto de consola y servidor interfaz de comandos.

Este procedimiento lo usaremos para entrar por primera vez en el equipo.

Nos conectamos al *hub* desde PC*N*2 (máquina real Windows) mediante una conexión de puerto serie. Para ello lanzamos alguna aplicación de emulación de terminal que tengamos en el ordenador (por ejemplo *hyperterminal)*. Debemos tener en cuenta que el servidor que nos atiende es el *Interfaz de Comandos*.

Las acciones más importantes a realizar en el *hub* son las siguientes:

1.- Reiniciar con los parámetros de fábrica (**`initialize`**).

2.- Definir una dirección IP en el *hub*, que no pertenezca a la subred IP del interfaz Ethernet del ordenador (por ejemplo, una de la red **`155.210.156.0`**).

3.- Conectar físicamente, mediante tecnología Ethernet, el ordenador al *hub*.

4.- Intentar hacer un **`ping`** desde el *hub* al ordenador, y comprobar que no llega.

5.- Definir ahora una dirección IP en el *hub* que sí pertenezca a la subred IP del ordenador.

6.- Comprobar que ahora funciona el **`ping`**.

De esta forma, sí podemos conectarnos al *hub* de forma remota. A pesar de todo debemos dar ahora los permisos necesarios para poder utilizar los diferentes servidores de administración del *hub*.

7.- Cambiamos el *password* (esto será necesario para usar los servidores *Telnet* y HTTP).

8.- Habilitamos la conexión remota.

9.- Definimos la *comunidad* (esto será necesario para usar el servidor SNMP).

10.- Para terminar, realizamos un **`initialize`**, de tal forma que borramos la configuración que acabamos de introducir y salimos de la conexión de consola.

2.1.4.- Gestión a través de los puertos Ethernet y servidor telnet.

Nos conectamos desde PC*N*2 (máquina real Windows) al servidor *Telnet* del *hub*, utilizando el siguiente comando:

```
> telnet <dirección IP del hubN>
```

Una vez conectados, vemos que el entorno es similar al de la interfaz de comandos.

A continuación, nos disponemos a realizar una serie de configuraciones relacionadas con los puertos y los segmentos del *hub* y a comprobar su funcionamiento:

1.- Comprobar las estadísticas de los puertos del *hub*.

2.- Ver en detalle los puertos 1 y 7.

3.- Ver el estado de los puertos 1 y 7.

4.- Comprobar las estadísticas de los segmentos del *hub*.

5.- Ver en detalle los segmentos 1 y 2.

6.- Cambiar los puertos 7 y 8 al segmento 2 y comprobar que el cambio se ha realizado.

Ahora vamos a ver que, si conectamos el ordenador a un segmento que no sea el 1, no se puede realizar una conexión remota. Esto ocurre por motivos de seguridad. Para ello se propone realizar las siguientes acciones:

7.- Salimos de *Telnet*.

8.- Comprobamos que funciona el **`ping`** al *hub*.

9.- Cambiamos la conexión al puerto 7 del *hub*, que está en al segmento 2. Vemos que no funciona el **`ping`**.

10.- Conectamos con un cable cruzado el puerto 8 (segmento 2) con el puerto 2 (segmento 1). Vemos que funciona el **`ping`**. Ahora entrando por el puerto 7 (segmento 2) podemos acceder al segmento 1, pudiéndose, ahora, realizar la configuración del *hub*.

Para finalizar, si hay tiempo suficiente y con carácter opcional, vamos a estudiar las estadísticas de los puertos 2, 7 y 8 y los segmentos 1 y 2, comprobando así el funcionamiento de la nueva configuración.

11.- Vamos a salir de *Telnet* y entrar en la interfaz de comandos (por puerto serie). De esta forma no interferimos en las pruebas que queremos realizar. En la interfaz de comandos realizamos una operación de **`reset`** que pone a cero las estadísticas del *hub*.

12.- Salimos de la interfaz de comandos y volvemos a entrar en *Telnet*. Realizamos algunas funciones para que se produzca tráfico (por ejemplo, navegar por alguna página web).

13.- Salimos de *Telnet* y entramos en la interfaz de comandos. Ahora estudiamos las estadísticas.

2.1.5.- Gestión a través de los puertos Ethernet y servidor http.

Nos conectamos desde PCN2 al servidor HTTP del *hub*, utilizando un navegador explorer (esta condición está impuesta porque el servidor web del hub es antiguo y no admite correctamente conexiones desde navegadores más modernos). Una vez conectados, podemos apreciar que el entorno es mucho más amigable, aunque más lento que los anteriores. Como antes de esta sesión se ha inicializado el *hub* y ésta es la primera vez que se entra en el servidor HTTP, lo primero que se nos propone (por decisión del fabricante) es la configuración de los parámetros básicos del equipo. Una vez realizada esta configuración inicial, que tendrá los mismos valores que en el apartado anterior, pasamos a realizar las siguientes acciones:

1.- Ver los parámetros del puerto serie.

2.- Ver los puertos que sirven para el apilado (25 y 26).

3.- Comprobar los segmentos del *hub* y los puertos que tienen conectados.

4.- Entrar en detalle en los puertos 1 y 7.

5.- Cambiar el segmento del puerto 9.

6.- Volver a la página inicial del servidor.

7.- Encontrar la dirección Ethernet del *hub*. En realidad no es la dirección del *hub* sino del equipo interno que gestiona el *hub*. Lo mismo pasa con la dirección IP.

8.- Verificar los datos de IP del *hub*.

Hemos comprobado que hay parámetros que no aparecen en el servidor *Telnet* y sí lo hacen en HTTP. Esto ocurre porque al tratarse de programaciones distintas en los distintos servidores, éstas pueden acceder a parámetros internos diferentes.

2.1.6.- Gestión a través de los puertos Ethernet y servidor SNMP

La conexión al servidor SNMP del *hub* se realizará desde cualquiera de las máquinas virtuales Linux, utilizando los siguientes comandos: **snmpwalk**, **snmpget** o **snmpset**. Para utilizar estos comandos es necesario haber instalado un gestor SNMP (**$ yum install net-snmp-utils**), mientras que el hub deberá tener instalado un agente SNMP. Este método es menos intuitivo que los anteriores, ya que se necesita conocer la codificación ASN.1 (MIB) de los parámetros de configuración del *hub*.

Las acciones a realizar son las siguientes:

1.-Verificar los segmentos que componen el *hub*.

```
snmpwalk –v 1 –c [comunidad] [IP] .1.3.6.1.4.1.43.10.26.1.1.1.5
```

Siendo ***[IP]*** la dirección IP del *hub*. El valor de ***[comunidad]*** es una palabra que debe ser configurada previamente en el menú snmp cuando accedemos con telnet y tiene un uso similar al *password*. El resultado del comando será una lista de los puertos del *hub* y del segmento al que están asignados. Este valor de segmento no es 1, 2, 3 o 4 como cabría esperar sino un valor numérico que varía de un *hub* a otro.

2.-Modificar el puerto 10 poniéndolo en el segmento 2. Obtenemos primero el valor **seg-2** asociado al segmento 2:

```
snmpget –v 1 –c [comunidad] [IP] .1.3.6.1.4.1.43.10.26.1.1.1.5.1.1002
```

El valor leído [seg-2] lo establecemos para el puerto 10:

```
snmpset –v 1 –c [comunidad] [IP] .1.3.6.1.4.1.43.10.26.1.1.1.5.1.10 i [seg-2]
```

Para comprobar el cambio realizado:

```
snmpwalk –v 1 –c [comunidad] [IP] .1.3.6.1.4.1.43.10.26.1.1.1.5
```

3.-Comprobar los valores de direccionamiento IP. Ejecutar:

```
snmpget –v 1 –c [comunidad] [IP] .1.3.6.1.4.1.43.10.27.1.1.1.15.1
```

Como respuesta obtendremos un valor numérico de la interfaz de configuración, que deberemos utilizar en el siguiente comando.

Para comprobar el valor de la dirección IP del *hub:*

```
snmpget –v 1 –c [comunidad] [IP] .1.3.6.1.4.1.43.10.28.1.1.2.[valor]
```

Para comprobar el valor de la máscara de la dirección IP del *hub*:

```
snmpget –v 1 –c [comunidad] [IP] .1.3.6.1.4.1.43.10.28.1.1.3.[valor]
```

Para comprobar el valor del índice de la dirección IP del *router* por defecto:

```
snmpget –v 1 –c [comunidad] [IP] .1.3.6.1.4.1.43.10.28.1.1.4.[valor]
```

4.-Modificar la dirección IP del *router* por defecto:

```
snmpset –v 1 –c [comunidad] [IP] .1.3.6.1.4.1.43.10.28.1.1.4.[valor] a
155.210.157.254
```

Siendo *[valor]* el índice de la IP del *router.*

En definitiva, para poner un ejemplo de comparación entre los tres servidores remotos, hemos visto el tiempo que se tarda en comprobar la segmentación del *hub*.

A.- El uso de SNMP nos proporciona la respuesta más rápida, aunque tenga el entorno menos “amigable”.

B.- El uso de *Telnet* es más amigable pero el tiempo de respuesta es mayor.

C.- El tiempo de respuesta del servidor web es el mayor, aunque se sitúa en un entorno de utilización al cual todos estamos acostumbrados (el navegador).

D.- El servidor SNMP debe permitir modificar cualquier valor, cosa que no ocurría en los otros servidores, que dependen de la programación.

2.1.7.- Trabajo de Gestión para entregar

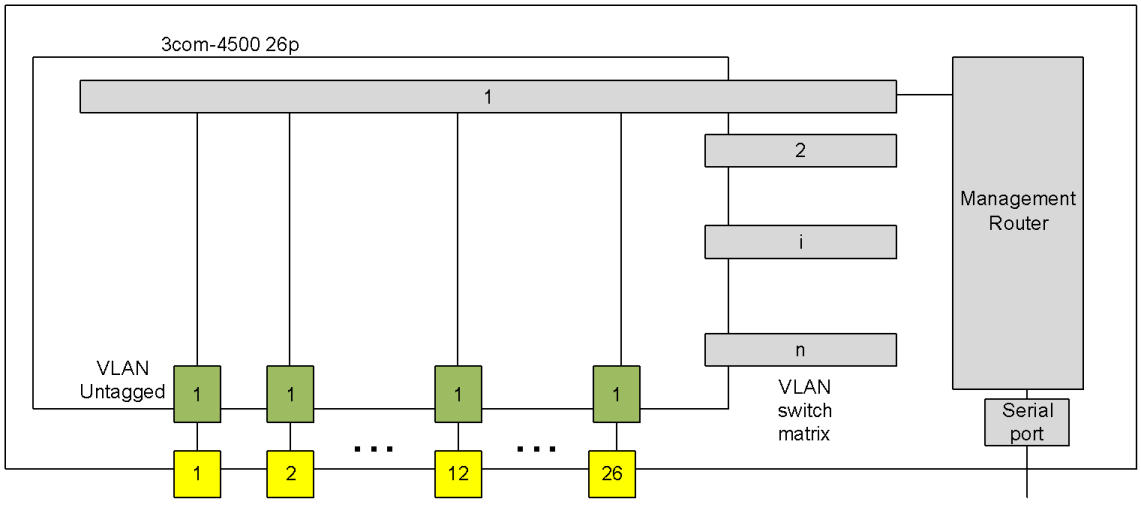
Como tarea adicional (obligatoria y evaluable) a la realización de la práctica de debe desarrollar un programa que realice (de la forma más eficiente, automática y desasistida posible, teniendo en cuenta que debe servir para gestionar varios *hub* simultáneamente) la asignación de puertos a segmentos de *hub*. Tanto el lenguaje de programación como el servidor al que se conecte la aplicación se deja a la elección del alumno (aunque se recomienda usar Shell y servidor SNMP, se pueden utilizar otras herramientas de programación, como Rubi, Python, etc).

Cada grupo deberá entregar el código fuente del programa desarrollado, y el ejecutable (preferiblemente que pueda correr en los PC del laboratorio o *Ubuntu for Windows*).

2.2. Introducción a la Configuración del switch.

Para los apartados 2.2.1, 2.2.2 y 2.2.3 de la práctica, no será necesario entregar ningún documento, sino que consta de una serie de ejemplos introductorios a la gestión del *switch*.

Recordemos el esquema del *switch* que hemos visto en la teoría:



Los *switch* del laboratorio tienen las siguientes características:

- 24 puertos 10/100 Mbps RJ45, 2 puertos 1Gbps con conector RJ45 o fibra.
- 1 puerto consola RJ45.
- Es apilable.

Al igual que en el *hub,* existen varios métodos para **configurar el *switch,*** de los cuales vamos a utilizar dos para realizar la configuración: A través del puerto de consola y servidor interfaz de comandos y a través de los puertos Ethernet y servidor http. Para ello utilizaremos como apoyo el documento "*quick reference guide*". Los *user* y *password* se darán durante la práctica.

2.2.1 Introducción a la Configuración del switch a través del puerto de consola y servidor interfaz de comandos.

En este apartado utilizaremos primeramente el modo de conexión a través de consola. Para realizar esta configuración utilizamos el interfaz de línea de comandos (*Command Line Interface*, CLI) del *switch* 4500. Hay que advertir que esta gestión sirve tanto para puerto de consola como para *telnet* y *ssh*:

- Puerto de consola: mediante una conexión local o bien a través de un módem. La conexión al *switch* ha de realizarse con un cable RJ-45 a DB-9 (ver Fig. 2.2).

- Conexión vía *telnet* o *ssh* al *switch*.: para ello se debe conectar la estación de trabajo a un puerto perteneciente a la VLAN 1. De lo contrario, no se podrá acceder a la gestión.

Usaremos un cable con RJ45 en el extremo *switch* y DB-9 en el extremo del **PCN2**. A continuación se presenta el esquema de conexiones del puerto de consola.

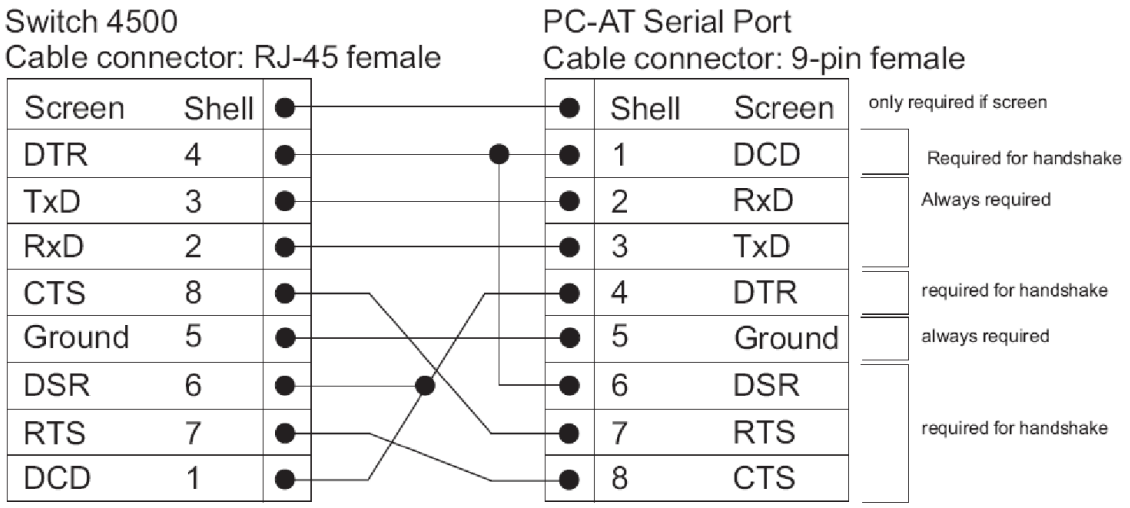


Figura 2.1. Conexionado RJ-45 a DB-9

Este sistema de configuración se utiliza, al menos la primera vez, para configurar una dirección IP y poder conectarnos por otros métodos de gestión a través de la red.

Vamos a utilizar un programa de conexión a través del puerto serie del PCN2 (*Hyperterminal* en Windows) con los siguientes parámetros:

- Conexión directa a través del puerto de comunicaciones COM1
- Velocidad de transmisión: 19200 bps
- Formato de trama: 8 bits, no paridad y 1 bit de stop (8N1)
- Control de flujo: ninguno

Pero antes de realizar modificaciones en la configuración vamos a exponer algunas consideraciones:

a) Este interfaz proporciona los comandos necesarios para configurar y gestionar el *switch*. El CLI en la familia de *switch* 4500 tiene las siguientes características:

Protección jerárquica de comandos: es posible controlar los comandos que cada usuario específico puede ejecutar para prevenir el acceso no autorizado a determinadas características del *switch*.

Ayuda online: los usuarios pueden obtener ayuda en cualquier momento tecleando el signo de interrogación (**?**).

Depuración: el *switch* es capaz de mostrar información de depuración para ayudar a diagnosticar y localizar los problemas de red.

Historia de los comandos introducidos: esta característica permite a los usuarios obtener los comandos ejecutados más recientemente para facilitar una nueva ejecución (flechas ↑ y ↓).

Completado automático de los comandos: el sistema permite introducir el texto de los comandos de forma parcial. El comando será ejecutado mientras el sistema sea capaz de identificar inequívocamente las palabras clave introducidas. También es posible completar el texto de un comando pulsando la tecla Tabulador.

b) El *switch* 4500 usa protección jerárquica de comandos para prevenir que los usuarios con menos privilegios puedan acceder a comandos de alto nivel para cambiar la configuración del *switch*. En función del privilegio, los comandos se clasifican en 4 niveles:

Visitante (*Visitor*, nivel 0): los comandos de este nivel se usan principalmente para diagnosticar la red y no pueden ser salvados en el fichero de configuración. Por ejemplo, los comandos **`ping`**, **`tracert`** y **`telnet`** son comandos de nivel 0.

Monitor (*Monitor*, nivel 1): los comandos de este nivel se usan principalmente para mantener el sistema y diagnosticar fallos de servicio, y tampoco pueden ser salvados en el fichero de configuración. Por ejemplo, los comandos de depuración y terminal pertenecen a este nivel.

Sistema (*System*, nivel 2): los comandos de este nivel se usan principalmente para configurar los servicios, e incluyen comandos de routing y de la capa de red. Estos comandos pueden ser usados para proporcionar servicios de red de forma directa.

Gestor (*Manage*, nivel 3): los comandos de este nivel están asociados con la operación y mantenimiento básicos del sistema. Estos comandos proporcionan soporte a servicios. Los comandos usados para el sistema de ficheros, bajada de ficheros a través de FTP/TFTP/Xmodem, gestión de usuarios y control de niveles de acceso requieren de este nivel.

c) Por defecto, el usuario que entra en el *switch* a través del puerto de consola es un usuario de nivel 3, mientras que los usuarios que entran a través de *telnet* y *ssh* son de nivel 0. Para poder ver los usuarios conectados al *switch* en cada momento,

así como su nivel de privilegio, basta con ejecutar el comando: **display users all**. También es posible ver desde dónde se conectan los usuarios con el comando: **display connection.** La información general sobre todos los usuarios del sistema se puede conseguir con el comando comando **display local-user**. Si se desea cambiar el nivel de privilegio, el comando a ejecutar es: **super <nivel>,** donde **<nivel>** es cualquiera de los niveles de privilegio, de **0** (mínimo privilegio) a **3** (máximo privilegio).

d) Los interfaces sobre los que aparece el CLI de cada usuario son de dos tipos, AUX y VTY. De esta forma, es posible tener varios usuarios simultáneos en el *switch*.

AUX: usado cuando se entra en el *switch* a través del puerto de consola. Existen 8 diferentes (**AUX0** hasta **AUX7**), y por defecto se usa el **AUX0**.

VTY (Virtual Type Terminal): usado cuando se entra en el *switch* a través de *Telnet* o *ssh*. Existen 5 diferentes (**VTY0** hasta **VTY4**), y por defecto se usa el **VTY0**.

e) Finalmente, cabe destacar que existen dos vistas diferentes en los menús de CLI:

Vista usuario (*User View*): esta vista es la mostrada cuando un Usuario se conecta al *switch* por primera vez y los comandos que se pueden introducir tienen que ver con información básica acerca de la operación y estadísticas del *switch*. El *prompt* que aparece en esta vista es **<4500>**.

Vista sistema (*System View*): esta vista posibilita la configuración de los parámetros del *switch*. Para poder pasar a esta vista, hay que teclear el comando *system-view*. El *prompt* para esta vista es **[4500]**. Para regresar a la vista usuario, basta con pulsar **<CTRL+Z>**.

La lista completa de comandos y sus correspondientes comandos web se encuentra en el documento *Quick Reference Guide* del *switch*.

2.2.2 Actualización del software del switch a través del puerto de consola.

OJO: NO VAMOS A REALIZAR NINGUNA ACTUALIZACIÓN pero sí que vamos a ver cómo se hace. El primer paso para trabajar con el *switch* es elegir y cargar la versión de *software* con la que se desea trabajar. Para actualizar el *software* del *switch* se deben seguir los siguientes pasos:

Conectar con www.3com.es y elegir la versión de software que se desea cargar en el *switch.* Las versiones de software son ficheros ejecutables, por ejemplo: s3n03_03_00s168.exe.

Lanzar el servidor TFTP en una máquina conectada al *switch.*

Almacenar el fichero de actualización en el directorio por defecto del servidor TFTP.

Conectarse al *switch* vía *telnet* desde otra máquina (tanto el usuario *admin* como *manager* pueden realizar la actualización del *software*).

Seguir los siguientes pasos en la conexión *telnet* con el *switch*:

```
> system-view
```

```
> control
> softwareUpgrade
   Enter the IP address of the TFTP Server: 155.210.157.82
   Enter the upgrade file name: s3n03_03_00s168.exe
```

En este momento aparecen dos mensajes por pantalla: "**Software Upgrade has begun**…." y "**Conection to host lost**". En este momento se pierde la conexión vía *telnet* con el *switch*.

Durante el tiempo que dura la actualización del *software* los leds del *switch* se iluminan en tono verde y una vez finalizada el *switch* se reinicia automáticamente.

2.2.3 Configuración de IP a través del puerto de consola.

El primer paso, antes de comenzar a trabajar con el *switch,* es asignarle una dirección IP que pertenezca a la subred donde se encuentran los ordenadores con los que vamos a trabajar. Esto nos permitirá, posteriormente, conectarnos vía web desde el equipo de gestión para realizar el resto de configuraciones del conmutador.

La dirección IP que es necesario asignarle al *switch* es la dirección correspondiente al etiquetado de su panel frontal (dentro de la red 155.210.157.0/24).

Para ello nos conectamos al *switch*, **desde PCN2** ejecutando en la **máquina real Windows** la aplicación de conexión puerto serie. De esta forma nos conectamos vía puerto de consola al *switch* y entramos en los siguientes menús:

```
>system-view
>interface Vlan-interface 1
>ip address <dirección IP> <mascara>
```

Después de completar estos comandos, podemos ver que la configuración ha surtido efecto en el interfaz seleccionado:

```
>display ip interface Vlan-interface 1
>display ip interface brief Vlan-interface 1
```

2.2.4 Configuración del switch a través de los puertos Ethernet y servidor http.

Esta configuración la vamos a realizar desde la máquina real Windows PCN2.

Lanzamos el navegador Internet Explorer (por el mismo motivo que con el *hub*) y nos conectamos a la dirección IP del *switch* que estemos configurando.

La apariencia de la página web del *switch* es la siguiente:

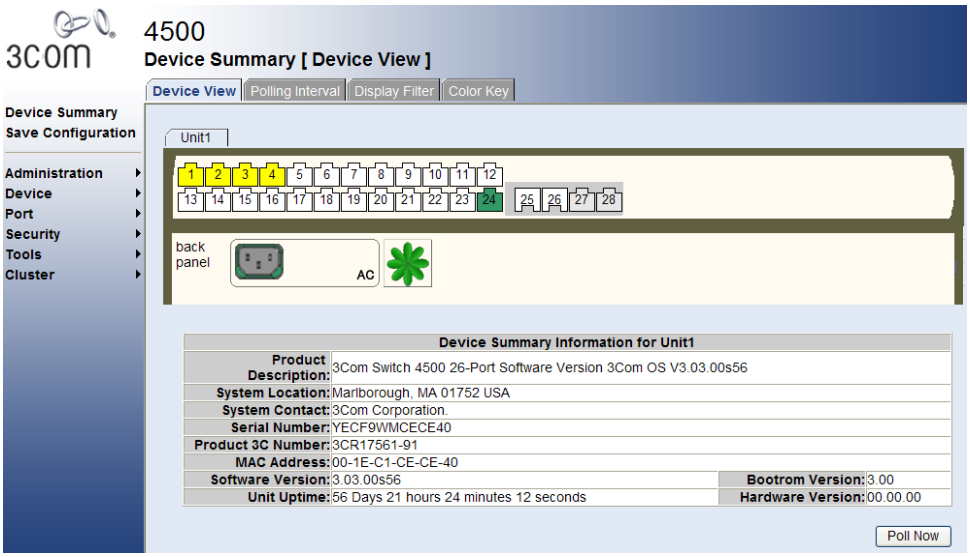


Figura 2.2. Gestión vía servidor web

En la parte izquierda aparecen los menús que vamos a seleccionar. En la parte central aparece la información correspondiente al menú seleccionado. En la parte superior central aparece el título del menú seleccionado. Más abajo hay unas pestañas para seleccionar, dentro del menú, la acción a ejecutar. Por último, en la parte inferior aparece la ventana principal con la información correspondiente a la acción que vayamos a realizar.

En la figura anterior estamos en el menú **Device Summary** y dentro del mismo en el **Device View** en el que podemos ver información sobre los diferentes puertos y parámetros básicos del *switch*.

El conmutador, como elemento de interconexión de nivel 2, es un equipo transparente a los equipos que forman la topología de red, es decir, podría decirse que "no es un equipo existente en la red IP". No obstante, este *switch* es un *switch* de nivel 3 con funciones adicionales de encaminamiento (como veremos al configurar las VLAN), con capacidad de gestión (como lo que estamos haciendo, conectándonos vía web), con funcionalidades de control (como la ejecución del Spanning Tree Protocol), etc.

P1. Teniendo esto en cuenta, identifica la dirección MAC del conmutador, ¿por qué crees que es necesaria?

Vamos a entrar en el resto de pestañas (**Polling interval**, **Display Filter** y **Color Key**) y ver la información correspondiente.

2.2.5 Configuración web de los puertos.

Vamos a entrar en el espacio de la web donde se configuran los puertos del *switch*. Para ello nos colocamos en el menú ***port*** y se despliega una ventana en la cual seleccionamos ***administation*** tal y como aparece en la figura. A partir de aquí ya no volveremos a mostrar una figura y simplemente nos referiremos a ir al menú ***port/administration***.

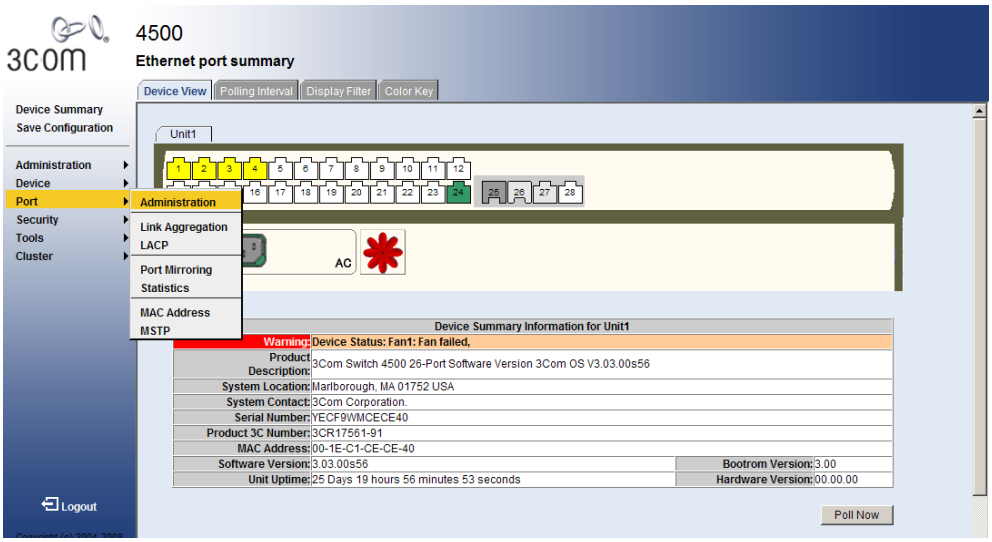


Figura 2.3. Configuración de los puertos del *switch* (Port/Administration)

Cuando lo hayamos hecho aparece la siguiente página (figura 2.4) donde vemos como título **port/administration**. Vemos también que hay tres pestañas **Sumary, Detail y Setup**. Y por último aparece el contenido central de la página donde se puede escoger la característica (***feature***) a presentar que en este caso es el ***portState***.

Vamos a realizar un repaso a las principales características de un puerto: Si el puerto está o no habilitado, qué tipo de enlace tenemos, si limitamos el número de direcciones MAC por seguridad, si la conexión es directa o cruzada (MDI), si hay control de flujo, si es *full* o *half duplex* o qué velocidad tiene el puerto Ethernet.

Se pueden comprobar cada uno de estos parámetros para todos los puertos o comprobar para cada puerto qué parámetros tiene (*Summary* o *Detail*).

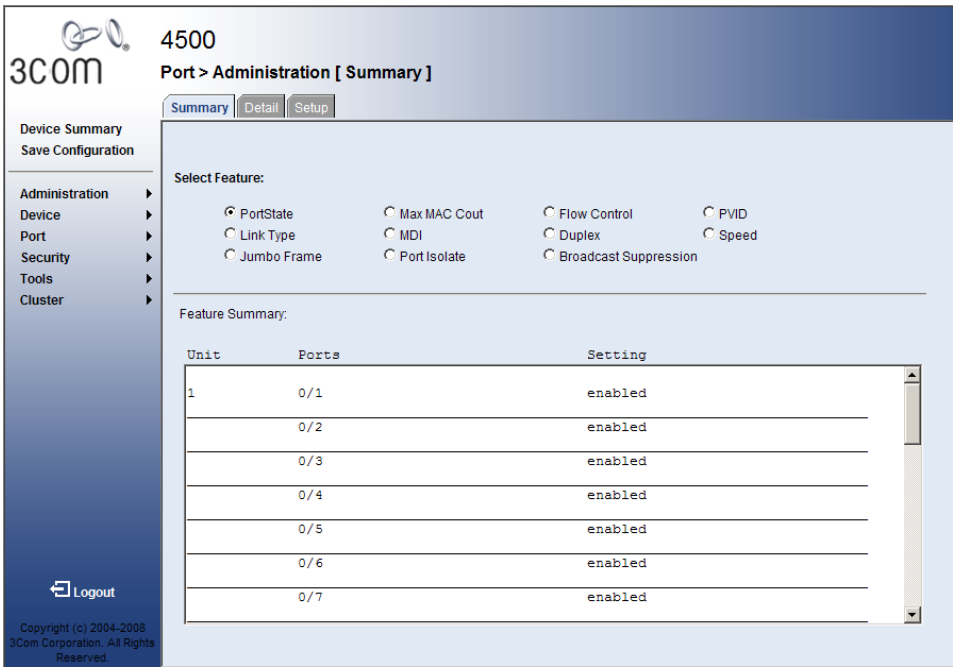


Figura 2.4. Resumen de configuración de puertos en el *switch* (Port/Administration Summary)

P2. Realizar la comprobación para los **puertos 1 y 5**. Indicar las diferencias observadas. Por último, se pueden modificar los parámetros seleccionando la pestaña **Setup**. Dos de los parámetros que cambiaremos en apartados posteriores de la práctica son Link Type y Max MAC Count, así que ahora es el momento de localizarlos y recordarlos.

2.2.6 Configuración web de los parámetros IP.

En este apartado vamos a estudiar la configuración de los parámetros IP de direccionamiento y encaminamiento.

Ya habíamos modificado la dirección IP en el apartado 2.1.2, pero ahora vamos a ver cómo se haría desde web.

En este caso se puede hacer de dos formas. La primera de ellas es a través del menú ***Administration/IP Setup***.

La otra posibilidad es entrar en ***Device/VLAN Interface***. En este menú tenemos varias pestañas: ***Summary, Create, Modify y Remove***. En este caso queda de manifiesto que el *switch* Ethernet puede tener direcciones IP en subredes IP distintas que pertenecen a VLAN distintas de tal forma que el equipo puede trabajar como *router*. Esto tiene su dificultad porque hasta ahora habíamos visto que los *router* accedían a LAN diferentes (o en general a redes diferentes) para conectarlas entre sí. Ahora tenemos un *switch* que puede hacer de *router* pero conectado a una misma LAN y lo que interconecta son LAN virtuales (VLAN). Por eso es muy importante que lo entendamos y el resto de la práctica va a contribuir a ello.

Hemos configurado el direccionamiento IP, el siguiente paso es configurar la tabla de encaminamiento IP. Entramos en el menú ***Devices/IP Route***. En este menú podemos ver, crear o borrar las entradas de la tabla de encaminamiento mediante la selección de la pestaña correspondiente: ***Summary, Create y Remove***. Podemos comprobar que sólo están las rutas de la propia subred y el *router* por defecto.

2.2.7 Configuración de las VLAN.

Vamos a configurar desde WEB las VLAN dentro del *switch* pero antes deberemos tener en cuenta algo sobre las VLAN:

Recordemos de la teoría que una VLAN es una agrupación de puertos físicos que son tratados de forma aislada al resto, como si pertenecieran a una LAN diferentes. Es un concepto comparable a los segmentos del *hub* pero a un nivel más alto en la arquitectura. Ethernet trabaja con VLAN usando el protocolo 802.1q “VLAN tagging “. Este añade 4 Bytes antes del campo TIPO de la trama Ethernet:

- TPID *(Tag Protocol ID,* 16 bits). Tendrá el valor **8100**.
- PCP *(Priority Code Point,* 3 bits). Valores: **0** (baja prioridad) – **7** (alta prioridad del paquete).

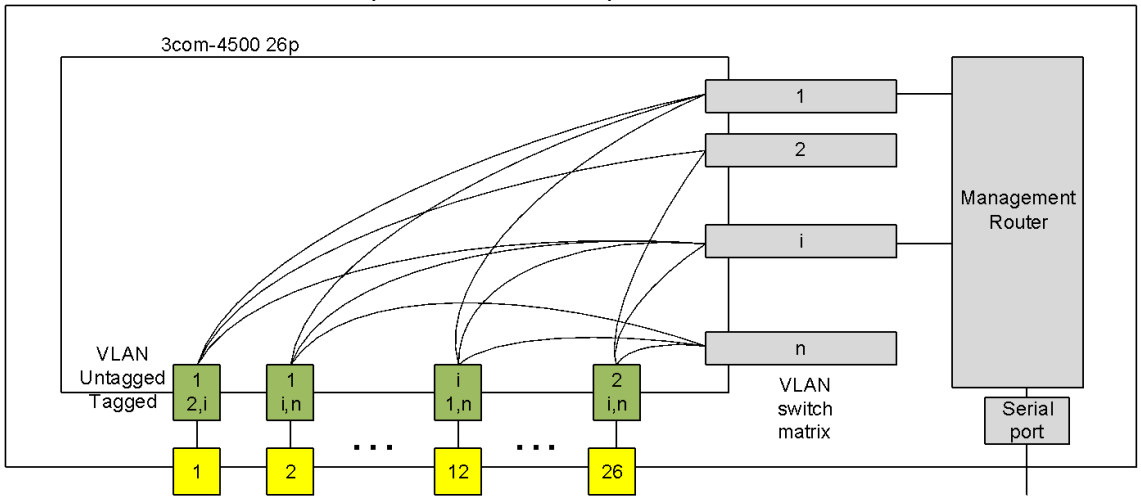
- CFI *(Cannonical Format Indicator,* 1 bit). Por compatibilidad con otras redes.
- VID *(VLAN ID,* 12bits). Habrá por tanto **4096** valores diferentes de VLAN, excepto **000** (la trama no pertenece a ninguna VLAN) y **FFF** (reservado).

Recordemos que el puerto desde el que nos conectemos para gestionar el *switch* tiene que pertenecer a la VLAN 1. Esto se cumple cuando realizamos la gestión desde PCN1.

E3/P3. Recordemos que en el apartado 2 se indicaba cómo debían estar configuradas las direcciones IP de PCN1-virtual y PCN3-virtual.
A continuación realiza un **ping** desde PCN1-virtual a PCN3-virtual. Debe funcionar correctamente.
¿Aparece en las tablas ARP de ambos equipos la correspondiente línea para el encaminamiento directo tras realizar el **ping**?

2.2.8 Untagged VLAN (identificación implícita).

Recordemos de nuevo el esquema del *switch* que hemos visto en la teoría:



- **Tagged** means that the switch gives the VLAN header field to the end node hearing in that switch port
- If the switch port is **untagged**, the machine is not able to see the VLAN header

Vamos a configurar una VLAN 2 de tal forma que el puerto del *switch* al que se conecta PCN3 pertenezca a dicha VLAN. Para ello entramos en el menú **Device/VLAN** en la pestaña de ***Setup*** y creamos la VLAN 2. Desde la pestaña ***Modify VLAN*** pasamos el puerto correspondiente como *untagged*, a la VLAN2. Comprobamos que lo hemos hecho en la pestaña ***Detail***.

E4/P4. Borra de nuevo las tablas ARP de PCN1-virtual y PCN3-virtual y vuelve a realizar el ping desde PCN1-virtual y PCN3-virtual. Mientras tanto ejecuta en PCN1-real y PCN3-real un software de captura (tcpdump o wireshark). Observamos que NO funciona el ping y NO se ve en la VLAN 2 el tráfico ARP *broadcast* de los equipos de la VLAN 1 ¿Por qué sucede esto?

A continuación vamos a configurar los interfaces que pertenezcan a la **VLAN 2** con una IP que sea de la red **192.168.*N*0.0/24** (donde ***N*** es el número de la bancada). En el caso del *switch*, esto lo haremos desde el menú ***Device/VLAN Interface*** en la pestaña **Create**. En el caso de PCN3-virtual lo haremos mediante el comando **ifconfig**.

E5/P5. Ejecuta un **ping** desde el *switch* (menú ***Tools/ping***) hacia PCN3-virtual (dirección IP privada). Mientras tanto captura el tráfico en PCN3-real ¿Se ve el tráfico ARP e ICMP correspondiente al **ping**? ¿Por qué?

Vamos a aprovechar que el *switch* tiene funciones de encaminamiento IP para interconectar las dos VLAN. Para ello es necesario configurar adecuadamente las tablas de rutas de PCN1-virtual y PCN3-virtual. Podemos utilizar el comando **route**:

route add –net <@red> netmask <mascara> gw <@gw>

P6. Efectúa un ping desde PCN1-virtual a PCN3-virtual y captura el tráfico en PCN1-real y PCN3-real. Comprueba, en base a las capturas, la dirección MAC de las tramas ICMP en ambas VLAN y el valor del TTL.

2.2.9 Tagged VLAN (identificación explícita).

Hasta ahora hemos trabajado con VLAN *untagged*. A continuación vamos a configurar la VLAN 2 como *tagged.* Dicha configuración va a realizarse en todos los equipos que pertenecen a la VLAN. En este caso, el *switch* y PCN3-virtual.

En el switch, tenemos que ir al menú Port/Administration y configurar los puertos que pertenecen a la VLAN 2 como hybrid para que puedan ser marcados como tagged. A continuación ya podemos acceder al menú de modificar VLAN y poner dichos puertos como tagged.

En PCN3-virtual:

- Activar el módulo **8021q** para habilitar el soporte del protocolo 802.1Q.

```
$ modprobe 8021q
```

- Añadir el ID de la VLAN (2 en nuestro caso) en la interfaz de red *eth0*:

```
$ vconfig add eth0 2
```

El comando ***vconfig*** crea un *vlan-device* en *eth0* que genera la interfaz *eth0.2*. A partir de aquí puede utilizarse el comando **$ ifconfig eth0.2** para ver y configurar los parámetros de dicha interfaz.

- Borrar la dirección IP del interfaz raíz (**eth0**) del que depende la interfaz VLAN.

```
$ ip -4 addr del <@IP>/<prefixlength> dev eth0
```

Las rutas asociadas a esta interfaz se borrarán de la tabla de rutas

- Asignar al interfaz *eth0.2* la dirección IP que antes tenía la interfaz *eth0* mediante el comando **ifconfig**:

```
$ ifconfig eth0.2 <@IP> netmask <mascara>
```

- Añadir la ruta que, como se ha indicado antes, se habrá borrado. En este caso, se observará que la interfaz de salida no será *eth0*, sino *eth0.2.*

```
$ route add –net <@red> netmask <mascara> gw <@gw>
```

P7. Realiza un ping desde PCN1-virtual hacia la dirección del interfaz *eth0.2* de PCN3-virtual. Mientras tanto captura el tráfico en PCN1-real y PCN3-real. Explica en base a las capturas en los diferentes interfaces dónde aparecen tramas 802.1Q (tagged).

Una vez que hemos terminado el apartado anterior, hay que volver a poner todos los puertos en la VLAN 1, borrar la VLAN 2 y la dirección IP privada. También hay que poner los tipos de puerto como *access* (y no como *hybrid*).

También hay que poner la configuración de PCN3-real en su estado inicial, sin VLAN.

```
$ vconfig rem eth0.2
```

2.2.10 Configuración y gestión de la tabla de encaminamiento del switch.

Esta operación se hace desde el menú ***Port/MAC Address***. Lo que aparece en el navegador es la tabla de encaminamiento en la que cabe destacar que:

- *MAC ADDr* es la dirección MAC
- *State* nos dice si la dirección MAC ha sido aprendida (*Learned*) o si se configura de manera permanente (*config static*)
- *Port INDEX* es la dirección del puerto a donde encaminar el tráfico.

Las entradas a la tabla aprendidas tienen un tiempo de vida que podemos variar en la pestaña ***Setup*** del menú ***Port/MAC Address***.

E8/P8. Haz una captura de pantalla (esto no es necesario para E8) con la tabla de conmutación y comprueba que en los puertos aparezcan las direcciones MAC de los PC. ¿En qué puerto aparecen la mayoría de las direcciones y por qué ocurre esto?

P9. Crea en PCN3-virtual una entrada en la tabla arp estática con la información de una **máquina inexistente (**Ejemplo: `arp -s 155.210.157.X 00:aa:bb:cc:11:22`). Recordar que la dirección IP de la máquina inexistente debe pertenecer a la red del laboratorio pero que no debe estar usada por otra máquina (podemos usar la dirección

reservada a la máquina virtual de PCN2 que no está encendida, la real de PCN2 más 4. Realiza un **`ping`** desde PC*N*3-virtual a PC*N*2. Conecta el cable **`ethernet`** de PC*N*2, a distintos puertos del *switch*. Captura en todo los casos, y explica lo que le sucede a las tramas echo *request* cuando no aparece la MAC en la tabla de conmutación del switch.

P10. En el puerto en el que tenemos la mayoría de las direcciones, vamos a limitar a 5 el número de direcciones MAC aprendidas para este puerto (menú ***Port/Administration***).

Comprueba el correcto funcionamiento con ***Port/MAC Address***. A continuación localiza un equipo de las otras bancadas cuya dirección MAC no se encuentre entre las 5 aprendidas por tu *switch* para dicho puerto, e intenta realizar un **`ping`** a dicho equipo. ¿Qué está ocurriendo? ¿Qué ocurre con los ARP? ¿Llegan a transmitirse los *request* del ping? ¿Por qué?

P11. A continuación ponemos el límite de direcciones aprendidas en el puerto a 0. Configura manualmente la tabla de conmutación del *switch* con la dirección MAC del *router* del laboratorio de tal forma que se permita el acceso a internet de los equipos de la bancada. ¿Puedes comunicarte con los equipos de otras bancadas? Configura de nuevo la tabla de conmutación añadiendo la MAC oportuna para poder comunicarte con un PC de otra bancada.

3. Realización práctica en GNS3

A continuación, procedemos a realizar la siguiente práctica en GNS3, con las indicaciones que vienen a continuación.

**** La evaluación de esta parte de la práctica requiere la entrega del escenario GNS3 con la configuración adecuada, las capturas correspondientes que avalen su correcto funcionamiento y un documento con la explicación oportuna. ****

**** Para facilitar la elaboración del documento explicativo aparecen una serie de cuestiones a lo largo del enunciado de la práctica que deberemos ir contestando. ****

Siguiendo la Figura 1.3, queremos configurar PC1 y PC3 en la VLan2 untagged y PC2 y PC4 en Vlan3 untagged. El enlace entre los switch C3725-1 y C3725-2 debe ser tagged con las dos Vlan presentes: 2 y 3. El switch C3725-2 hará de *router* para interconectar las VLAN. **Para trabajar con Ethernet en los equipos C3725 lo haremos con la tarjeta que tiene 16 puertos Ethernet, que es la FastEthernet 2.**

Para facilitar la configuración se proporciona el siguiente guión que no está completo pero sí que tiene todas las instrucciones:

En los *switch*:

Nos conectamos a la consola de C3725-1

Para ver las vlan existentes

C3725-1# show vlan-switch para ver vlan untagged

C3725-1# show vlan-range para ver vlan tagged

Para crear vlan

C3725-1# vlan database

C3725-1(vlan)# show muestra las vlan existentes.

C3725-1(vlan)# vlan 2 para crear la vlan 2.

C3725-1(vlan)# no vlan 2 si la queremos borrar.

C3725-1(vlan)# exit Salva los cambios y sale.

Para la asignación de puertos a una vlan untagged:

C3725-1#configure terminal

Cambia la vlan del puerto 1

C3725-1(config)# interface FastEthernet 2/1

C3725-1(config-if)# switchport mode access

C3725-1(config-if)# switchport access vlan 2

C3725-1(config-if)# exit

Cambia la vlan del puerto 2

C3725-1(config)# interface FastEthernet 2/2

C3725-1(config-if)# switchport mode access

C3725-1(config-if)# switchport access vlan 3

C3725-1(config-if)# exit

Guardar los cambios

C3725-1(config)# exit

C3725-1# write

Para la asignación de puertos a una vlan tagged:

C3725-1#configure terminal

Cambia la vlan del puerto 0

C3725-1(config)# interface FastEthernet 2/0

C3725-1(config-if)# switchport mode trunk

C3725-1(config-if)# vlan-range dot1q 2 3 el puerto 0 lleva vlan tagged 2 y 3

C3725-1(config-if)# exit (dos veces pues el anterior comando nos ha introducido en un submenú, si ponemos el comando *end* en lugar de *exit*, nos saca de todos los submenús y no deja en el directorio raíz)

Guardar los cambios

C3725-1(config)# exit

C3725-1# write

C3725-1# show vlan-switch para ver vlan untagged

C3725-1# show vlan-range para ver vlan tagged

Configuración de un router en los switch para unir las diferentes VLAN.

En C3725-2 debemos realizar una configuración similar a C3725-1 que no se va a repetir en al guion y además configurar direcciones IP de diferentes redes en las diferentes VLAN y habilitar el *routing* (*forwarding*). Para esta configuración IP nos conectamos a la consola de C3725-2.

C3725-2# show ip interface brief (para ver la configuración)

C3725-2# configure terminal

C3725-2(config)# interface vlan 2

C3725-2(config-if)# ip address 192.168.2.254 255.255.255.0

C3725-2(config-if)# exit

C3725-2(config)# interface vlan 3

C3725-2(config-if)# ip address 192.168.3.254 255.255.255.0

C3725-2(config-if)# exit

C3725-2(config)# ip routing

C3725-2(config)# end

C3725-2# write

C3725-2# show ip interface brief (para ver la configuración)

En los *host*:

Nos conectamos a la consola de PCn

Configuración IP

PCn> show ip

PCn> ip 192.168.2.1 255.255.255.0 192.168.2.254

PCn> save

Con estos comandos configuramos el direccionamiento y el encaminamiento IP de los host. Hay que poner atención en que las direcciones de los PCs deben pertenecer a la VLAN a las que estén conectados.

Este apartado se debe hacer sin más indicaciones para lo cual aplicaremos lo ya aprendido

P12. Deberemos entregar el project que hayamos creado con GNS3 junto con los comandos de hayamos utilizado en la configuración. Además entregaremos las capturas que demuestren que funciona correctamente con su correspondiente explicación en el informe. Para realizar esta captura se propone, que una vez que nos aseguremos de que las tablas ARP de PC1 y PC2 están vacías (si es necesario reiniciamos PC1 y PC2), hacer un ping entre ambos PC (que pertenecen a diferentes redes IP) y capturar en el enlace entre switch comprobando la existencia de tramas ARP e ICMP y comprobando los valores MAC, IP y TTL de estas últimas.