Curso 2018-19

E.T.S. de Ingeniería
Universidad de Sevilla

3er curso
Grado en Ingeniería
de las Tecnologías de
Telecomunicación

[PRÁCTICAS DE REDES MULTISERVICIO]

Departamento de Ingeniería Telemática

ÍNDICE

Organización

Las prácticas se llevarán a cabo en grupos de 4 alumnos a lo largo de 4 sesiones de 3 horas, estando previsto el desarrollo de una práctica en cada sesión:

- Práctica 1: Manejo básico de un conmutador
- Práctica 2: Configuración básica de conmutadores
- Práctica 3: Configuración avanzada de conmutadores
- Práctica 4: Manejo de puntos de acceso Wi-Fi

En cada una de ellas llevará a cabo los ejercicios que se le propongan de forma consecutiva, dejando constancia de sus resultados y respondiendo a las cuestiones finales que se le planteen.

Al finalizar las prácticas deberá entregar una Memoria de grupo conteniendo la resolución de dichas cuestiones para lo que puede ser necesario que guarde información (configuraciones, pantallas, volcados, etc.) temporalmente en disco local y la pase después a cualquier sistema de almacenamiento en red (dispondrá de acceso a Internet) con el fin de utilizarla en la redacción final de la Memoria. Cuando sea el caso se le indicará esta circunstancia en un párrafo que comenzará con la etiqueta [**Memoria**].

El plazo de entrega de las prácticas será el último día lectivo antes de las vacaciones de navidad.

Material

Cada grupo contará con el siguiente hardware:

- 2 ordenadores
  - Windows 7
  - 2 tarjetas Ethernet
    - Una está conectada a una roseta con un cable rojo y permite el acceso a Internet con un router/nat ubicado en la red del laboratorio. **No tocar nunca**.
    - La otra está libre para su utilización en las prácticas… (cable verde)
  - 1 adaptador 802.11 (WiFi) (en la práctica que corresponda)
- 2 conmutadores HP ProCurve
  - HP2510 o HP2530 (sin capacidad de *routing*)
  - HP2610 o HP2630 (con capacidad de *routing*)
- 1 punto de acceso WiFi (en la práctica que corresponda)
- 2 cables de consola para conectar con cada conmutador (color negro, RJ45 en un extremo y DB9-puerto-serie en el otro)
- Latiguillos de conexión RJ-45 (2 cortos: PC-conmutador, 1 largo: entre conmutadores). Son de color gris.

Procure dejar el hardware en el mismo estado en que lo encontró al llegar al laboratorio. Recuerde que otros compañeros utilizarán también el material.

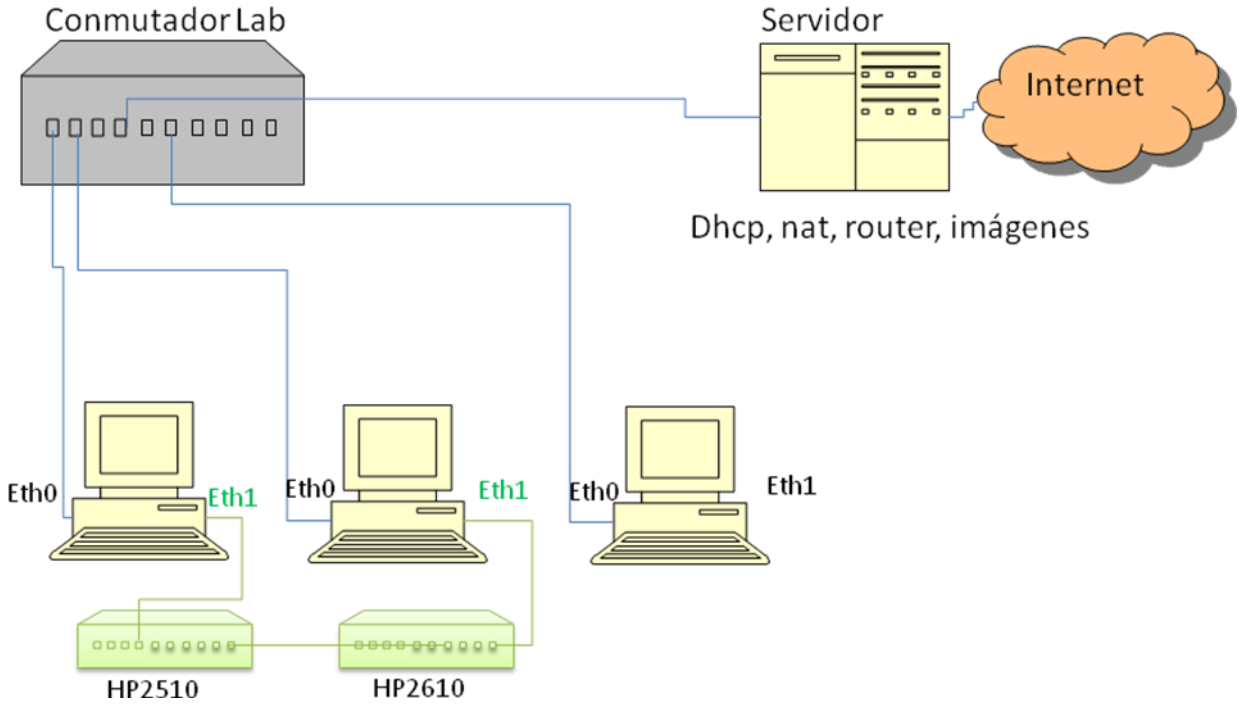
Los ordenadores tendrán las siguientes aplicaciones:

- Cliente *telnet, ssh, y consola vía puerto serie (Putty)*
  - *Opción 1: Ejecutar desde una Shell (cmd) en la carpeta de su grupo de prácticas*
  - *Opción 2: Ejecutar desde el acceso directo ubicado en el Escritorio*
- Cliente http (wget.exe) y cliente tftp *(tftp.exe)*
  - *Ejecutar mediante una Shell (cmd) en la carpeta de su grupo de prácticas*
- Servidor http (miniweb.exe) y servidor *tftp (OpenTFTP.bat)*
  - *Ejecutar desde el acceso directo ubicado en el Escritorio*
  - Opciones para verificar el funcionamiento del servidor:
    - A): observar la salida del cmd tras ejecutarlo
    - B): abrir un nuevo cmd y verificar con netstat que el proceso está escuchando en el puerto correpondiente
    - C): para http se puede abrir un explorador y poner la URL 127.0.0.1:8000
    - D): para tftp se puede abrir un nuevo cmd e intentar descargar un fichero en local
- Analizador de protocolos *Wireshark*
- Software para recortes de pantalla (anclado en la barra de herramientas)

Debe considerar como material básico los distintos manuales del fabricante, accesibles en el espacio "Material de prácticas->Manuales" de la asignatura en Enseñanza Virtual que usted deberá consultar de manera habitual para abordarlas, aunque se recomienda que haga un trabajo previo de familiarizarse con ellos evitando pérdidas de tiempo innecesarias en el desarrollo de las prácticas. Recuerde que su tiempo en el laboratorio es limitado y no debe emplearlo en tareas que pueda haber realizado con antelación.

Preparación del entorno de trabajo

Compruebe que su puesto de trabajo dispone de todos los elementos hardware del punto anterior. Encienda el PC y arranque en local con el sistema operativo Windows 7. Una vez en Windows seleccione el usuario Redes Multiservicio (clave: RRMM). El esquema de la red del laboratorio es el siguiente:



Su equipo dispone de dos interfaces Ethernet: una está conectada a la red del Laboratorio (cable rojo) y le permitirá salir a Internet mientras que la otra está libre (cable verde) y la usará para conectarse a los conmutadores HP y realizar las prácticas. Es conveniente que identifique cuál es cada una y su configuración desde la consola de Windows (**ipconfig**, **ipconfig/all** o **tracert**). Puede acceder a la cmd desde el acceso directo del escritorio o desde el menú Inicio->Ejecutar->cmd (si lo precisa, ejecútelo con permisos de Administrador)

Lo primero que debe hace es crear una carpeta en el escritorio con el nombre de su grupo (Grupo*i*) dentro de la carpeta "Grupos_RRMS" para tener toda la información que necesite guardar o utilizar, sin alterar el resto de directorios del equipo o su contenido (programas, ficheros de prueba, etc.); no obstante, dado que el PC es común para otros grupos y laboratorios, deberá asegurarse de salvar toda la documentación que haya archivado en su carpeta antes de abandonar el Laboratorio (dispone de acceso a internet, puede utilizar consigna.us.es, DropBox, Google Drive, …) puesto que por motivos de mantenimiento se podría eliminar la información que su grupo pudiera haber almacenado. **NO UTILICE PEN DRIVE USB PARA COPIAR LOS RESULTADOS DE SUS PRÁCTICAS**.

Práctica 1: Manejo básico de un conmutador (*switch*)

Para esta práctica, su grupo de prácticas se organizará en dos subgrupos de 2 alumnos que estarán identificados por un número de grupo y de subgrupo:

- Grupo***i*** (i = 1, 2, … 39)
- Subgrupo***j*** (j = 1, 2)

Los numerales ***i*** y ***j*** le servirán en las configuraciones que usará en las prácticas: carpetas del ordenador, direcciones IP, nombres del conmutador, etc. Cada subgrupo trabajará con un

ordenador y un conmutador, si bien en el momento en que se conecten los dos conmutadores entre sí será preciso trabajar en grupo.

Identifique los conmutadores que tiene en su puesto de prácticas, localice sus manuales comenzando por el "*Installation and GettingStarted Guide*" y familiarícese con sus características básicas: puertos (tipo, velocidades, estándares, cobre, fibra, etc.), PoE, capacidad de routing, etc.

Encienda los conmutadores conectando el cable de red eléctrica (no dispone de interruptor de encendido) y espere a que pase la rutina de autocomprobación (se encenderán todos los leds y después parpadearán consecutivamente en cada uno de los puertos), tras ella quedará encendido el led Act.

Esquema de funcionamiento

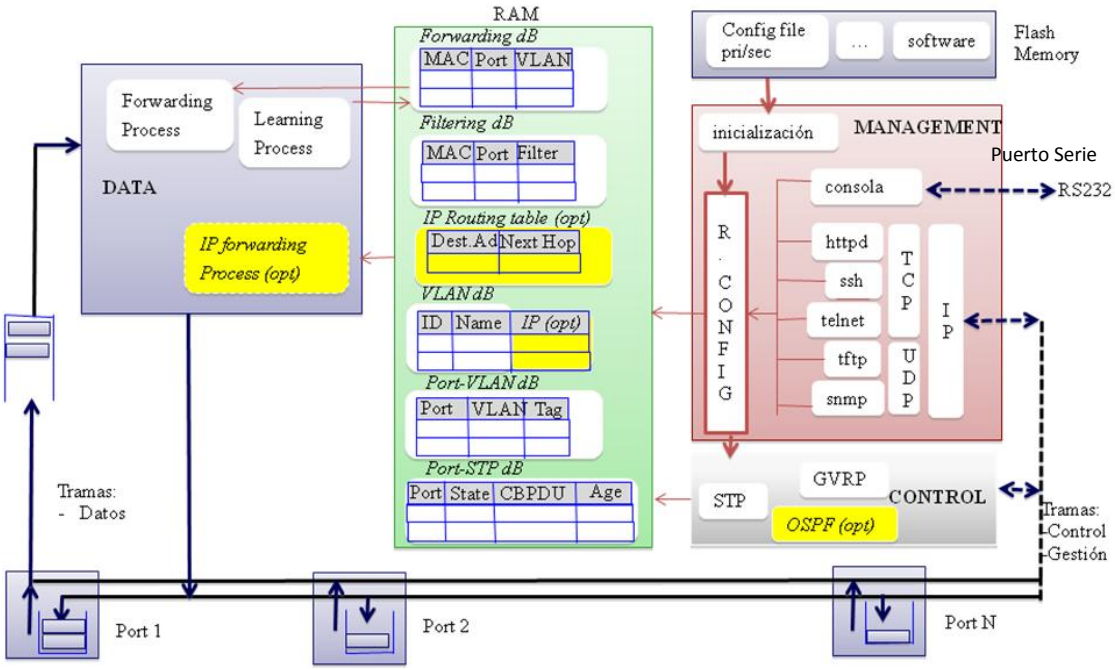
Un *switch* funciona como un ordenador con un hardware especial (muchos adaptadores de red), un sistema operativo propio del fabricante (por ejemplo IOS de Cisco) que ejecuta software para implementar las distintas funcionalidades (802.1D, 802.1p, etc.) en una o varias CPUs. Estas funcionalidades pueden encuadrarse en distintas áreas:

- **Gestión**: permite consultar y alterar la configuración que determina el comportamiento de un conmutador. Se utiliza para fijar parámetros operativos (ejemplo: *Hello time* para STP, velocidad de los puertos), consultar estadísticas (ejemplo: paquetes transmitidos en un puerto) o configurar el funcionamiento de un protocolo en el switch (ejemplo: si queremos ejecutar STP, RSTP o MSTP). El usuario puede acceder a la gestión de diversas formas (consola, telnet, web,…) que veremos con posterioridad
- **Control**: permite la ejecución de protocolos que determinan el comportamiento del reenvío de datos.
- **Reenvío de datos**: ejecutan la funcionalidad básica del conmutador. Suele ejecutarse en una CPU dedicada en exclusiva a esta tarea para conseguir mayor velocidad.

Además de la entidad de reenvío y aprendizaje, existen entidades de capa superior como las que se encargan de STP o de la gestión de propio conmutador.

A nivel de implementación, es habitual que los conmutadores tienen memoria no volátil (NVRAM, Flash,…) para almacenar estructuras de datos y ficheros necesarios para su funcionamiento. En este almacenamiento permanente se guardan los ficheros de configuración y el propio sistema operativo (software) del conmutador.

El siguiente esquema puede resumir el funcionamiento de un conmutador:



En este esquema se omiten gran cantidad de detalles como las distintas colas a la salida de los puertos a favor de la simplicidad. También se presenta como opcional (en color amarillo) la integración de reenvío y encaminamiento IP usual hoy en día en la mayoría de los conmutadores, lo que significa extender su funcionalidad de nivel 2 para ampliarla hasta nivel 3 (IP). Esta característica está disponible sólo en los conmutadores HP 2610 o superiores.

Las diversas CPUs ejecutan los diferentes procesos que forman parte de sistema operativo o software. Una vez lanzado el equipo al mercado resulta habitual que el software mejore conforme se van detectando fallos y anomalías de funcionamiento (algo similar a los parches de los sistemas operativos), por lo que conviene tenerlo actualizado a la última versión disponible.

Como puede ver en el bloque de gestión del esquema general, un conmutador puede disponer de una variedad de formas de acceso para su configuración, la mayoría a través de protocolos de la familia TCP/IP, lo que implica que necesitará configurar una dirección IP de gestión para poder utilizarlos. También existe la alternativa de configurarlo a través del puerto serie (COM) por consola (RS232 en el gráfico anterior).

En los conmutadores que tiene en su puesto de laboratorio dispone de las siguientes opciones:

Desde el puerto Serial del PC:

- Modo consola (puerto serie del switch): Acceso a la línea de comandos (CLI)del conmutador mediante el software *Putty* instalado en su PC conectado por el puerto serie a la consola de configuración del conmutador.

Desde el puerto Ethernet del PC vía torre de protocolos TCP/IP:

- Interfaz web: Mediante un navegador escribiendo **http**://*dirección_IP_de_gestión*
- Telnet / ssh: Mediante *putty* con los protocolos **telnet o ssh** *dirección_ IP_de gestión.* El protocol ssh es similar a *telnet* pero con la ventaja de utilizar técnicas de cifrado que hacen que la información viaje de forma segura.

- SNMP: Empleado en Gestión de Red. No trabajaremos con este modo en las prácticas

Acceso en Modo consola (CLI: Command Line interface)

Utilice el cable especial de consola (DB9/RJ45) que trae el conmutador, conectándolo al puerto serie del PC (conector DB9) y a la entrada de consola del conmutador (consola, a la izquierda). A continuación comuníquese con él abriendo *Putty* en Windows (carpeta Software del Escritorio) con los parámetros

- Comunicación puerto Serial: COM1, 8 bit, Sin Paridad (NO), Control Flujo XoXoff, velocidad: 9600

Tras seleccionarlo espere unos segundos antes de pulsar *Intro* varias veces. Si tiene algún problema puede cambiar la velocidad e intentarlo nuevamente. Recuerde pulsar *Intro* para obtener la respuesta del terminal.

Una vez que el conmutador le haya respondido con el *prompt* (*Nombre_del_switch***#**) podrá comunicarse mediante comandos. **Es muy útil en el modo consola la utilización de las teclas tabulador o ? (función de autocompletar)** que le muestran las posibles opciones a teclear en cada momento, por ejemplo los comandos disponibles, las alternativas, la continuación de la sintaxis del comando que está utilizando o incluso le completan el comando a partir de los caracteres que ya haya escrito, si fuera posible. Se recomienda encarecidamente el uso de este mecanismo.

El *prompt* se forma con el nombre del switch (por defecto o asignado por usted en la configuración) más un símbolo y una palabra clave que le indican en qué nivel se encuentra en su interacción con el conmutador:

- …**#**
  Nivel de gestor (máximo nivel). Para pasar a nivel de configuración global: **configure**
- …**>**
  Nivel de operador (más limitado). Para pasar al nivel de gestor, escribir: **enable**
- … **(*config*) #**
  Nivel de configuración global
- … **(<*contexto*>) #**
  Nivel de configuración asociado al contexto de un comando (por ejemplo puerto, VLAN, etc.)

En cada nivel dispone de opciones diferentes. Puede comprobar que por defecto el conmutador se inicia en el modo de gestor.

Puede comenzar con un vistazo a la lista de comandos disponibles con ***help***, tecla tabulador o ?. En la guía de prácticas usaremos a partir de ahora la convención #***comando*** para indicarle el que debe teclear en cada momento en el modo consola.

Teclee el comando #***show*** y a continuación un espacio y el tabulador o ?, observando sus posibilidades y ejecutando alguna de las órdenes cuya información le resulte familiar.

Pruebe también los comandos #***exit***, #***logout*** junto con #***help*** y observe sus efectos.

Primeros pasos con el modo consola (CLI) :

- Niveles de trabajo

  Muestre de nuevo los comandos disponibles (#***help***, tabulador, ?), a continuación teclee el comando #***exit*** y vuelva a mostrar la lista de comandos. Observe la diferencia en el *prompt* y en las posibilidades que tiene ahora razonando el porqué.

  Revise la nueva lista hasta encontrar un comando que le restaure la situación original con todas sus posibilidades (#***enable***)

- Restauración de los valores de fábrica

  Esto eliminará cualquier configuración previa que pueda provocarle problemas, utilice para ello el comando #***erase startup-config*** (se recomienda su uso cada vez que comience su turno de prácticas). Observe el efecto que tiene sobre el conmutador.

  Con la configuración de fábrica sólo queda definida una VLAN por defecto (DEFAULT_VLAN) y todos los puertos están asignados a ella como *untagged*.

  Compruebe esta situación: relación de VLAN configuradas en el conmutador, su nombre, ID_VLAN, los puertos asignados, la configuración de un puerto concreto y la de todos sus puertos con #***show***.

  Si ha tecleado sólo #***show*** habrá comprobado que se rechaza como incompleto. Como norma general, cuando suceda esto, utilice la función de auto completar con el tabulador para que le muestre las alternativas e incluso le complete automáticamente el término del comando si es posible, también puede usarlo para ir obteniendo la sintaxis correcta que le permita completar el comando.

  Si ha seguido este consejo llegará a comandos como #***show vlans***, #***show vlans 1***, #***show vlans ports 7 detail***. Interprete la información obtenida con el segundo comando.

- Configuración básica del conmutador

  Asigne un nombre a su conmutador y sitúelo en la red 10.10.***i***.0/24 asignándole su una dirección IP y una máscara para el acceso a la pila de gestión del conmutador desde su VLAN. Esta dirección IP le permitirá a usted comunicarse desde su PC con la gestión del conmutador usando protocolos como telnet, ssh o http desde cualquier otro ordenador que tenga conectividad IP con él. En primer lugar verifique la configuración IP del conmutador (#***show ip)*** . Si tiene que cambiarla escriba los comandos #***vlan 1 ip address*** **<**ip> <mask> (puede ayudarse del tabulador o '?' para ver los argumentos y sintaxis de los comandos). Busque el comando que permite cambiarle el nombre al conmutador. Puede verificar los resultados de la configuración realizada con #***show*** (#***show ip***, #***show config***). Tenga en cuenta que los cambios realizados se perderán si reinicia el conmutador.

- Manejo de configuraciones

  El conmutador distingue dos tipos de ficheros de configuración: el que mantiene en memoria no volátil para utilizarlo en el arranque (*startup-config*) y el que mantiene en memoria volátil durante el tiempo de ejecución (*running-config*). Cuando se arranca, el conmutador carga la configuración de inicio (*startup-config*) como configuración actual (*running-config*) y a partir de ese momento todas las modificaciones que vaya

efectuando con, por ejemplo, los comandos de consola quedarán en su configuración actual (*running-config*).

Puede mantener hasta tres ficheros de configuración de arranque distintos para elegir la forma en que se inicia el conmutador. Puede ver la lista con #***show config files***. NOTA: en los conmutadores 2510 tan sólo hay 1 fichero de configuración (startup-config), por lo que no se aplica lo anterior.

Entre en el modo de configuración (#***configure***) y defina una VLAN con ID = 2 denominada G***i***SG***j*** utilizando para ello el conmando #***vlan*** (necesitará consultar el manual para ver la sintaxis del comando o ayudarse con el tabulador). Tras realizarlo vuelva a observar las configuraciones de arranque y actual utilizando los comandos del párrafo anterior para ver cómo han quedado y sus diferencias.

Si el listado fuese más amplio y le resultase tedioso compararlas puede ayudarse de un comando que no le marcará las diferencias pero sí al menos le indicará si son coincidentes o no. Busque este comando partiendo de #***show config***… o #***show running-config***… utilizando el tabulador hasta encontrarlo (# … ***status***). Ejecútelo.

A continuación practicará con algunas de las posibilidades para guardar o recuperar configuraciones:

- Configuración actual (running-config) -> Configuración de arranque (startup-config). Pude pasar su configuración actual a la configuración de arranque mediante #***write memory***. Ejecute el comando y compruebe el resultado cerciorándose de que son coincidentes (#***…status***)

- Configuración actual -> Fichero en disco del PC (con *Xmodem*, protocolo para transmisión y recepción de ficheros mediante el puerto serie COM1)

  Cuando estamos conectados por puerto serie sólo tenemos acceso a la consola. Si quiero enviar un fichero desde mi PC hacia el conmutador o quiero recibir un fichero desde el conmutador a mi PC debo utilizar el comando: #***copy [origen] [destino].*** (tenga en cuenta que usted está ejecutando el rol del conmutador desde *Putty*). El fichero de configuración deberá almacenarlo en su carpeta Grupo*i* en un fichero denominado G***i***SG***j***cfg_1.txt para lo que empleará el comando #***copy …*** (investigue qué opciones presenta este comando con el tabulador). Una vez ejecute la orden **#copy** …. deberá pulsar ENTER y recibir un fichero desde el PC, para lo que tiene que activar el protocolo de transferencia *Xmodem* del *Putty* (seleccionar en el menú superior de la ventana: FileTransfer/Xmodem recibir fichero) e indicar el nombre del fichero. Tenga en cuenta que para el conmutador nuestro PC será Xmodem. El fichero se habrá recibido en el directorio donde se ejecutó Putty (Desktop), por lo que debe moverlo desde allí hasta su directorio de trabajo. Compruebe con el Bloc de notas o con un editor de texto el contenido del fichero recibido, y muévalo al directorio de su grupo Grupoi).

- Modificar fichero en disco del PC -> Configuración de inicio (con XMODEM)

Vamos a hacer modificaciones con el Bloc de notas o con un editor de texto sobre el fichero de configuración guardado en disco en el paso anterior y posteriormente cargarlo en conmutador como configuración de inicio. Por ejemplo abra el fichero G***i***SG***j***cfg_1.txt que almacenó, cambie el nombre del conmutador a "(2530 o *2610)-Gi-SGj_cambiado"* y guárdelo como G***i***SG***j***cfg_2.txt. A continuación cargue este fichero como configuración de inicio en el conmutador, en un fichero denominado config_bis, utilizando el protocolo XMODEM con el comando **#copy** (recuerde que ahora el origen será el PC (xmodem) y el destino su conmutador). NOTA: si está utilizando el conmutador HP2510 tan sólo se permite un fichero de configuración: startup o default config

Compruebe con el comando adecuado que *config_bis* aparece en la lista de los ficheros de arranque disponibles, reinicie el conmutador (#***boot***) y observe si ha tenido éxito en el *prompt* (debería tener el nuevo nombre). Si no es así intente averiguar el porqué.

- Elegir el fichero configuración que se ejecutará al arrancar el conmutador

  Si no ha conseguido resolver la pregunta planteada en el punto anterior introduzca el comando #***startup-default …*** para seleccionar *config_bis* como configuración de inicio ayudándose con el tabulador para completar la sintaxis o con el manual del equipo. Notará que ha resuelto el problema cuando tras un reinicio el conmutador le muestre el *prompt* con el nuevo nombre ("2510(ó 2610)-Gi-SGj_cambiado").
  Observe ahora cómo ha quedado la tabla con los ficheros de configuración de inicio disponibles (#***show config files***)

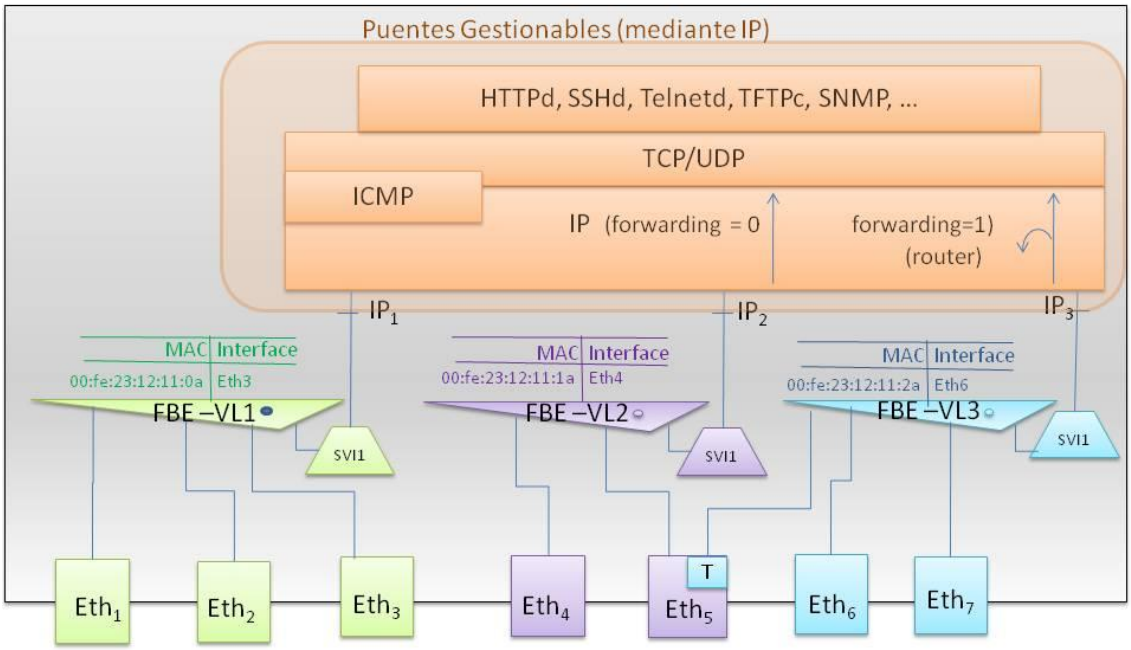
  [**Memoria**] Guarde en disco una imagen de la consola con la tabla de ficheros de configuración disponibles. Debe aparecer el comando utilizado y su resultado.

- Eliminar configuraciones de inicio
  Puede borrar ficheros de configuración con #***erase …***, por ejemplo el último que ha cargado. Inténtelo, si no se lo permite pregúntese por qué y realice los cambios necesarios hasta conseguir que desparezca de la tabla de configuraciones de inicio (compruébelo con el comando adecuado).

Configuración vía IP desde los puertos Ethernet

Ahora utilizaremos a nivel de enlace los puertos Ethernet tanto del PC como del conmutador. Para ello recuerde utilizar el puerto Ethernet del PC con el cable verde.

El esquema de protocolos será:



Donde desde un puerto Ethernet accedemos a diversas aplicaciones y servicios que el conmutador tiene para facilitar su configuración. Para ello debemos asignar una dirección IP al puerto virtual (SVI) que el conmutador crea por cada VLAN con el fin de permitir el acceso al nivel IP. Mediante IP es posible acceder a diversos servicios de configuración en el conmutador: servidor web, servidor ssh, servidor telnet, cliente tftp (para transferir ficheros tanto con la imagen del software del conmutador como con su configuración), o snmp.

Recuerde que la configuración a nivel IP del switch (dirección IP del puerto SVI de la VLAN correspondiente) y del PC (en la interfaz ethernet utilizada) deben pertenecer a la misma subred. Una buena costumbre es verificar la conectividad entre ambos mediante un #ping (se puede ejecutar desde el conmutador o desde el PC con un cmd). Si no hubiera conectividad debemos arreglar el problema de configuración IP antes de seguir.

Acceso al interfaz CLI vía TCP/IP mediante Telnet y SSH.

Una opción desde la red para comunicarse con el conmutador es abrir una sesión *telnet* o *ssh* desde cualquier ordenador que tenga conectividad con él utilizando la dirección IP de gestión que le configuró al conmutador anteriormente (puede verificar la conectividad con el comando *ping*).

Conecte el ordenador a un puerto del conmutador, utilice la aplicación Putty y lance *telnet* o *ssh* a la dirección IP citada (recuerde que ahora estamos utilizando Ethernet como puerto físico en el ordenador y en el conmutador). Si no le responde el conmutador analice el problema con las sugerencias del apartado anterior. Si va a utilizar *ssh* debería primero generar un certificado

en el conmutador: ***(config)#crypto key generate ssh*** , así como habilitar el uso de ssh (en modo CLI por consola puede habilitarlo: #***ip ssh***)

Observará que tiene a su disposición el intérprete de línea de comandos del modo consola (CLI) que ya ha utilizado con anterioridad, pero en esta ocasión las comunicaciones van por TCP/IP. Compruebe con algunos comandos que dispone de la misma funcionalidad y que se ejecutan con normalidad.

Cierre la sesión telnet con el comando #***logout***.

¿Sería posible alterar la configuración del conmutador del otro subgrupo? Inténtelo y, si es posible, ejecute algún comando que modifique su configuración actual.

Acceso mediante Interfaz web (servidor http en el conmutador)

En este punto va a realizar operaciones en el conmutador comunicándose con él a través del protocolo http que utiliza la torre de protocolos TCP/IP, desde cualquier ordenador que tenga conectividad IP con el conmutador, utilizando un navegador para conectarse al servidor *http* que lleva incorporado el conmutador en la dirección IP de gestión que configuró anteriormente y en el puerto TCP 80.

Conecte el PC con un cable de red a cualquier interfaz *ethernet* del conmutador, abra el navegador y teclee la dirección IP que configuró anteriormente para el conmutador: obtendrá la página de inicio para configuración del conmutador. Necesitará tener instalado *java* y tener autorizada la ejecución de JavaScript para la dirección IP de gestión del equipo (Panel de Control/Java/ Seguridad añadir http://10.10.i.j a la lista de excepción de sitios y reabrir el navegador y permitir la ejecución de Javascript)

Si no le aparece la página del conmutador revise su instalación comenzando por la capa física (cable, conexiones, …), LAN (misma VLAN, asignación de puertos, …), red (conectividad a nivel IP con *ping*, …) y si es necesario arranque *Wireshark* y analice las comunicaciones. Esta recomendación le será útil durante todo el período de prácticas para resolver los problemas que se le planteen.

Familiarícese con las distintas pestañas y opciones de configuración moviéndose por ellas, realizando modificaciones y viendo los resultados.

Por ejemplo:

- Vea el estado de todos los puertos y sus características (*Status*)
- Deshabilite los puertos 10, 15 y 20 (*Configuration->Device View*)
- Cambie el cable de conexión al puerto 10 y compruebe que no responde, vuelva al puerto original
- Configure los puertos 18 como *half-dúplex* a 10 Mb/s y 19 como *full-dúplex* a 100 Mb/s con control de flujo (*… ->Port Configuration*)
- Cree las VLANsG***i***SG***j***-A y G***i***SG***j***-B (*… ->VLAN Configuration*)

- Asigne los puertos 6 (*untagged*) y 7 (*tagged*) a la VLAN G***i***SG***j***-A (*… ->VLAN Configuration*)

[**Memoria**] Guarde en disco el fichero con la configuración actual y la pantalla obtenida con *Diagnostics-ConfigurationReport*.

Ejercicios para practicar

Ha visto que existen varias formas de gestionar el conmutador, si bien la más completa y la que le permite cualquier tipo de operación es el modo CLI (*Command Line interface*) accesible mediante consola, telnet o ssh. Para que se familiarice con una serie de opciones y comandos útiles para trabajar con el conmutador lleve a cabo los siguientes ejercicios:

- Primeros pasos: configurando VLANs

  Una los dos conmutadores con un cable Ethernet a través de los puertos Gigabit y lancen un *ping* desde el ordenador de un subgrupo al del otro. Si no vuelve el eco analicen el problema con las recomendaciones habituales hasta conseguir un resultado positivo.

  Dibujen sobre el papel un pequeño esquema donde se muestre el escenario con los dos ordenadores y los dos conmutadores conectados, anotando los puertos utilizados y las direcciones IP de cada entidad alcanzable (no se olvide de las direcciones de gestión de los conmutadores).

  Lance un ping desde cada ordenador al resto de direcciones IP del escenario, confirmando que son alcanzables (si no fuera así estudie y resuelva el problema) y a continuación obtenga la tabla de reenvío de cada conmutador con el resultado de lo que ha aprendido (#***show mac-address***).Observe el resto de posibilidades del comando.

  Obtenga las direcciones MAC de los ordenadores y compruebe que el aprendizaje ha sido el correcto en los puertos utilizados. Aproveche también para comprobar las tablas de *arp* de los ordenadores (desde la consola cmd ***arp –a***).

  [**Memoria**] Guarde las tablas de reenvío de los conmutadores, las tablas de ARP de los ordenadores y el resultado del ping. Explique los resultados obtenidos

- Actualizar el software del conmutador

  El conmutador funciona con un software que carga en el arranque y que se puede elegir de entre dos imágenes que tiene almacenadas (primaria y secundaria), esto permite tener una misma versión de software de manera redundante (por si una imagen se corrompe) o instalar una nueva y probarla manteniendo la alternativa de volver a la versión previa en caso de necesidad. Dado que los fabricantes actualizan el software periódicamente conviene saber actualizar dicho software.

  En primer lugar identifique las imágenes que tiene instaladas y con cuál está funcionando en la actualidad con los comandos #***show flash*** y #***show version***

Puede cambiar el arranque con la otra imagen utilizando #***boot system flash***, hágalo y vuelva a comprobar la imagen con la que está funcionando el conmutador.
En segundo lugar consulte las versiones disponibles en la web del fabricante (https://h10145.www1.hpe.com/support/SupportLookUp.aspx)
Recuerde que debe permitir la ejecución de *JavaScript* para dicho servidor (Panel de Control/Java/Seguridad). Se recomienda buscar por el modelo (2510, 2530, 2610, …) y luego elegir de la lista el modelo exacto (puede leerlo en el conmutador):

- 2510-24 J9019B
- 2540-24 J9782A
- 2610-24 J9085A

Tras descargar la imagen con el software que desea, debe pasarla al switch. Para ello dispone de varias opciones: Xmodem (protocolo de transferencia mediante puerto serie, muy lento) o vía IP mediante Interfaz Web o mediante TFTP. Investigue en la interfaz web cómo puede descargar la imagen (no es necesario actualizarla).

[**Memoria**] Guarde la pantalla de consola (comando y resultado) con la información de las imágenes que tiene ahora el conmutador y la que está en activo en el arranque. Guarde también la pantalla de la interfaz web con la opción que permite actualizar la imagen software del conmutador.

Práctica 2: Configuración básica de conmutadores

A partir de ahora se considera que usted se ha familiarizado lo suficiente con el manejo de los conmutadores como para que sólo se le describa el ejercicio a realizar y se le dé una referencia a los comandos que puede utilizar cuando sean desconocidos, formando parte de la práctica la búsqueda de la información necesaria (manual del fabricante o ayuda en la línea de comandos) para completarlos con la sintaxis adecuada.

Conecte los ordenadores a los conmutadores a través de su **cable de consola**.

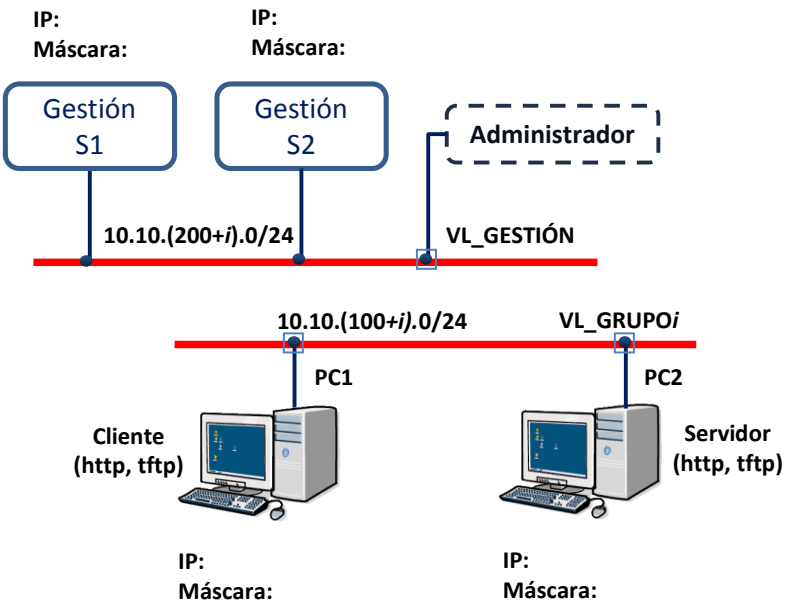
Como cada vez que comienza su trabajo en el laboratorio debe restaurar los valores de fábrica en los conmutadores con el comando que ya conoce para dejarlos con la configuración por defecto. Como ya sabe, todos los puertos quedarán asignados “sin etiquetar” (*untagged*) a una única VLAN por defecto(ID = 1, *DEFAULT_VLAN*), el conmutador tendrá un nombre también por defecto (*ProCurveSwitch 2510-24 ó 2610-24*) y carecerá de una dirección IP de gestión. Utilice **#*show config***, **#*show vlans***, **#*show vlans 1***.

Por el momento sólo debe dar un nombre a su conmutador:

- Nombre: (ejemplo:_ 2510(ó 2610)-G***i***-SG***j***)

VLANs de gestión y de usuarios

El ejercicio consiste en reproducir el escenario de la figura:



En el esquema anterior se distinguen dos tipos de puertos o interfaces de conexión: los señalados con un círculo y un cuadrado, que indican interfaces Ethernet físicas de un conmutador, y los señalados con un círculo, puertos 'virtuales' (SVI) creados en el propio conmutador por cada VLAN para acceder a su pila de protocolos TCP/IP interna con el fin de facilitar la gestión desde la red mediante ssh, telnet, web,… Los puertos SVI se crean de forma automática al asignar una dirección IP de gestión en una vlan determinada (ver figura página 11) y permiten al conmutador reconocer cuándo un paquete va para otro destino en la misma VLAN (envío a la función de bridging) o si debe ser enviado al protocolo IP. Existe un mapeo 1 a 1 entre la VLAN y el SVI correspondiente. Las ventajas de SVI son:

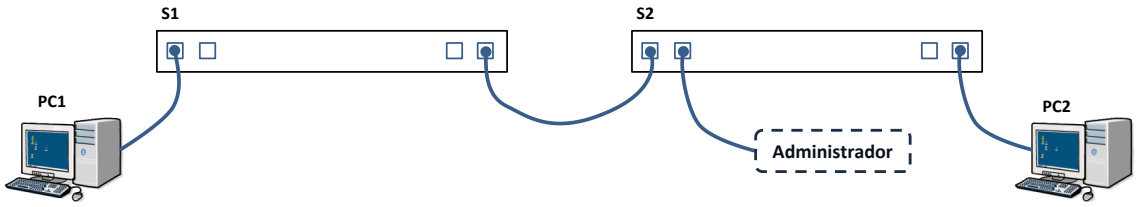
- permiten configurar el dispositivo desde cualquier equipo de la red con conectividad IP.

- si el conmutador dispone en su capa de red IP la posibilidad de reenviar paquetes IP entre las interfaces SVI (IP forwarding) se puede encaminar el tráfico entre VLANs (default Gateway para esa VLAN), sin necesidad de un router externo. Adicionalmente permite implementar por ejemplo listas de acceso (ACL) para filtrar paquetes (firewall básico)

Con respecto a la dirección MAC asignada a los interfaces SVI, cabe señalar que depende del implementador. En muchos fabricantes por defecto un conmutador trae una dirección MAC que asigna a todos las interfaces SVI (como cada interfaz SVI está en una VLAN distinta lo anterior no debería ser un problema). Hay equipos que permiten configurar direcciones MAC diferentes para cada SVI (comando mac-address). En otros casos se utiliza una dirección MAC base para los SVI(s) e incrementan en 1 para cada interface. Por ejemplo: la dirección MAC base para los SVI(s) en a VLAN1 es: 000d.bd43.6800 el primer interface (fa0/1) tendrán la 000d.bd43.6801, el segundo la 000d.bd43.6802.

Conecte cada ordenador (PC*j*) a un conmutador (S*j*) por un puerto 10/100-BaseT y los conmutadores entre sí por puertos 10/100/1000-BaseT.Puede serle de ayuda el contar con un

esquema como el siguiente en donde anotar el número del puerto que está usando, la VLAN a la que pertenece y su situación como "etiquetado" o "sin etiquetar"(*tagged/untagged*) que corresponda en cada caso.



Cree dos VLANs basadas en puertos:

- VL_GRUPO***i*** (ID = 100+***i***)
- VL_GESTIÓN (ID = 200+***i***)

La primera va a dar servicio a los usuarios (PC1 y PC2) y la segunda servirá para aislar la gestión de los conmutadores de forma que no esté accesible desde los puertos de usuario y sólo sea posible desde un único puerto que configuraremos en uno de los dos conmutadores para el acceso del administrador de la red.

Deberá realizar las actuaciones que sean necesarias en los ordenadores (PC1 y PC2) y en los conmutadores (S1 y S2). Esto último se le aconseja hacerlo desde el modo de configuración (#***configure***) desde línea de comandos (CLI), que tiene acceso completo a todos los elementos de configuración:

- Creación de las dos VLANs (#***vlan …***)
  (En cualquier momento puede mostrar las VLANs que tiene con #***show vlans***)
- Asignación de direcciones IP y máscara a los ordenadores
- Asignación de direcciones IP y máscara a los conmutadores S1 y S2 para gestión (#***vlan*** *ID_de_la_VLAN* ***ip*** …) –recuerde que esto crea un puerto 'virtual' en la vlan correspondiente del conmutador que permite acceder a la gestión mediante la torre de protocolos TCP/IP-
  (En cualquier momento puede mostrar las direcciones IP asignadas con #***show ip***)
- Configuración de los cinco puertos (#***vlan*** *ID_de_la_VLAN* ***untagged|tagged*** …)
  - 2 de usuario, uno en cada conmutador S1 y S2, los que decida usar
  - 1 de administrador (puerto 24 en S2)
  - 2 para la unión entre los conmutadores, los que decida usar

  (En cualquier momento puede mostrar los puertos de cada VLAN con #***show vlans*** *ID_de_la_VLAN*)
- Extraiga los cinco puertos que va a usar de la DEFAULT_VLAN (#***no vlan*** *ID_de_la_VLAN* ***untagged|tagged*** …)

Preste mucha atención a los requisitos de "etiquetado/sin etiquetar" (*tagged/untagged*) decidiendo cuál debe usar en cada puerto según sea el caso.

Confirme el correcto funcionamiento de la configuración mediante *ping* entre PC1 y PC2, *ping* entre S1 y S2 y la falta de conectividad de cualquier PC1/PC2 con S1/S2.

Ahora re-utilice uno de los PC1 o PC2 como administrador y abra dos sesiones *telnet* simultáneas, usando sendas consolas de Windows, con S1 y S2 desde uno de los dos ordenadores que conectará al puerto 24 de S2 (tenga en cuenta que necesitará retocar momentáneamente la configuración IP del ordenador que vaya a utilizar como Administrador). Confirme el acceso a los conmutadores desde las sesiones de *telnet* con la ejecución de los comandos ***#show ip***, ***#show vlans***, ***#show vlans*** *VL*_GESTIÓN (o ID_*VL_GESTIÓN*), ***#show vlans*** *VL_GRUPO**i*** (o *ID_VL_GRUPO**i***) y ***#show vlans*** DEFAULT_VLAN (o *ID_DEFAULT_VLAN*).

Muestre en la pantalla la configuración actual (*running-config*) y vea cómo han quedado en él las órdenes de configuración que ha ido introduciendo.

[**Memoria**] Guarde las pantallas de las sesiones de *telnet* con todos los comandos ***#show …*** anteriores, la configuración IP de los ordenadores y los resultados de los *ping* PC1-PC2 y S1-S2.

Pruebas de tasa media o caudal (servicios http y tftp)

En este ejercicio va a utilizar el escenario del apartado anterior con el mismo conexionado y configuración: los dos ordenadores conectados a la VLAN de usuarios (*VL_GRUPO**i***) en los puertos habilitados y con direcciones IP coherentes con la dirección de red. Compruebe la conectividad entre ambos PC's con un *ping* entre PC1 y PC2.

Se trata de medir el rendimiento de los protocolos *http* y *tftp*, para lo que necesitará configurar un ordenador como cliente (C) y el otro como servidor (S) utilizando las aplicaciones que se le proporcionan en el PC para el rol cliente y server respectivamente. En este ejercicio va a descargar desde el cliente http y desde el cliente TFTP el fichero *vanGogh.jpg* a fin de comparar los resultados.

Instrucciones para el uso de las aplicaciones:

- Servidor *http* (*MiniWeb*)

  Se debe iniciar desde el enlace directo que existe en el escritorio. Tras ejecutarse el acceso abre un cmd donde se indica la dirección IP y puerto TCP (por defecto 8000) donde está escuchando el servidor, mostrando un log con las peticiones recibidas. Una vez arrancado el servidor, queda a la espera de peticiones *http* y tiene habilitado por defecto como directorio raíz la carpeta *Default_HTTP* del escritorio contiene los ficheros que serán servidos. Puede verificar que el servidor *http* está activo lanzando desde el navegador una petición a la dirección local (http://127.0.0.1:8000). Para detener el servidor basta presionar CTRL+c. o cerrar la cmd.

- Cliente *http*(*wget*)

  Se inicia desde la consola de comandos que puede abrir desde el acceso directo del escritorio. Tras ello hay que situarse en el directorio que ha creado para su grupo (comando **cd**) y ejecutar wget. Para descargar un recurso (fichero) se utiliza la sintaxis *wget URL -P directorio_destino*, que en su caso se traducirá en:

  wget *dir_IP_Servidor:8000/nombre_fichero.jpg -P carpeta_destino*

- Servidor *tftp* (*Open TFTP Server Multithreaded*)

  Se ejecuta desde el enlace directo en el Escritorio (Servidor_tftp): abre un cmd que indica la(s) dirección(es) IP y puerto UDP (por defecto 69) donde está a la escucha de peticiones, mostrando un log con las recibidas. Para detener el servidor se presiona CTRL+c o se cierra el cmd. Por defecto el servidor estará a la escucha en el puerto UDP 69 en todas las interfaces de red y el directorio raíz será: *Default_TFTP* ubicado en el Escritorio y que contiene los ficheros que podrán ser servidos.

  Para verificar el funcionamiento del servidor puede: a) observar la salida de la ejecución del servidor en el cmd b) verificar con netstat –a que existe un proceso escuchando en el puerto UDP 69 c) abrir un cliente tftp y descargar algún fichero en local.

- Cliente *tftp*

  Se inicia desde la consola de comandos (hay que situarse en el directorio Escritorio/GruposRRMS/Grupo_i). Para descargar un fichero del servidor se utiliza la sintaxis *tftp -i dir_IP_Servidor GET nombre_fichero directorio_destino**nombre_fichero*, que en su caso se traducirá en:

  tftp *-i dir_IP_Servidor GET nombre_fichero.jpg carpeta_destino*\ *nombre_fichero.jpg*

  Escriba tftp –help para ver las distintas opciones. Por ejemplo puede probar:

  tftp -i 127.0.0.1:69 GET anochecer.jpg

  investigue cómo se cambia el tamaño de los bloques transferidos.

Descargue el fichero *vanGogh.jpg* (34 MB) desde el servidor utilizando el protocolo *http* y, a continuación, con el protocolo *tftp*. Observe que los clientes *http* y *tftp* usados le proporcionan el dato del tiempo de descarga, deberá anotarlo para calcular la tasa media o caudal de que ha dispuesto la aplicación.

[**Memoria**] Explique si existen diferencias de tiempo al usar uno u otro protocolo y la causa que las motiva, tanto teórica como práctica sobre la base de datos obtenidos de las pruebas (número de paquetes, longitud de los paquetes, etc.). Ayúdese en su justificación con información obtenida mediante *Wireshark*.

Realice las descargas con los enlaces entre los conmutadores a distintas velocidades, para lo que deberá usted configurar el puerto desde la línea de comandos entrando en configuración (#***configure***) y usando #***interface*** *nº_puerto* ***speed-duplex*** ....

Configure y descargue el fichero (*http* y *tftp*) con el enlace a:

- 1 Gb/s (tendrá los datos del experimento anterior)
- 100 Mb/s
- 10 Mb/s

[**Memoria**] Realice un cuadro con los tiempos y la tasa media obtenidos para cada velocidad del enlace y protocolo. Explique los resultados ayudándose de información obtenida con wireshark.

Tras los análisis y conclusiones anteriores realice la misma "descarga" internamente en el ordenador (cliente y servidor en la misma máquina) lanzando la petición del cliente a la dirección local 127.0.0.1 donde está el servidor. Anote los tiempos de "descarga" y calcule la "tasa media de descarga".

[**Memoria**] Explique si estos últimos resultados modifican en algo las conclusiones que redactó tras los experimentos de descarga entre ordenadores usando la red del escenario (acaba de obtener una nueva referencia de tiempos que puede serle de utilidad para ello).

STP y RSTP

En este ejercicio va a utilizar el escenario del apartado 5.1 con el mismo conexionado y configuración que guardó en fichero.

Recupere el escenario original con los dos ordenadores conectados a la VLAN de usuarios (*VL_GRUPOi*) en los puertos habilitados y con direcciones IP coherentes con la dirección de red. Compruebe la conectividad con un *ping* entre PC1 y PC2.

Deshabilite el protocolo Spanning Tree (**(config)# spanning-tree disable**) y enlace los conmutadores con un segundo latiguillo empleando puertos 10/100/1000Base-T. En este nuevo escenario la topología física de la red ha formado un bucle (recuerde que el protocolo STP debe estar desactivado). Lance un *ping* de PC1 a PC2 que deberá de recibir eco. Observe los *leds* de los puertos de los conmutadores, le darán una indicación a simple vista de actividad en la red. Lance un ping de PC1 a una dirección del misma subred que PC2 pero diferente a la asociada a PC2 y observe el resultado. ¿cuáles son los efectos del bucle en los conmutadores y en los PC's?

A continuación quite uno de los dos cables que unen ambos conmutadores para eliminar el bucle. Entre el modo configuración (**#*configure***) y habilite *spanning-tree* en los conmutadores con **#*spanning-tree*** para definir la versión (STP, RSTP o MSTP) que quiere utilizar. Si tiene problemas de comunicación con el conmutador desconecte previamente el segundo enlace y conéctelo tras habilitarlo. Empezaremos con el protocolo STP (**#*spannig-treeforce-versionstp-compatible*** fuerza la versión STP) comprobando que ha quedado correctamente configurado con **#*show*** … Una vez configurado STP en ambos conmutadores vuelva a conectar físicamente un bucle entre ellos y lance los pings anteriores.

a. Identifique cuál es el conmutador raíz y el estado en que han quedado los puertos que está usando en su escenario (**#*show spanning-tree***).

b. Compruebe el tráfico de CBPDUs que recibe por la interfaz de su ordenador con *Wireshark*, analice una de ellas identificando los parámetros que ya conoce (*Root_ID*, *Bridge_ID*, …) y compruebe si dicho tráfico es coherente con el parámetro *Hello Time* que transporta. Desconecte y vuelva a conectar el enlace activo mientras captura las tramas.

Nota: Los conmutadores le permiten observar lo que sucede en un puerto desde otro utilizando la opción de "*portmirroring*" de manera que puede definir un puerto como espejo (*mirror*) al cual se envía una copia de todas las tramas que se presenten en otro u otros puertos a monitorizar. El comando empleado es **#*mirror-port*** *nº_de_puerto* (puerto donde se va a recibir una copia de las tramas) e **#*interface*** *nº_de_puerto* ***monitor*** (puerto o lista de puertos bajo observación). Para comprobar si la configuración ha sido la deseada puede utilizar **#*show monitor***. Utilice este mecanismo para monitorizar en su ordenador con Wireshark el tráfico de CBPDUs STP en un puerto del enlace entre conmutadores repitiendo el experimento del punto descrito en párrafos anteriores.

[**Memoria**] Indique la trama CBPDU entre conmutadores capturada con mirror-port.

Tablas de reenvío y ARP

Para terminar la práctica se le propone un sencillo ejercicio teórico-práctico en el que se evaluará su conocimiento sobre el funcionamiento de los conmutadores partiendo del escenario más simple posible.

Restaure los valores de fábrica y dé nombre a su conmutador:

- Nombre: 2510(ó 2610)-G***i***-SG***j***

Conecte cada ordenador a una interfaz de un conmutador (cada PC a un conmutador diferente) y los conmutadores entre sí con un único latiguillo. Si los ordenadores conservan direcciones IP de la misma subred debería de funcionar el *ping* de uno a otro (DEFAULT_VLAN). Compruébelo, y si no es así corrija las configuraciones de los ordenadores hasta que funcione el *ping*.

Se recomienda anotar los últimos dígitos hexadecimales de las tarjetas de red de los ordenadores para poder identificarlas en las tablas de reenvío de los conmutadores. Obtenga esas tablas y confirme que han aprendido correctamente las direcciones.

A partir de ahora utilice un solo ordenador (PC1) donde tendrá que tener abiertas dos ventanas de consola, desde una se lanzará un *ping* continuo y observará el resultado, desde la otra introducirá alguna orden cuando se le indique.

Lleve a cabo los siguientes pasos:

1) Lance un *ping* continuo (***ping –t***) desde un ordenador (PC1) al otro (PC2) y manténgalo durante todo el ejercicio. Compruebe que recibe la secuencia de respuestas (eco)

2) Desconecte el segundo ordenador (PC2) del puerto del conmutador, manténgalo así unos segundos y compruebe que ha dejado de recibir respuestas de eco. Conéctelo de nuevo y compruebe que se reanuda la recepción del eco
3) Desconecte PC2 del conmutador al que estaba conectado, espere unos segundos comprobando que ha dejado de recibir el eco y conéctelo a un puerto del otro conmutador donde está conectado PC1.

En teoría el conmutador debería seguir enviándolo al otro conmutador, pues la entrada debería estar en la tabla de reenvío...

[**Memoria**] Explique por qué llega el ping (puede ayudarse de wireshark). En ambas respuestas aporte los datos obtenidos de los conmutadores o del ordenador que los respalde.

Práctica 3: Configuración avanzada de conmutadores

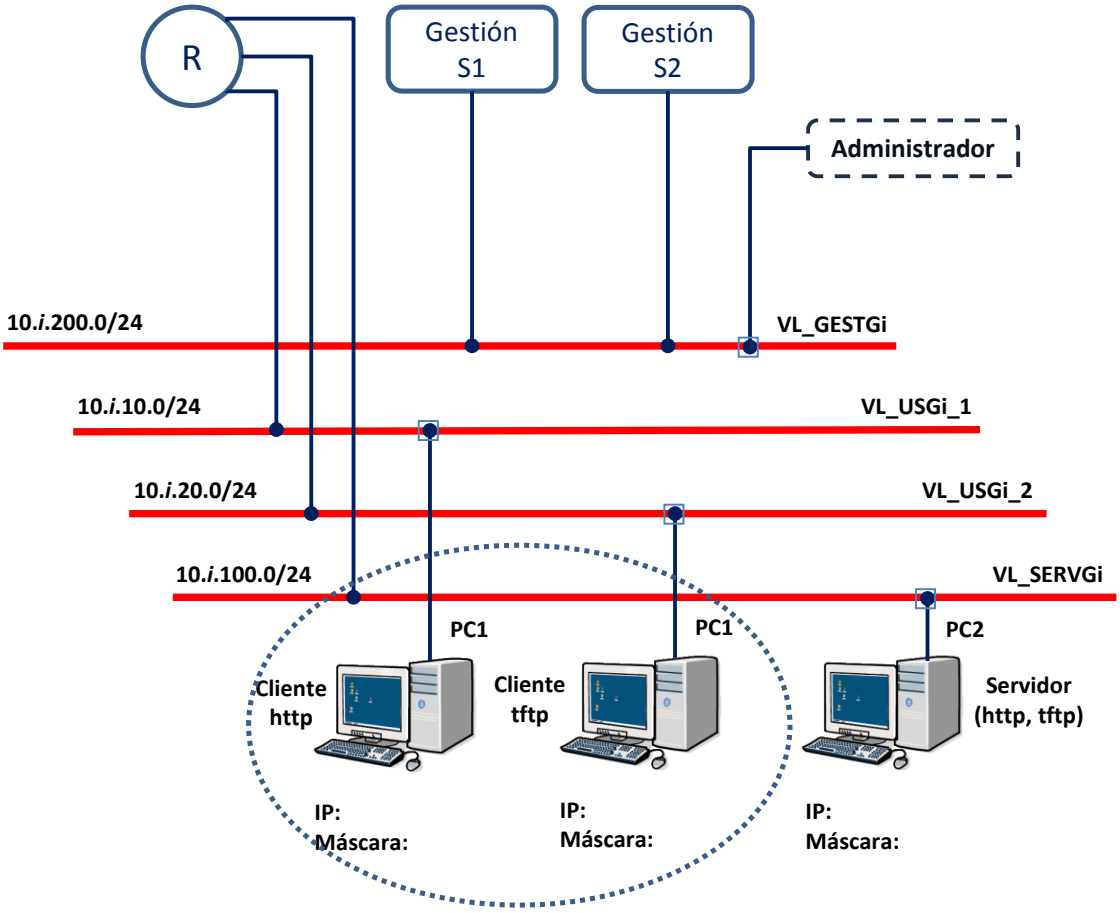
Conecte los ordenadores a los conmutadores a través de su cable de consola restaure los valores de fábrica con el comando que ya conoce para dejarlos limpios.

Por el momento sólo debe dar un nombre a su conmutador:

- Nombre: 2510(ó 2610)-G***i***-SG***j***

Escenario complejo

El ejercicio consiste en reproducir el siguiente escenario con varias subredes IP y VLANs:



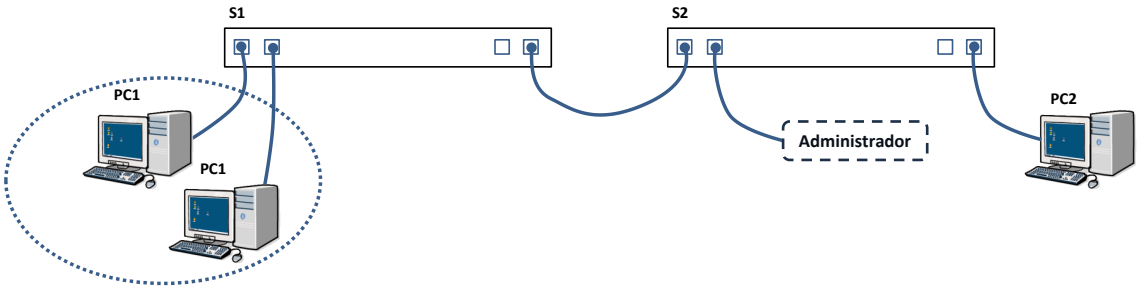
Se puede apreciar lo siguiente:

- 2 VLANs para usuarios de dos tipos (clientes *http* y clientes *tftp*)
- 1 VLAN para servidores (*http* y *tftp*)
- 1 VLAN de gestión aislada
- *Router* para encaminar de una VLAN a otra

Puesto que cada grupo sólo dispone de 2 ordenadores utilizará uno de ellos (PC2) como servidor y el otro (PC1) como cliente, conectándolo alternativamente a una u otra VLAN de usuario según el ejercicio que se lleve a cabo.

Para enrutar los paquetes entre subredes utilizará la función de *routing* disponible en el conmutador HP-2610 o HP-2630 según se le indicará. Esta función encamina en el nivel IP del conmutador entre las distintas interfaces virtuales SVI asociadas a las diferentes VLANs.

La conexión a los distintos conmutadores se realizará como indica la figura, cambiando de puerto a PC1 cuando sea necesario. Los ordenadores (PC***j***) se conectarán al conmutador (S***j***) por un puerto 10/100-BaseT y los conmutadores entre sí por puertos 10/100/1000-BaseT.



Creación de VLANs

Por el momento omita la parte del escenario relativa al *router* R, la utilizará más adelante.

Cree las VLANs del escenario con ID=10 para UsG***i***_1, ID=20 para UsG***i***_2, ID=100 para ServG***i*** e ID=200 para GestG***i*** y realice la asignación de puertos a VLAN que necesite actuando sobre ambos conmutadores de forma que los clientes estén en puertos de S1 y el servidor en un puerto de S2. El puerto del administrador será el 24 del conmutador S2 donde se sitúa el servidor.

No se olvide de dar visibilidad a los conmutadores en la VLAN de gestión y de configurar los ordenadores situándolos en la subred que corresponda (PC1 puede ubicarlo de momento en la subred de UsG***i***_1).

Tampoco se olvide extraer de la DEFAULT_VLAN los puertos utilizados, eliminando su pertenencia a ella.

Conmutadores L2/L3 (función de *routing*)

Para poder comunicar equipos situados en subredes distintas se precisa de una función de enrutamiento en capa IP, la cual se lleva a cabo en equipos intermedios denominados enrutadores o *routers*. Los conmutadores trabajan a nivel 2, por lo que no realizan esta función. Sin embargo, hoy en día es frecuente que en conmutadores de gama media ya se incorpore esta capacidad de enrutamiento de capa IP que puede activarse mediante comandos de configuración. En estos casos es habitual utilizar la denominación de conmutadores L2/L3 y su grupo dispone de al menos uno con estas características: el HP-2610 (y el HP2630). Puede ayudarse del esquema de la pagina 11 para entender el funcionamiento de estos equipos,

donde sobre dicho esquema se activa la funcionalidad de reenvío IP (IP forwarding) entre las interfaces SVI. Se comportará, por tanto, como un router que será utilizado por los PC de cada una de las VLANs para encaminar el tráfico.

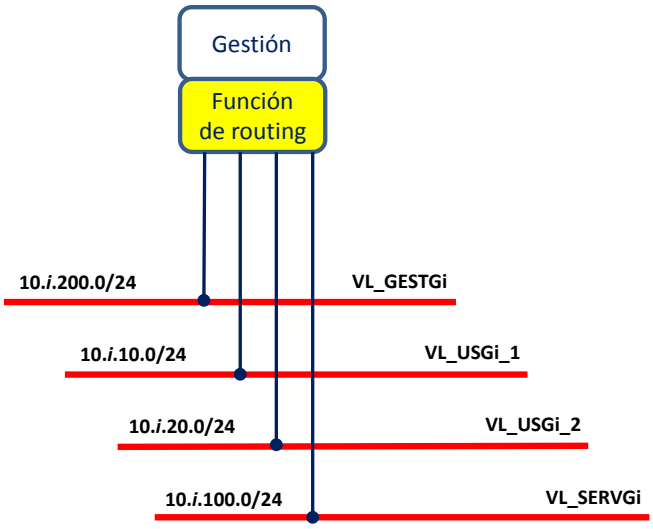
Para aquellos grupos que tengan 2 conmutadores 26x0 deben utilizar solamente uno de ellos con su funcionalidad L2/L3 (*routing*), el otro deberán usarlo sólo como conmutador (sin *routing*).

Tras la restauración de los valores de fábrica el conmutador 2610 queda con la función de *routing* deshabilitada. Compruébelo con **#show ip**, actívela (sólo en uno de los 2610) con ***#ip routing*** y vuelva a comprobar su estado con ***#show ip***.

Esta función de *routing* va a estar representada en el escenario por la entidad R, la cual necesita, como es lógico, disponer de interfaces en cada una de las subredes para poder enrutar paquetes entre ellas.

La creación de estas interfaces 'virtuales' se realiza de la misma forma que cuando se crea una interfaz IP para acceder a los sistemas Gestión del Conmutador (por web, telnet, ssh,…): con ***#vlan*** *ID_VLAN* ***ip address*** …, siendo ID_VLAN la VLAN en la que desea crear la interfaz IP del *router*.

Cree las interfaces que necesite la función de *routing* en el conmutador 2610 (sólo en 1 si su grupo dispone de 2) según el escenario del punto anterior y muestre la situación final de configuración de los dos conmutadores con ***#show vlans*** y ***#show ip***. Aunque puede asignar la dirección IP que desee dentro de la subred, es común elegir la terminada en .1, por ejemplo 10.***i***.10.1 para la interfaz conectada a VL_UsG***i***_1. El esquema de funcionamiento en el conmutador 2610 cuando se habilita la función de *routing* sería el siguiente:



Recomendación: es muy aconsejable que anote en la figura del escenario las direcciones IP y las máscaras asignadas a cada interfaz (R, gestión, PCs, administrador), le ayudará en gran medida.

Aún le falta un detalle para conseguir el funcionamiento completo y es definir para PC1 y PC2 la puerta de enlace predeterminada o *gateway*, que será la dirección IP asignada a la interfaz virtual SVI de la VLAN correspondiente que acaba de crear en el conmutador L2/L3.

Compruebe mediante *ping* que ha conseguido reproducir el escenario y tener conectividad entre PC1 (sitúelo tanto en la subred de UsG***i***_1 como de UsG***i***_2) y PC2. Si no tiene éxito en las pruebas de conectividad, intente averiguar el motivo capturando tramas con wireshark para ayudar a discriminar si el error está en los conmutadores o en los PC. Si fuera en los PC debería revisar la tabla de encaminamiento e introducir en ella las entradas que estime oportunas.

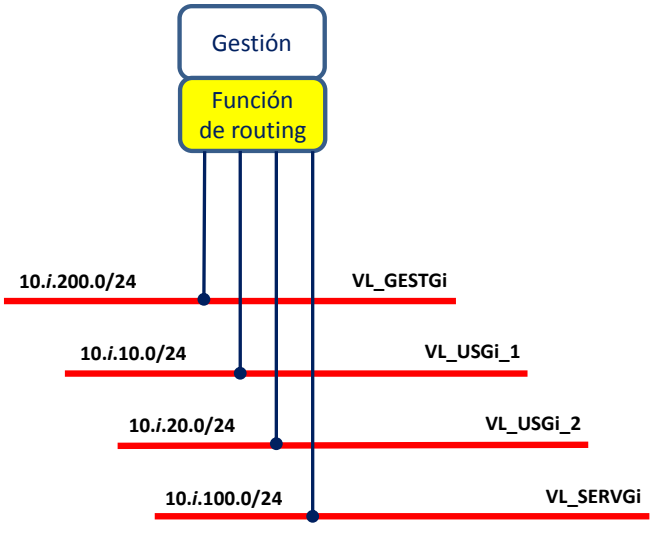
Una vez conseguida la conectividad con ping, compruebe con las aplicaciones cliente y servidor de que dispone en la carpeta *Software* que PC1 puede descargar el fichero Van*Gogh.jpg* tanto a través de la VLAN VL_UsG***i***_1 como de VL_UsG***i***_2, con protocolo *http o tftp (en tal caso el ficher es VanGogh2.jpg)*.

[**Memoria**] Registre la configuración de los dos PC y los dos conmutadores en donde se muestren las VLANs, la asignación de puertos (*tagged*/*untagged*) y las interfaces IP disponibles en el conmutador.

VLAN de gestión (sin enrutar)

Desde cualquier ordenador PC1 o PC2, conectados al puerto configurado para la VLAN que les corresponda, intente abrir una sesión de *telnet* con cualquier dirección IP asignada a la función de *routing* o al bloque de gestión, verá que se acepta y que, por lo tanto, podría gestionar los conmutadores desde una estación conectada a cualquier puerto que esté asignado a una cualquiera de las 4 VLANs del escenario. Esta situación no consigue aislar la VLAN de gestión y habilitarla sólo desde el puerto 24 de S2.

El problema surge en cómo entiende el 2610 las interfaces que se le han creado y que se muestra esquemáticamente en la figura; al fin y al cabo VL_GestG***i*** no es más que otra VLAN, creada con una intención diferente a las demás, aunque no ha sido posible dado que todas las interfaces IP del conmutador están accesibles tanto para la función de *routing* como para la de gestión.

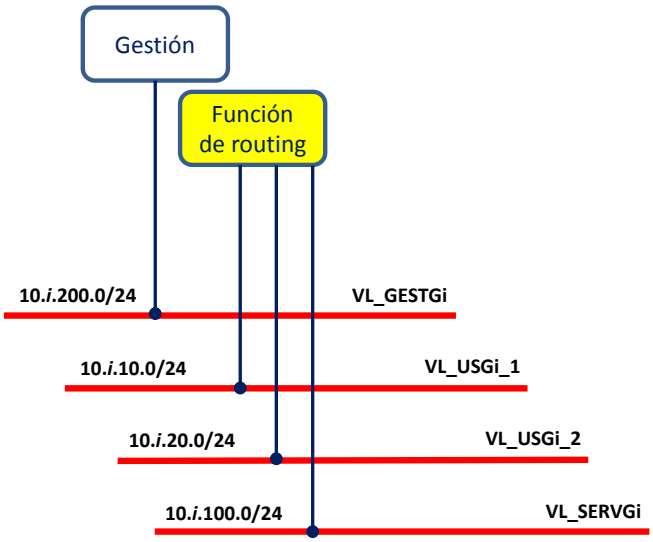


La solución la proporciona un comando de configuración: #***management-vlan****VLAN_ID* que permite definir una VLAN (la de VLAN_ID) como de gestión, aislándola de función de *routing* y evitando que puedan enrutarse paquetes con destino a VLAN. Con ello queda aislada del resto de VLANs y se habrá conseguido el objetivo.

Utilice el comando citado y compruebe mediante *ping* que ya no es posible alcanzar la gestión de los conmutadores salvo por el equipo situado en el puerto 24. Compruebe que es posible gestionarlos desde ese puerto con sendas sesiones de *telnet* simultáneas.

[Memoria] Especifique el fichero de configuración de los dos conmutadores. Guarde la configuración para futuras prácticas.

La figura muestra el cambio de situación que origina el comando.



Agregación de enlaces

Como ha comprobado, si conecta los dos conmutadores con un segundo latiguillo por los puertos 10/100/1000-BaseT se forma un bucle que hay que eliminar activando el protocolo STP o RSTP, el cual bloqueará uno de los puertos e impedirá que un enlace curse tráfico, lo que a su vez elimina la posibilidad de incrementar la capacidad del enlace entre los conmutadores.

La solución la proporciona el protocolo LACP que permite la agregación de enlaces.

En primer lugar habilite *spanning-tree* en su versión RSTP con los comandos que ya conoce, a continuación conecte el segundo latiguillo entre conmutadores en la forma descrita en el párrafo anterior. Compruebe con el comando adecuado que un puerto ha pasado al estado de *Blocking*.

Configure los puertos de los dos enlaces entre conmutadores a 10 Mb/s, para ello basta con actuar en uno de ellos configurando su velocidad en a*uto-10* (***#interface 25,26 speed-duplex auto-10***) lo que provocará una negociación y el otro se adaptará a ella. Compruebe que ha tenido efecto con ***#show interfaces brief 25,26*** en ambos conmutadores, asegurándose de que quedan trabajando en modo *full-dúplex* a 10 Mb/s. Si tuviera algún problema con el comando

de configuración fuerce manualmente el modo de funcionamiento a *10-full* en ambos conmutadores.

Descargue el fichero *VanGogh.jpg* con el protocolo *http* anotando los tiempos de descarga y la tasa media.

Cree un enlace agregado o "trunk" estático denominado *trk1* (también existe la posibilidad de crearlo dinámico) con protocolo LACP que agrupe los puertos 25 y 26 con ***#trunk 25.26 trk1 lacp*** y compruebe el resultado con ***#show trunks*** y ***#show lacp***

Observe cómo han quedado los puertos con ***#show interfaces brief 25,26***, ***#show spannig-tree*** y ***#show spanning-tree 25*** (ó 26) ¿Qué ha pasado con los puertos 25 y 26? Quizás pueda ayudarle un último comando: ***#show spanning-tree trk1***.

Asegúrese de que el agregado está configurado para trabajar por cada enlace a la velocidad de 10 Mb/s *full-dúplex* con ***#show interfaces brief 25,26***, si no fuera así configúrelo para que la siguiente medida sea coherente con la que ha realizado anteriormente sin agregación.

Repita la descarga del fichero *vanGogh.jpg* anotando los mismos datos de tiempos y tasa media de descarga.

[**Memoria**] Guarde el resultado de pantalla que confirme la creación del enlace agregado en los conmutadores, y compare los resultados obtenidos en ambos experimentos comentando si éstos son acordes con lo esperado. Justifique la respuesta.

MSTP

Elimine la agregación de enlaces manteniendo los conmutadores conectados mediante doble enlace por puertos 10/100/1000-BaseT. Para facilitarle el seguimiento de posibles problemas se recomienda que cada latiguillo de conexión utilice el mismo número de puerto en ambos conmutadores.

En primer lugar deberá activar STP o RSTP con los comandos que ya conoce para evitar la formación de un bucle, si bien se recomienda el uso de RSTP por las ventajas que supone frente a STP.

Confirme que mantiene la conectividad IP (*ping*) del escenario: cada cliente *http* o *tftp* (PC1) con el servidor (PC2) y el administrador con los conmutadores S1 y S2.

Compruebe la existencia del árbol de expansión sin bucles creado con RSTP mostrando el estado de los puertos usados para conectar los conmutadores.

En este apartado va a utilizar el protocolo MSTP (*MultipleSpannig-TreeProtocol*) para llegar a una topología lógica que permita utilizar los dos enlaces que unen los conmutadores, de manera que el tráfico no esté soportado sólo por uno de ellos como sucede tras habilitar STP o RSTP.

Para alcanzar este objetivo con MSTP necesita (en <u>todos</u> los conmutadores):

- Definir una región (con su "nombre" y "número de revisión")

- Definir varias instancias del protocolo (MSTI)
- Asociar un conjunto de VLANs a cada instancia

Huelga decir que esta configuración deberá ser coincidente en todos los conmutadores que pertenecen a la misma región.

En primer lugar active MSTP con #***spanning-treeforce-version mstp-operation***, si ya tenía *spanning-tree* activado, si no fuese así tendrá que activarlo primero. A continuación compruebe que está activo (#***show spanning-tree***).

Dé nombre y asigne un número de revisión a la región (el número de revisión permitiría trabajar con varias versiones de la región activando la que se deseara en cada momento) con los comandos #***spanning-treeconfig-name*** *REG_G**i*** y #***spanning-treeconfig-revision i***. Compruebe con #***show spanning-tree config*** que ha creado la región y la revisión deseadas.

En este momento sólo tiene una instancia de protocolo activa: la IST (*InternalSpanning-TreeInstance*) o MSTI0. Con el comando #***show spanning-tree instance …*** confirme el ID de la IST y las VLANs que tiene mapeadas por defecto.

Cree las instancias que desee definir para la región con el comando #***spanning-tree instance*** *nº_instancia* ***vlan*** *ID_VLANn ID_VLANm…*(como sabe, cada instancia generará un árbol de expansión). En su caso debe crear dos con la siguiente asignación de VLANs:

- Instancia 1: UsG***i***_1, ServG***i***
- Instancia 2: UsG***i***_2, GestG***i***

Compruebe cómo ha quedado globalmente la configuración de MSTP con #***show spanning-tree mst-config*** o cada instancia individualmente con #***show spanning-tree instance …***

[**Memoria**] Muestre la configuración de MSTP (instancias, asignación de VLANs a cada instancia) y los árboles de expansión creados, indicando qué enlace (puerto S1-puertoS2) se está utilizando para el tráfico de cada VLAN. ¿Ha conseguido el objetivo de distribuir el tráfico entre enlaces?

Si considera que no es así tal vez deba actuar sobre los parámetros de prioridad con comandos del tipo #***spanning-treeinstance***…***priority***… hasta conseguirlo.

[**Memoria**] Muestre de nuevo los árboles de expansión creados, indicando qué enlace (puerto S1-puertoS2) se está utilizando para el tráfico de cada VLAN. Confirme ahora si ha conseguido el objetivo de distribuir el tráfico entre enlaces y explique qué ha modificado en la configuración para ello.

Práctica 4: Redes 802.11 (Wi-Fi)

Material

Al material relacionado en el punto 2 de esta Guía se le añade otro específico para la práctica con redes 802.11.

Cada grupo contará con el siguiente hardware adicional:

- 1 punto de acceso (AP)
  D-Link DAP-2590 Dual Band (2,4 y 5 GHz) 802.11 a/b/g/n
- 2 adaptadores USB Wi-Fi
  DWA-160 N Dual Band (2,4 y 5 GHz) 802.11 a/b/g/n

Y la aplicación:

- Wifiscanner (puede utilizar cualquier aplicación desde su móvil)
- Wireshark
  La aplicación es la misma que utilizó en las prácticas previas, no tiene la opción de capturar tramas 802.11 y ver sus cabeceras pero sí puede observar el tráfico de la interfaz en formato Ethernet con el mismo contenido.
  Conociendo esta limitación puede usarlo cuando necesite realizar alguna captura de la actividad en la interfaz 802.11

Trabajo previo

En primer lugar realice un análisis de la ocupación del espectro y de las redes activas en donde pretende situar su red 802.11: bandas de 2,4 GHz, 5 GHz, canales y niveles de señal generados por otras redes WiFi. Para ello inicie el programa de escaneo de wifi pero tenga en cuenta que la observación en ambas bandas sólo será posible si su adaptador wiFi es capaz de trabajar en las dos.

Observe toda la información que le proporciona el programa sobre las redes 802.11: SSID, nivel de señal, canal, seguridad habilitada, BSSID (dirección MAC del AP) y estándar 802.11 utilizado (g, n, …). Si selecciona una red podrá conocer además su velocidad máxima, el número de redes que usan el mismo canal o un canal que tenga solape y la actividad que está teniendo lugar en el canal.

El programa de wifi scanner suele proporcionar una puntuación o "*Link Score*" a cada una de las redes que ha detectado, de forma que cuanto más alto es su valor mejor sería una hipotética asociación con ella. Esta información permitiría tener una estimación de la situación de recepción frente a otras redes en distintos puntos de la zona cubierta por un AP si nos desplazamos con un dispositivo portátil.

El análisis de los datos del wifi scanner le permitiría decidir en qué banda y canal situar su red 802.11 para configurar a continuación su AP, si bien tendría otros condicionantes como el de la banda en la que pueden trabajar su estaciones (adaptadores WiFi en su caso).

Durante el desarrollo de esta práctica conviene que detenga la ejecución la aplicación ya que consume casi por completo el uso de la interfaz inalámbrica que deberá usar para enviar y recibir tráfico.

[**Memoria**] Comente su decisión aportando la información del programa en la que se ha basado.

Configuración básica del AP

La comunicación con el AP se realiza por un puerto LAN mediante un navegador web. La configuración de fábrica o tras un *reset* le permite acceder con http://192.168.0.50, usuario "admin" y clave en blanco.

Este apartado deberá realizarlo desde un único ordenador (PC1 o PC2).

Conecte el AP a la red eléctrica, su ordenador al AP mediante un cable de red y entre en la configuración del AP. Previamente tendría que haber configurado su ordenador para situarlo en la misma subred.

Antes de introducir cualquier modificación reponga los valores de fábrica del AP desde el menú con ***System -> Restore to Factory Default Settings*** y espere, sin desconectar la alimentación, tal y como le indica el mensaje que aparece en la pantalla.

Una vez restablecidos los valores defina los parámetros básicos de su AP:

a) ***Home->Basic Settings->Wireless*** (parámetros de la interfaz inalámbrica)

- Banda: 5 GHz
- Modo: Punto de acceso
- SSID: Grupo_***i***
- Visibilidad del SSID: Habilitado
- Selección de canal automática: Habilitado
- Ancho del canal: Auto 20/40 MHz
- Autenticación: WPA-Personal
    - Modo WPA: WPA2
    - Cifrado: AES
    - Clave: 12345678

Guarde los cambios introducidos en la pantalla con "*Save*".

b) ***Home->Basic Settings->LAN*** (configuración IP del AP)

- IP: Estática (Manual), tendrá que fijar usted la dirección IP del AP en la siguiente línea
- Dirección IP: 192.168.***i***.50
- Máscara de subred: 255.255.255.0
- Gateway: en blanco por el momento

Guarde los cambios introducidos en la pantalla con "*Save*".

A pesar de haber guardado los cambios aún no se han hecho efectivos en el AP; para ello debe dar una orden explícita con ***Configuration->Save and Activate*** y esperar a que actualice la configuración.

Entre de nuevo para continuar con la configuración del AP. Si le ha surgido algún problema en la comunicación averigüe el porqué y resuélvalo.

Confirme con el InSSIDer que ha aparecido una red con el SSID, banda y canal que usted ha elegido. Tras ello vuelva a desactivar InSSIDer para no interferir en el resto de la práctica.

Los pasos anteriores suponen el haber creado la BSS con SSID Grupo_***i*** cuyos equipos estarán en la red 192.168.***i***.0/24, siendo la dirección IP del AP 192.168.***i***.50.

A partir de este momento puede asociar estaciones WiFi al AP, si bien tendrá que configurarles manualmente las direcciones IP/Máscara para que pertenezcan a la misma subred. Para conseguir una asociación sin necesidad de esta configuración manual de la estación es necesario activar el servidor DHCP del AP que asignará direcciones IP dinámicas a las STAs. Puede hacerlo desde ***Home->Advanced Settings->DHCP Server->Dynamic Pool Settings***.

Active el servidor DHCP para que asigne direcciones IP dinámicas en el rango 192.168.***i***.100 a 199 en su red 192.168.***i***.0/24.

Desconecte el cable de red de ordenador del puerto Ethernet del AP, ya puede comunicarse con él utilizando su adaptador WiFi. Confirme que efectivamente es posible, que el AP le asigna una dirección IP del rango establecido y que tiene conectividad IP con el AP (*ping*).

Entre en la pantalla de configuración del AP a través de su interfaz WiFi como última comprobación de que ha conseguido comunicarse con él.

Puede ver las eventos de asociaciones y asignación de direcciones IP en ***Home->Status->Log->View Log***, las direcciones IP asignadas en ***Home->Advanced Settings->DHCP Server->Current IP Mapping List*** y la relación de clientes asociados al AP en ***Home->Status->Client Information***

[**Memoria**] Proporcione evidencias de la configuración del AP, la asociación de su ordenador (STA) al AP, la dirección IP asignada y la conectividad IP.

Medidas de rendimiento

En los apartados siguientes irá tomando referencias de tiempo de descarga de un fichero (*Gogh.jpg*) con el protocolo http para realizar una tabla comparativa del rendimiento (caudal) conseguido en el experimento bajo distintos escenarios.

En todos ellos tendrá un ordenador como cliente (C) y otro como servidor (S). El ordenador que utilice interfaz Wifi ejecutará el sistema operativo Linux Debian (para asignar rutas por defecto deberá utilizar la herramienta gráfica. Refresque cómo se puede consultar en Linux las tablas de encaminamiento para ver si son correctas).

Los escenarios a comparar serán los siguientes:

1. C y S con interfaces Ethernet a 100 Mb/s
2. C con interfaz 802.11 N (banda 5 GHz) y S con interfaz Ethernet a 100 Mb/s

Comience con el escenario 1, el más sencillo, con C y S usando interfaces Ethernet a 100 Mb/s:

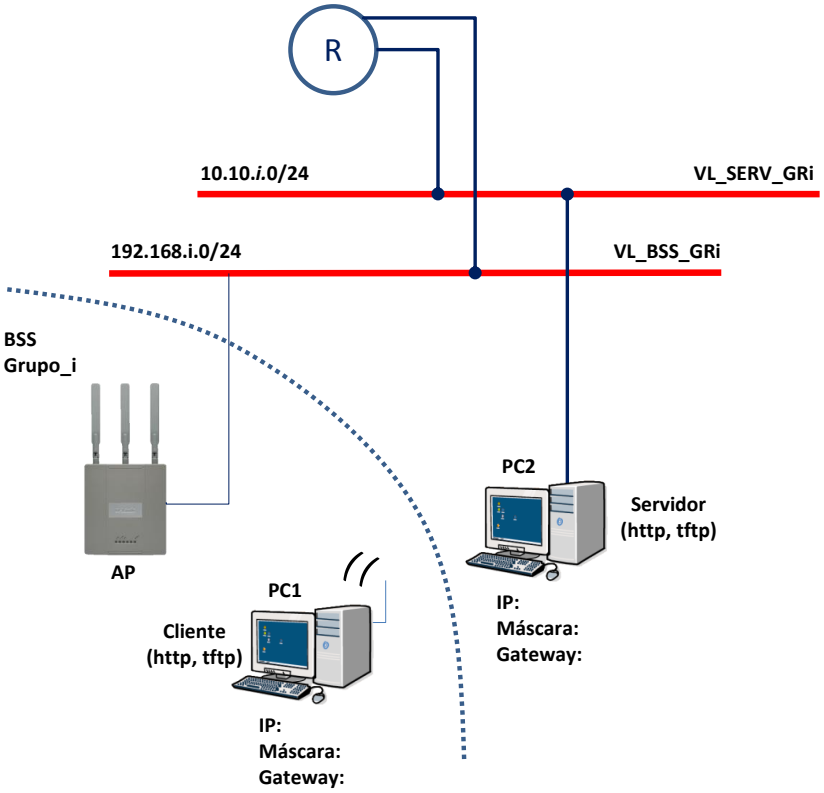
- Desactive los adaptadores WiFi para tener la seguridad de que no se están utilizando
- Conecte PC1 y PC2 al mismo conmutador en dos puertos 10/100-BaseT
- Asigne los puertos a la misma VLAN (si no quiere crearla use la DEFAULT_VLAN)
- Asigne direcciones coherentes a los ordenadores
- Compruebe la conectividad IP entre ellos (*ping*)
- Realice la descarga del fichero y **anote los tiempos**

[**Memoria**] Aporte evidencias de que la configuración realizada coincide con la exigida para el escenario 1.

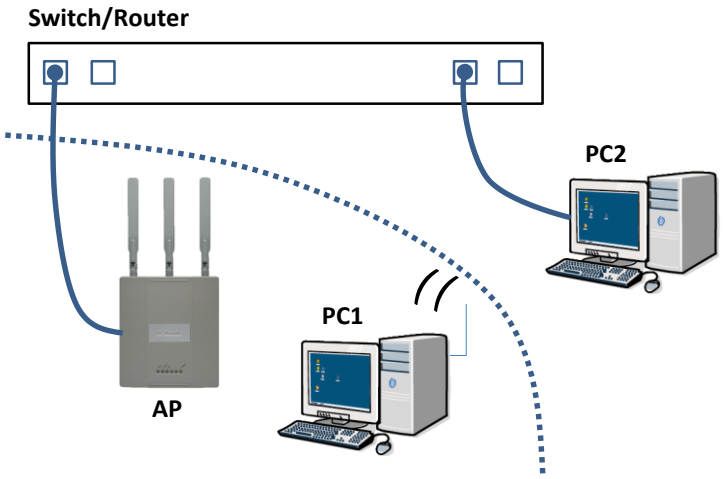
Conexión de la BSS a una red

La BSS se puede conectar a una red utilizando el puerto Ethernet del AP (hasta ahora se ha usado para configuración) y conectándolo al puerto de un conmutador en una LAN o VLAN.

En este apartado va a crear un escenario con un cliente inalámbrico que va a descargar un fichero de un servidor cableado con interfaz Ethernet, estando situados ambos en distintas subredes.



Utilice un solo conmutador, el HP-2610 cuya funcionalidad de *routing* habrá que activar, al que conectará los distintos elementos, eligiendo los puertos 10/100-BaseT que desee.



Conecte temporalmente un cable de red desde un ordenador al AP para configurarlo (también podría hacerlo a través de un adaptador WiFi), desconéctelo una vez finalizada la operación. Recuerde realizar la configuración de la tarjeta Ethernet del ordenador de manera coherente.

Configuración del AP:

- Es válida la configuración realizada hasta ahora
- Añada un *gateway* por defecto: 192.168.***i***.1 (***Home->Basic Settings->LAN***)
- Haga efectivos los cambios con ***Configuration->Save and Activate***

Configuración de C y S:

- Configure adecuadamente C (PC1) y S (PC2) con las direcciones IP, máscara y gateway predeterminado (cuando sea necesario) de acuerdo con el escenario
- Desconecte la interfaz Ethernet de C o desactive la tarjeta para tener la seguridad de que no se está utilizando. Haga lo mismo con S referido a su adaptador WiFi

Configuración del conmutador HP-2610:

- Creación de dos VLANs: VL_SERV_GR***i*** y VL_BSS_GR***i*** (si hace falta, reinicie de fábrica)
- Asignación de puertos a VLAN
- Creación de interfaces IP para el conmutador en ambas VLANs coherentes con el escenario
- Activación de la función de *routing*
- Comprobación de la conectividad IP
    - PC1 con AP (WiFi)
    - PC1 con su *router*
    - PC2 con su *router*
    - PC1 con PC2

Una vez conseguido el escenario 2 realice la descarga del fichero y anote los tiempos.

[**Memoria**] Aporte evidencias de que la configuración realizada coincide con la exigida para el escenario 2.

Comparativa de rendimientos

[**Memoria**] Realice una tabla en la que muestre para cada escenario los tiempos de descarga del fichero y el rendimiento (caudal) obtenido. A partir de ahí aporte sus conclusiones analizando los resultados empíricos con los que cabría esperar a la luz de factores como interfaces, banda, canal, velocidad, protocolo, ocupación del espectro, etc.

Tras finalizar la práctica reponga los valores de fábrica del AP desde el menú con ***System -> Restore to Factory Default Settings***. Esto permitirá al próximo grupo realizar la práctica partiendo desde la misma situación que su grupo.

SSIDs múltiples

El AP que está utilizando permite tener varias BSS activas simultáneamente si bien tienen que compartir el mismo canal y banda de frecuencia, o lo que es lo mismo, distribuir la capacidad total de la interfaz entre ellas.

En este apartado va a definir dos BSS adicionales y comprobar que efectivamente están teniendo visibilidad y que se puede conectar a cualquiera de ellas.

Configuración del AP:

- Es válida la realizada hasta ahora, aunque con las modificaciones que siguen
- Active la opción de SSIDs multiples (**Home->Advanced Settings->Multi-SSID**)
  - *Enable Multi-SSID*
- Defina las dos SSIDs
  - Index: SSID 1
  - SSID: GR_***i***_A
  - Security: WPA-Personal
  - WPA Mode: WPA2 Only
  - Cypher Type: AES
  - Passphrase: 12345678-A
  - Pulse “Add”

  - Index: SSID 2
  - SSID: GR_***i***_B
  - Security: WPA-Personal
  - WPA Mode: WPA2 Only
  - Cypher Type: AES
  - Passphrase: 12345678-B
  - Pulse “Add”

  - Guarde los cambios con “Save”
- Haga efectivos los cambios con ***Configuration->Save and Activate***

Confirme con InSSIDer que tiene visibilidad de las tres BSS y observe los canales en los que se encuentran disponibles.

Intente asociarse a cualquiera de las 3 BSS que tiene disponible, confirmando que lo ha conseguido no sólo desde el PC sino también consultado los "*logs*" del AP y la relación de clientes que tiene asociados cada SSID (***Home->Status->Log->View Log*** y H***ome->Status->Client Information***).

Explore las posibilidades de insertar el tráfico en una red conectando el puerto del AP a un puerto de un conmutador de forma que pueda diferenciarse según la BSS (SSID) a la que esté asociada la estación, definiendo distintas VLANs, una para cada SSID. Para ello eche un vistazo en **Home->Advanced Settings->VLAN** y sus posibilidades *tagged*/*untagged* para cada puerto (las distintas SSIDs y la LAN).