Departamento de
Automática y Computación
Automatika eta
Konputazio Saila

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

Práctica 1: Configuración básica de conmutadores Ethernet Cisco

1- Objetivos

En esta práctica se aprenderá cómo obtener información sobre la configuración y funcionamiento de un conmutador Ethernet con Cisco IOS así como a configurar sus parámetros básicos por puerto y un empleo básico de la información obtenida mediante CDP. Finalmente, veremos la necesidad de un protocolo de control para topologías con bucles.

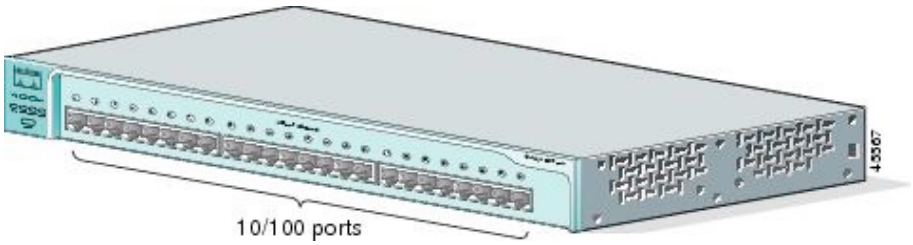


Figura 1- Catalyst 2950-24 (http://www.cisco.com)

2- Conocimientos previos

- Saber configurar IP en un PC con linux
- Saber acceder por el puerto de consola a un equipo Cisco
- Mínima experiencia con comandos del CLI del IOS
- Comprender cómo funciona un puente transparente

3- Acceso al conmutador por consola

Consulte la documentación sobre configuración de routers Cisco. El acceso a la configuración de los switches se lleva a cabo de igual forma, a través del puerto de consola.

4- Viendo el estado del conmutador en el panel frontal

El conmutador tiene una luz para cada uno de los puertos que puede estar apagada, en verde o en amarillo. El significado de estas luces depende del modo en que se encuentren (hay otras luces para indicar el modo actual, ver Tabla 1). Puede ver las diferentes combinaciones de modos en la Tabla 2. Se cambia de modo mediante el botón *Mode* (tenga cuidado de no mantenerlo pretado demasiado tiempo pues entonces entraría en un proceso de reset de la configuración del conmutador).

Departamento de
Automática y Computación
Automatika eta
Konputazio Saila

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

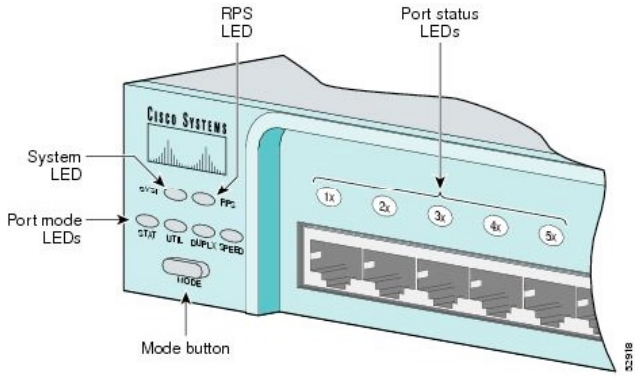


Figura 2- LEDs del Catalyst 2950-24 (http://www.cisco.com)

Mode LED	Port Mode	Description
STAT	Port status	The port status. This is the default mode.
UTIL	Switch utilization	The bandwidth in use by the switch.
DUPLX	Port duplex mode	The port duplex mode: half duplex or full duplex.
SPEED	Port speed	The port operating speed: 10 or 100 Mbps for 10/100 ports and 10, 100, or 1000 Mbps for 10/100/1000 ports.

Tabla 1- LEDs de Modo (http://www.cisco.com)

Port Mode	Color	Meaning
STAT (port status)	Off	No link.
	Solid green	Link present.
	Flashing green	Activity. Port is sending or receiving data.
	Alternating green-amber	Link fault. Error frames can affect connectivity, and errors such as excessive collisions, CRC errors, and alignment and jabber errors are monitored for a link-fault indication.
	Solid amber	Port is not forwarding. Port was disabled by management, an address violation, or Spanning Tree Protocol (STP). Note After a port is reconfigured, the port LED can remain amber for up to 30 seconds while STP checks the switch for possible loops.

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

UTIL (utilization)	Green	The current backplane utilization that is displayed over the amber LED background on a logarithmic scale.
	Amber	The maximum backplane utilization since the switch was powered on.
	Green and amber	Note If the current utilization exceeds the maximum utilization, the maximum utilization is automatically updated.
DUPLX (half or full duplex)	Off	Port is operating in half duplex.
	Green	Port is operating in full duplex.
SPEED	10/100 ports	
	Off	Port is operating at 10 Mbps.
	Green	Port is operating at 100 Mbps.
	10/100/1000 ports	
	Off	Port is operating at 10 Mbps.
	Green	Port is operating at 100 Mbps.
	Flashing green	Port is operating at 1000 Mbps.
	1000BASE-X GBIC module ports	
	Off	Port is not operating.
	Green	Port is operating at 1000 Mbps.

Tabla 2- Significado de los LEDs del puerto (http://www.cisco.com)

Compruebe el funcionamiento del panel frontal. Por ejemplo:

- Conecte un hub a un puerto y vea el indicador de velocidad y de duplex
- Conecte un par de PCs, genere tráfico entre ellos y vea la indicación de utilización, el duplex y velocidad de cada puerto

5- Información de los Interfaces

En el interfaz de gestión del conmutador (por el puerto de consola), observe la información que puede obtener sobre cada interfaz del conmutador (ignore de momento toda referencia a VLANs) mediante el comando:

```
> show interfaces
```

Departamento de
Automática y Computación
Automatika eta
Konputazio Saila

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

¿Qué información en concreto se obtiene con este comando?:

```
> show interfaces description
```

Observe la salida del comando:

```
> show interfaces status
```

Conecte un PC a un puerto del conmutador y vea qué aparece en la columna *Duplex* y en la columna *Speed* para ese puerto.

Conecte un Hub y repita la operación. ¿De qué velocidad es el hub?

Puede obtener las estadísticas de contadores de paquetes y bytes recibidos y transmitidos para todos los interfaces con:

```
> show interfaces counters
```

6- Tabla de direcciones MAC

Uno de los elementos fundamentales de un conmutador es su tabla de direcciones MAC, la cual le permite relacionar estas direcciones con el puerto por el cual se alcanzan (y VLAN como veremos más adelante). Puede ver dicha tabla del conmutador con el comando:

```
> show mac address-table
```

No se preocupe por entradas en la tabla tipo:

```
Vlan Mac Address     Type Ports
---- ----------- -------- -----
All 000f.9056.e9c0 STATIC CPU
All 0100.0ccc.cccc STATIC CPU
All 0100.0ccc.cccd STATIC CPU
All 0100.0cdd.dddd STATIC CPU
```

La primera es una de las direcciones MAC del conmutador, que empleará seguramente al enviar tramas (ojo, no al reenviar, al reenviar normalmente no cambia nada en la trama). Las tres siguientes son direcciones MAC multicast empleadas por protocolos propietarios de Cisco (DTP, VTP, CDP, SSTP, CGMP).

Conecte al conmutador alguno de sus PCs y/o routers, genere tráfico entre ellos y observe cómo se va poblando la tabla. ¿Qué tipos de entradas aparecen en la tabla?

Averigüe con algún comando cuánto tiempo debe transcurrir sin ver tramas provenientes de una dirección MAC para que el conmutador la elimine de esta tabla.

Interconecte sus dos conmutadores Cisco. A uno de ellos conecte uno de los PCs y genere tráfico con él. Practique cómo puede localizar el puerto al que está conectado un PC empleando el comando:

```
> show mac address-table address H.H.H
```

7- CDP

CDP son las siglas del *Cisco Discovery Protocol*. Este es un protocolo que funciona directamente sobre el nivel de enlace, protocolo propietario de Cisco y empleado para que los equipos vecinos se informen sobre sus capacidades. Por defecto lo implementan todos los equipos Cisco (routers, conmutadores, etc.). Por ejemplo, interconecte sus dos conmutadores Cisco y conecte uno de sus

upna Universidad Pública de Navarra Nafarroako Unibertsitate Publikoa
Departamento de
Automática y Computación
Automatika eta
Konputazio Saila

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

tres routers a uno de ellos[1]. Desde el conmutador que tiene conectado al router podrá ver sus dos vecinos con el comando:

```
> show cdp neighbors
```

Por defecto los mensajes CDP se envían por todos los puertos. Conecte uno de sus PCs a uno de los puertos del conmutador y observer con `wireshark` el formato y contenido de dichos mensajes. ¿Qué tipo de encapsulación Ethernet emplean?

8- Configuración estática vs automática de puertos

Pruebe cómo puede cambiar la configuración de velocidad y duplex de cada interfaz del conmutador con los comandos:

```
(config-if)# speed [10|100|1000|auto]
(config-if)# duplex [auto|full|half]
```

Compruebe que los cambios son efectivos. Por ejemplo conecte 2 PCs al conmutador y mida el RTT entre ellos a medida que cambia la velocidad de sus puertos.

9- Topologías con bucles

Vamos a ver los problemas que pueden surgir en una topología Ethernet con bucles. Interconecte sus dos conmutadores Cisco por al menos 2 puertos simultáneamente, de manera que tengamos un ciclo en la topología de conmutadores. El objetivo es conseguir ver una inundación por culpa de ese bucle, o sea, algún paquete dando vueltas sin fin.

Por defecto los conmutadores Cisco emplean el Spanning Tree Protocol (STP) para evitar el problema que vamos a provocar en unos momentos. Por ello, lo primero que vamos a hacer es desactivar STP **en ambos conmutadores**. Para ello haga en cada uno de ellos:

```
Switch(config)# no spanning-tree vlan 1
```

Conecte un PC a un interfaz de uno de los conmutadores. Asígnele dirección IP e intente hacer ping a una dirección de su misma red a la que nunca haya hecho ping. En realidad lo que queremos es generar una trama ethernet de broadcast. Para ello, si queremos mandar un paquete IP (en este caso el mensaje ICMP) a una máquina en nuestra red cuya MAC no conocemos se generará un mensaje ARP para averiguar dicha dirección MAC, y ese mensaje va en una trama ethernet de broadcast.

Puede ver el incremento en la utilización del conmutador con los indicadores del panel frontal del mismo.

Si sucede que los PCs que tenga conectados a los conmutadores quedan bloqueados ¿a qué puede deberse esto? Para desbloquearlos puede por ejemplo desconectarlos del conmutador.

Punto de control: Muestre al profesor de prácticas que ha logrado recrear el problema

10- Evaluación

Mediante punto de control

[1] Según el modelo de router puede no traer CDP activado. Puede activarlo desde el modo configuración del router, con "cdp run". Recuerde que también debe activar el interfaz del router ("no shutdown")

Departamento de
Automática y Computación
Automatika eta
Konputazio Saila

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

Práctica 2: Configuración de VLANs en conmutadores Cisco

1- Objetivos

En esta práctica veremos cómo crear VLANs y asignar puertos a ellas en conmutadores con Cisco IOS. También veremos cómo crear enlaces de trunk entre conmutadores empleando encapsulado 802.1Q.

2- Conocimientos previos

- Funcionamiento de un puente/conmutador Ethernet
- Acceso por consola a un switch Cisco
- Configuración IP en PCs con Linux
- Qué son las VLANs
- 802.1Q
- Configuración de acceso por telnet a un router Cisco

3- Empleo de VLANs en un switch

Los conmutadores Cisco traen creada por defecto una VLAN, la VLAN 1, y todos los puertos asignados a ella de forma nativa (sin encapsulación 802.1Q). Pueden ver esto con el comando:

```
Switch> show vlan
```

Verán también creadas las VLANs 1002-1005, que no nos van a interesar. Puede que haya más VLANs creadas en caso de que no hayan sido borradas tras otras prácticas.

Vamos a crear un par de VLANs en un conmutador Cisco. Empleen para ello el switch1. Primero pongan el conmutador en modo VTP transparente (pueden ver el apartado sobre VTP para entender esto, es otro protocolo propietario de Cisco):

```
Switch(config)# vtp mode transparent
```

A continuación creen las VLANs de números 2 y 3 con el comando `vlan` (entrarán en el modo de configuración de VLANs, pueden salir directamente de él pues ya han creado la VLAN, si quieren hay varios comandos que pueden probar en ese modo).

```
Switch(config)# vlan 2
Switch(config-vlan)#
```

Para configurar un interfaz del conmutador en una de esas VLAN deben ir al modo de configuración del interfaz en cuestión. Primero deben indicar que dicho interfaz estará en modo acceso, es decir, solo empleará una VLAN (en vez de estar en modo trunk, por ejemplo):

```
Switch(config-if)# switchport mode access
```

Y ahora ya pueden especificar la VLAN en concreto en la que configurar ese puerto:

```
Switch(config-if)# switchport access vlan {número}
```

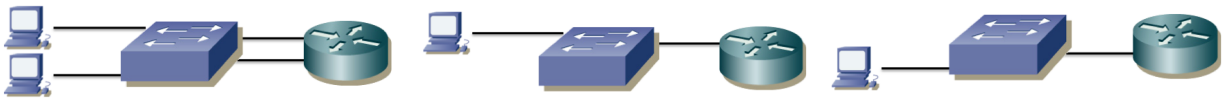
Configuren dos puertos FastEthernet del conmutador en la VLAN 2 y otros dos en la VLAN 3. Comprueben que efectivamente las LANs son independientes. Para ello pueden emplear PCs o routers de los que disponen, conectándolos, generando tráfico y empleando `tcpdump` para

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

comprobar en qué máquinas lo ven. Incluso pueden probar a emplear las mismas direcciones IP pero en VLANs diferentes.

¿Cómo puede averiguar las direcciones MAC que el conmutador ha aprendido por cada puerto?

Empleando uno de los routers con dos interfaces ethernet, conéctelos en puertos del conmutador en diferentes VLANs y haga que enrute el tráfico entre ellas (Figura 1).



(a) (b) (c)

Figura 1 – Topología a) física, b) VLAN 2, c) VLAN 3

Punto de control: Muestre esta última configuración a su profesor de prácticas

4- Trunking

Pongan también el segundo switch (switch2) en modo transparente y creen en él las VLANs 2 y 3. Configuren unos puertos en ese switch en la VLAN 2 y otros en la VLAN 3.

Interconecten los switches por dos parejas de puertos, unos en la VLAN 2 y otros en la VLAN 3. Comprueben la comunicación entre máquinas conectadas a cada conmutador así como el aislamiento del tráfico.

Ahora tenemos un nuevo bucle físico. ¿Si desactivamos STP como hicimos en la práctica anterior tendremos de nuevo un problema de inundación?

Deshagan la configuración anterior. Lleven a cabo el conexionado físico de la figura 2 (atención a cables rectos y cruzados). Al estar ahora los conmutadores con su configuración de fábrica estarán todos sus puertos en la VLAN 1. En el PC C conectado al hub no necesita configurar una dirección IP, vale con que su interfaz esté activado y arranquen `wireshark` o `tcpdump` sobre él. Ese PC nos servirá para ver las tramas Ethernet que intercambian los dos conmutadores. El hub y el PC conectado a él no son necesarios para la comunicación entre los switches; hubiéramos podido conectarlos directamente pero hemos preferido esta disposición para poder ver el tráfico que circula entre ellos.

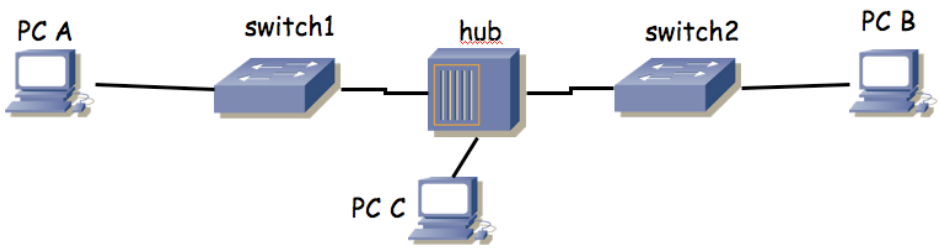


Figura 2.- 2 conmutadores interconectados a través de un hub

Configuren en modo trunk el puerto de cada conmutador que sirve para interconectarlos. Para ello, en modo de configuración del interfaz pueden hacer:

```
Switch(config-if)# switchport mode trunk
```

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

Configuren los puertos de los conmutadores que van a PC A y PC B en la VLAN 2 y configuren direcciones IP en los interfaces de PC A y B en la misma subred IP. Prueben la comunicación entre los PCs A y B y vean el tráfico 802.1Q que circula entre los dos conmutadores. Cambien la configuración de los puertos de los conmutadores a los PCs para que ahora estén en la VLAN 3 y vea de nuevo el encapsulado 802.1Q.

Punto de control: Muestre el encapsulado 802.1Q al profesor de prácticas.

Vea la información que puede obtener con el comando:

```
Switch> show interfaces trunk
```

En IOS puede especificar para un puerto de un switch que quiere que el puerto esté en modo acceso o en modo trunk según qué se conecte a dicho puerto. Para llevar a cabo esta negociación Cisco dispone de sus propios protocolos. Puede especificar este modo con la opción `dynamic` del comando `switchport mode`.

Interconecte sus dos conmutadores Cisco por un par de puertos. Configure que en modo acceso esos puertos estarán en una VLAN en concreto pero que desean establecer un trunk (vea las opciones de `switchport mode dynamic`). Compruebe que entre ellos establecen el trunk pero que si los desconecta y en ese mismo puerto conecta un PC su tráfico se asigna a la VLAN especificada en el modo acceso.

Pueden ver el estado actual de un puerto (incluyendo su VLAN nativa si está en trunk, si desea trunk, las VLANs que pasan por él, etc.) mediante el comando:

```
Switch> show interfaces switchport
```

5- VLAN nativa

En un enlace de trunk 802.1Q existe una VLAN para la que no se emplea el encapsulado 802.1Q sino que las tramas se envían con encapsulado normal Ethernet (sin etiqueta de VLAN, "untagged"). Esta es la que también se llama la VLAN nativa. Las tramas que entran por un puerto de trunk sin encapsulado 802.1Q se asignan a esa VLAN. Por defecto en los switches Cisco la VLAN nativa de un puerto en trunk es la VLAN 1. Podemos configurar en un puerto en trunk una VLAN nativa distinta de la VLAN 1 mediante el comando:

```
Switch(config-if)# switchport native vlan {número}
```

Los puertos C de las mesas llevan a un conmutador Cisco. Todos los puertos de este conmutador están configurados en modo trunk. La VLAN nativa configurada es la VLAN 5. Si a ellos no se conecta otro switch que establezca un trunk sino que se conecta un PC que envía tramas sin encapsulado 802.1Q entenderá que éstas pertenecen a la VLAN nativa de ese puerto y así las etiquetará para reenviarlas dentro de la estructura de conmutadores del laboratorio. Sin embargo, acepta también tramas con encapsulado 802.1Q de la VLAN 30 (el resto de VLANs empleadas en el laboratorio no se propagan por esos puertos). Puede verlo si hace telnet a ese conmutador (IP: `10.2.1.4`, password: `tlm`) y emplea el comando `show interfaces switchport`

6- Evaluación

Mediante puntos de control

upna Universidad Pública de Navarra Nafarroako Unibertsitate Publikoa

Departamento de
Automática y Computación
Automatika eta
Konputazio Saila

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

Práctica 3: Spanning Tree Protocol

1- Objetivos

En esta práctica crearemos algunos escenarios simples en los que ver el Spanning Tree Protocol en funcionamiento. Alteraremos parámetros de configuración del protocolo para controlar las topologías resultantes. Finalmente veremos cómo balancear el tráfico de diferentes VLANs entre trunks empleando STP por VLAN.

2- Conocimientos previos

- Funcionamiento del Spanning Tree Protocol: qué problema resuelve, cómo, qué es un nodo raíz, etc.
- Configuración básica y de VLANs en conmutadores Cisco
- VLANs y 802.1Q

3- STP en funcionamiento

Conecte uno de los PCs a uno de los puertos de sus conmutadores Cisco. Empleando `wireshark` vea los diferentes campos de las BPDUs (es decir, de los mensajes del protocolo STP).

Interconecte sus dos conmutadores Cisco (Figura 1a). En uno de esos conmutadores vea la información que puede obtener con las diferentes opciones del comando `show spanning-tree`. Por ejemplo, vea cómo averiguar cuál es el root del árbol o el coste hasta él, qué puertos están reenviando o bloqueados, el coste de cada uno, etc. Confirme la dirección del root con las BPDUs que recibe el PC.

Interconecte ahora los dos conmutadores por dos pares de puertos, de forma que exista un bucle (Figura 1b). Conecte un PC a cada conmutador y compruebe que el tráfico entre ellos no inunda los conmutadores. Averigüe qué puerto ha sido bloqueado y por qué.

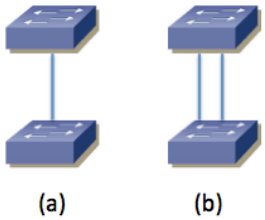


Figura 1 – Interconexión física de conmutadores para pruebas de STP

Desconecte la interconexión en la cual hay un puerto bloqueado y compruebe que el tráfico entre los PCs no se interrumpe. Vuelva a conectarla.

Desconecte el cable de interconexión por el que está yendo el tráfico del árbol entre los conmutadores y vea cómo se corta el tráfico entre los PCs pero al poco tiempo se recupera porque pasa a usarse el otro cable. ¿Cuánto tiempo tarda? Fíjese en el cambio de estado en los puertos de los conmutadores durante ese tiempo. Reconéctelo y vea cómo vuelve a cambiar el árbol al estado original (habrá un nuevo corte breve). ¿Por qué vuelve al camino original?

Desconecte de nuevo la interconexión en uso. Volverá a cambiar el árbol a emplear la otra.

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

Interponga un hub entre los puertos que ha desconectado. Ahora al volverlos a conectar (con el hub) no se selecciona ese camino. ¿Por qué?

Dentro del modo configuración tiene el comando `spanning-tree` para hacer cambios en STP. Consiga controlar cuál de los dos conmutadores es la raíz del árbol.

Punto de control: Muestre esta última configuración a su profesor de prácticas, explicando los cambios que ha hecho para lograr controlar la raíz del árbol.

4- STP en topología con 3 conmutadores

Configure la topología física de la Figura 2, con todos los PCs con dirección IP en la misma subred.

Garantice que el switch1 sea la raíz del árbol de expansion mediante la configuración de prioridades. Averigüe el Bride ID de cada conmutador y calcule qué puerto va a estar bloqueado. Posteriormente verifíquelo mirando el rol y estado de todos los puertos. Ponga un ping continuo entre cada pareja de PCs y compruebe si se detiene alguno de ellos cuando desconecta el enlace que tiene un puerto bloqueado.

Fuerce la velocidad del enlace entre switch1 y switch3 a 10Mbps mediante la configuración de la velocidad en los puertos de los conmutadores. Compruebe cómo queda ahora el árbol de expansión.

Devuelva la velocidad del enlace entre switch1 y switch3 a 100Mbps. Ponga un ping continuo entre PCB y PCC. Simularemos el reinicio del switch1. Para ello desconecte los cables de red de los puertos del switch1. Compruebe qué sucede con el ping y qué cambia en el árbol de expansion. Espere un par de minutos y reconecte todos los puertos del switch. Compruebe qué sucede con el ping y qué cambia en el árbol de expansión en el tiempo hasta un minuto después de que lo haya reconectado.

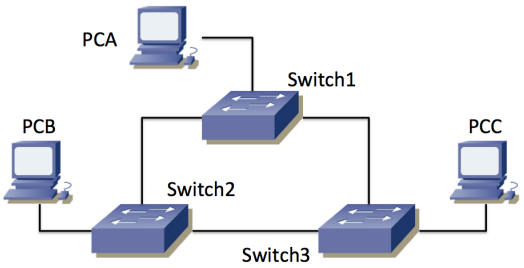


Figura 2 – Topología con 3 conmutadores

Punto de control: Muestre esta última configuración a su profesor de prácticas, explicando lo que sucede.

5- Reparto de carga con PVST

Interconecte sus tres conmutadores siguiendo la topología física de la Figura 3. Cree dos VLANs de forma que existan en todos ellos (en este apartado va a requerir 2 VLANs simultáneamente en los switches y supondremos que son las VLANs 2 y 3 pero podrían tener otro número). Todos los enlaces entre conmutadores deben ser enlaces de trunk, de forma que ambas VLANs puedan emplearlos. Si los conmutadores están con la configuración por defecto crearán los trunk sin más

que interconectarlos[2]. Configure todos los enlaces de trunking a 10Mb/s.

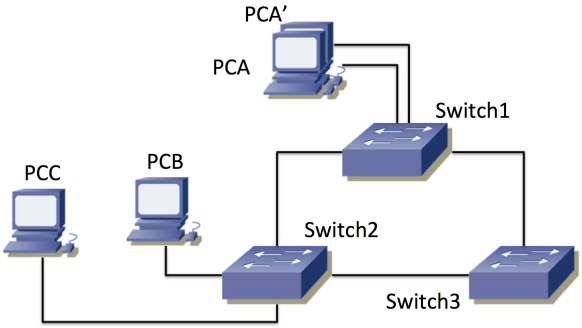


Figura 3 – Topología física con dos interfaces de un PC en uso

Como no disponemos de 4 PCs emplearemos 2 interfaces de PCA para que hagan las funciones de 2 PCs diferentes. Los llamaremos PCA y PCA'. Configuraremos el puerto de Switch1 al que se conecta PCA en la VLAN 2, así como el puerto del Switch2 al que se conecta PCB. Configuraremos el puerto de Switch1 al que se conecta PCA' en la VLAN3, así como el puerto de Switch2 al que se conecta PCC. PCA y PCB se configurarán con direcciones IP de una subred y PCA' y PCC de otra independiente (ver figura 4).

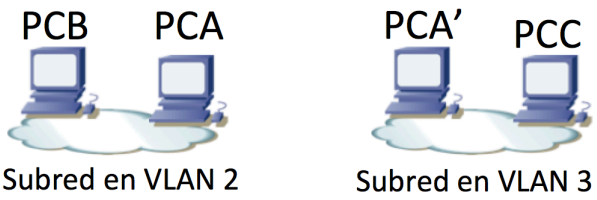


Figura 4 – Topología de nivel de red IP

Recuerde que Cisco está empleando un Spanning Tree por cada VLAN en estos conmutadores (lo que llama PVST o *Per VLAN Spanning Tree*). Como la configuración de STP para ambas VLANs es inicialmente idéntica terminamos usando los mismos trunk para las dos y bloqueando un puerto del tercero. Sería más eficiente que el tráfico inter-switch de las VLANs pudiera sacar provecho a todos los enlaces de trunk. Esto require mayor complejidad de configuración y una red más compleja.

Modifique la configuración de los respectivos STs (costes, prioridades, etc) de forma que la comunicación entre PCA y PCB no comparta enlaces con la comunicación entre PCA' y PCC. Por ejemplo, la figura 5 muestra lo que podría ser el resultado de los árboles de expansión (hay más soluciones posibles). En este caso el enlace entre switch1 y switch3 no está en uso en la VLAN 2, mientras que en la VLAN 3 es el enlace entre switch1 y switch2 el que tiene un puerto bloqueado.

[2] Si quiere forzar el modo trunk en los conmutadores tenga en cuenta que switch3 requiere que primero se le indique el encapsulado a emplear (dot1q)

Departamento de
Automática y Computación
Automatika eta
Konputazio Saila

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

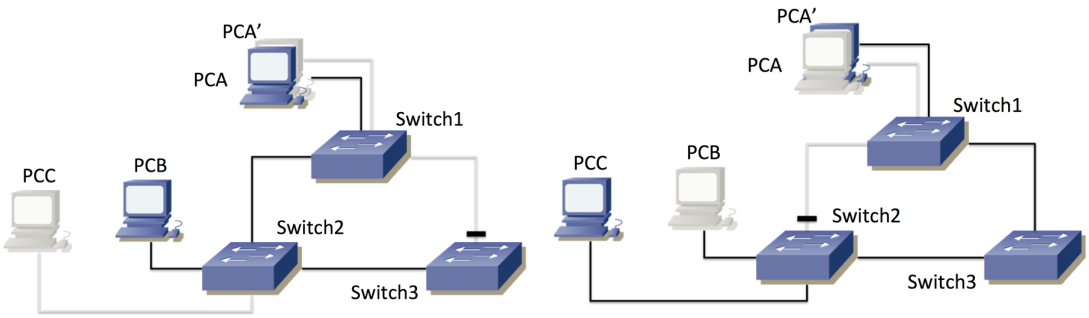


Figura 5 – Posibles resultados de los dos STs, a) VLAN 2, b) VLAN 3

Punto de control: Muestre esta última configuración a su profesor de prácticas

Con esta configuración podrá tener un flujo IP sostenido de cerca de 10Mb/s entre PCB y PCA por la subred de la VLAN 2 al mismo tiempo que mantiene un flujo de esa misma tasa entre PCA' y PCC por la subred de la VLAN 3, porque no comparten ningún enlace. Puede probarlo por ejemplo haciendo dos transferencias simultaneas de un fichero grande.

Para crear un fichero grande puede hacer por ejemplo lo siguiente:

```
PCA$ dd if=/dev/zero of=/tmp/ficheroGrande count=1000 bs=1000000
```

Este comando creará un fichero /tmp/ficheroGrande con 1.000.000.000 ceros de contenido.
Ahora puede copiarlo al otro ordenador de la siguiente forma:

```
PCA$ scp /tmp/ficheroGrande <ipPCB>:/dev/null
```

Debe sustituir <ipPCB> por la dirección IP del otro ordenador. Si le pide que cofirme un *fingerprint* conteste *Yes*. También deberá introducir la password del usuario *ftpr* en la otra máquina.
Como el fichero es de 10^9 bytes, a 10Mb/s tardará más de 10 minutos en transferirse. No se preocupe por borrarlo en la máquina destino, ya que le hemos pedido que lo guarde en /dev/null, que es similar a no guardarlo, pero eso no quita que se transfiera (sí debe recordar borrar al terminar la práctica el fichero /tmp/ficheroGrande del ordenador donde lo creó).
El comando scp le dará una estimación de la velocidad a la que se está transfiriendo el fichero (medido en datos de usuario transferidos, no tiene en cuenta cabeceras de transporte, red y enlace pues no sabe las que se están emplando).
Ponga una transferencia de PCA a PCB y otra simutánea de PCA' a PCC. Debería ver aproximadamente 10Mb/s (1.2MB/s) en cada una.
Durante esas transferencias desconecte el enlace entre Switch1 y Switch3. Se atascará la transferencia a PCC pero una vez que se recalcule el árbol de expansión de la VLAN 3, la transferencia debería continuar. La diferencia ahora estriba en que el tráfico entre PCA y PCC tiene que estar utilizando el camino Switch1-Switch2. Los dos flujos coinciden en ese enlace, así que ya no podrán alcanzar 10Mb/s cada uno sino que entre los dos deberán sumar menos de 10Mb/s. Compruébelo. También puede reconectar el enlace y ver cómo vuelve a cambiar el camino y se recuperan las dos transferencias a 10Mb/s (gracias al control de congestión de TCP).

Punto de control: Muestre esta última configuración a su profesor de prácticas

A continuación conecte un PC al punto C de su mesa. Si recuerda de una práctica anterior ese punto pertenece a un conmutador que tiene el interfaz en trunk, cursando el tráfico de 2 VLANs, por un lado la VLAN 5 en modo nativo, por otro lado la VLAN 30 con encapsulado 802.1Q. Vea los

Departamento de
Automática y Computación
Automatika eta
Konputazio Saila

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

mensajes de STP en ambas VLANs. Localice en los mensajes la dirección MAC identificadora del puente raíz del árbol de expansión (probablemente sea el mismo para ambos árboles). Intente localizar ese conmutador, ¿qué *hostname* tiene? (recuerde que puede perseguir una dirección MAC a través de las tablas de MACs de los conmutadores y que siendo todos los switches de nuestra red Cisco puede usar la información obtenida mediante CDP para averiguar quiénes son los vecinos de un switch).

6- Evaluación

Mediante puntos de control

Departamento de
Automática y Computación
Automatika eta
Konputazio Saila

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

Práctica 4: Agregación de enlaces y monitorización en switches Cisco. 802.1Q en GNU/Linux

1- Objetivos

En esta práctica veremos cómo emplear 802.1Q en PCs Linux. Veremos cómo agregar varios interfaces Ethernet en uno solo lógico y finalmente alteraremos el comportamiento de un conmutador para que nos permita ver todo el tráfico que reenvía por una VLAN.

2- Conocimientos previos

- Configuración IP básica de PCs con Linux y de routers Cisco
- VLANs y 802.1Q
- Configuración básica y de VLANs en conmutadores Cisco
- 802.3ad

3- Etherchannel

Etherchannel es la forma que tiene Cisco de llamar a la agregación de interfaces Ethernet. La gestión de esta agregación se puede basar en el protocolo estándar LACP (802.3ad) o en el protocolo propietario de Cisco PAgP.

Cuando se crea un EtherChannel se crea un interfaz lógico. A partir de ahí se pueden asignar manualmente interfaces físicos al interfaz lógico del Etherchannel.

En este apartado vamos a crear un canal entre dos conmutadores que agregue dos puertos de cada uno.

En primer lugar lleve a cabo la configuración de la figura 1, donde los dos enlaces entre los conmutadores (por ejemplo los puertos 23 y 24 en ambos) estarán configurados como trunks y spanning-tree habrá bloqueado automáticamente uno de ellos. Coloque los tres PCs en la misma LAN y genere tráfico simultáneamente desde los PCs B y C hacia el PC A. Compruebe por qué enlace entre los switches circula el tráfico.

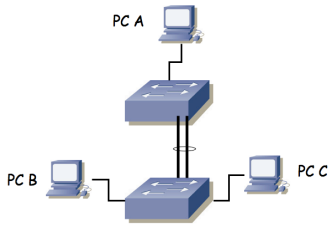


Figura 1.- Escenario con interfaz Etherchannel

Ahora crearemos la agrupación de los enlaces de trunk. En cada switch debemos colocar los puertos de interconexión dentro del mismo grupo, para lo cual, dentro de la configuración de cada uno de esos interfaces deberíamos hacer:

```
Switch(config-if)# channel-group 1 mode active
```

Suponiendo que queremos añadir el interfaz al grupo 1 y queremos que emplee LACP (802.3ad en lugar de la solución propietaria de Cisco, ¿qué ventajas puede tener emplear la solución estándar?)

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

Dado que vamos a repetir el mismo comando en varios interfaces, existe otra forma más cómoda de hacerlo. Podemos aplicar los mismos comandos a varios interfaces. Para ello debemos entrar en modo configuración de varios al mismo tiempo. Por ejemplo, en este caso se podría hacer del siguiente modo:

```
Switch(config)# interface range fa0/23 -24
Switch(config-if-range)# channel-group 1 mode active
```

El resultado es el mismo, es una simple cuestión de comodidad y rapidez.

Por supuesto, debemos repetir los comandos de configuración en el segundo conmutador.

Podemos ver ahora información sobre el estado de la agrupación con:

```
Switch> show interfaces etherchannel
```

Analice la información que puede obtener.

También podemos ver el nuevo interfaz lógico (`Port-channel1`) en el resultado de comandos como por ejemplo `show interfaces summary`.

Estudie el estado actual de los puertos en el spanning-tree.

Repita el envío de tráfico simultáneamente de PC B y C a PC A.

Punto de control: Muestre esta última configuración a su profesor de prácticas.

¿Qué enlace emplean las tramas? Y si genera tráfico de PC A a PC B y C simultáneamente ¿qué camino siguen?

Las respuestas a las cuestiones anteriores dependen de cómo estén haciendo los conmutadores el reparto de la carga entre los enlaces del etherchannel. Cisco permite dos modos de reparto de carga que se controlan con el comando:

```
Switch(config)# port-channel load-balance {dst-mac|src-mac}
```

Estudie las diferentes opciones y pruébelas.

Pista: Si configura los puertos a 10Mbps es fácil saturarlos con una transferencia de un fichero de un host a otro y comprobar por qué puerto están pasando los paquetes.

En la topología de la figura 1 ¿cuál sería la configuración de reparto de carga más rentable para aprovechar ambos enlaces?

4- 802.1Q en un PC

A continuación vamos a ver cómo emplear 802.1Q en un PC con Linux. Haremos que un PC tenga interfaces lógicos en varias VLANs con un solo interfaz físico.

Conecte el interfaz 0 del PC A al switch1 y configure ese puerto del switch en modo acceso y en la VLAN 2. Configure la IP del interfaz del PC dentro de la subred A. Conecte el interfaz 0 del PC B al switch1 y configure ese puerto del switch en modo acceso y en la VLAN 3. Configure la IP del interfaz del PC dentro de la LAN B.

Conecte ahora el PC C a un puerto del switch1. Configure ese puerto del switch en trunk. El resultado del conexionado físico se ve en la figura 2.

Departamento de
Automática y Computación
Automatika eta
Konputazio Saila

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

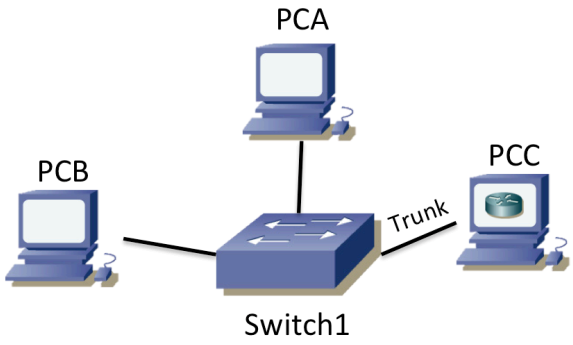


Figura 2 – Topología física

Para crear los interfaces lógicos en el PC primero debemos asegurarnos de que el interfaz físico está activo, por ejemplo:

```
$ sudo ifconfig eth0 up
```

Ahora puede emplear el comando `vconfig` para crear cada interfaz lógico asociado a una VLAN. Por ejemplo, para crear uno asociado a la VLAN 2 (empleando encapsulado 802.1Q) sería:

```
$ sudo vconfig add eth0 2
```

Nota: puede que salga el siguiente mensaje de aviso. Esto no quiere decir que no se haya creado la interfaz lógico, para eso hay que comprobarlo con ***`ifconfig`***.

```
Could not open /proc/net/vlan/config. Maybe you need to load the 802.1q
module, or maybe you are not using PROCS
```

A partir de ese momento debería tener un interfaz llamado `eth0.2`

Si en algún momento quiere borrar un subinterfaz de estos deberá emplear el mismo comando vconfig con la opción '`rem`'

Cree de esta forma el subinterfaz en el PC C para la VLAN 2 y el de la VLAN 3. Asigne dirección IP a cada uno de ellos en la subred que les corresponde. Compruebe que puede hacer ping desde PC C a PC A y a PC B. Puede ver las cabeceras de las tramas con wireshark, tanto en PC C como en A y B.

Configure ruta por defecto en PC A y PC B con siguiente salto la dirección IP de PC C en el interfaz en la misma subred que el PC. Active el reenvío de paquetes IP en PC C. El resultado en capa 3 se ve en la figura 3. Pruebe ahora a hacer ping entre PC A y PC B y vea las tramas en los 4 interfaces. Analice cómo cambia el encapsulado Ethernet y la cabecera IP.

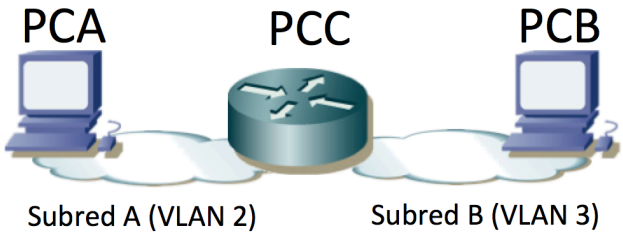


Figura 3 – Topología capa 3 una vez completada la configuraciónn

Departamento de
Automática y Computación
Automatika eta
Konputazio Saila

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

Punto de control: Muestre esta última configuración a su profesor de prácticas mediante una captura en la que se vea el cambio en el encapsulado al pasar un paquete IP de una VLAN a la otra.

5- SPAN

Como recordará, si tenemos varios PCs conectados en un hub o en varios que formen un solo dominio de colisión, cualquiera de ellos puede ver el tráfico que generan todos los demás. Esta característica es muy útil en muchas tareas de mantenimiento. Sin embargo, en el caso de tener conmutadores el dominio de colisión se limita a un puerto por lo que desde un PC conectado a un puerto no podremos ver los paquetes que se intercambian otras máquinas (salvo que vayan dirigidos a la MAC de broadcast o alguna de multicast).

Algunos conmutadores soportan la funcionalidad SPAN (*Switched Port Analyzer*) que permite que las tramas que se envían/reciben por uno o varios puertos o VLANs se copien en otro puerto al que se conectaría el analizador de tráfico.

Con los conmutadores Cisco del laboratorio podemos configurar un puerto de SPAN que vea el tráfico de otros puertos del conmutador. Esto se hace con el comando `monitor` en modo configuración.

Conecte 3 PCs a uno de sus conmutadores Cisco. Establezca una comunicación entre dos de ellos y compruebe que desde el tercero no puede capturar esos paquetes. Ahora active en el conmutador que clone en el puerto del tercer PC los paquetes enviados y recibidos por uno de los puertos de los otros PCs.

6- Evaluación

Mediante puntos de control

Departamento de
Automática y Computación
Automatika eta
Konputazio Saila

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

Práctica 5: Encaminamiento entre VLANs mediante conmutadores Cisco Layer 2/3

1- Objetivos

En esta práctica veremos el funcionamiento de un conmutador Layer 2/3 capaz tanto de conmutar tráfico de una misma VLAN y como de encaminar tráfico entre diferentes VLANs.

2- Conocimientos previos

- Funcionamiento de un conmutador Ethernet Layer 2/3
- Acceso por consola a conmutadores y routers Cisco
- Configuración IP en PCs con Linux y en routers Cisco
- Configuración básica y de VLANs en conmutadores Cisco

3- Encaminamiento entre VLANs

Un conmutador Layer 2/3 se puede ver como un conmutador que tiene interfaces virtuales en las VLANs de tal manera que puede encaminar tráfico entre las subredes IP empleadas en las mismas. Lleve a cabo la el conexionado físico de la Figura 1.

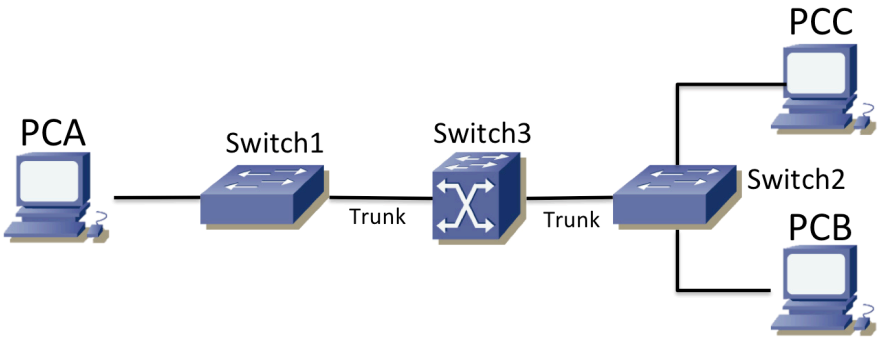


Figura 1.- Dos VLANs encaminadas a través de un conmutador Layer 2/3

El puerto de switch1 a PC A y el de switch2 a PC C están en la VLAN 2, mientras que el puerto de switch2 a PC B está en la VLAN 3. Los puertos de los enlaces que conectan los conmutadores 1 y 2 con el conmutador Layer 2/3 (etiquetado en el armario como Switch3) se tienen que configurar en modo trunk. PCA y PCC tendrán configurada dirección IP de la subred A mientras que PCB de la subred B. El conmutador Layer 2/3 encaminará el tráfico entre las diferentes VLANs. El objetivo es lograr la topología de capa 3 que se ve en la figura 2.

Departamento de
Automática y Computación
Automatika eta
Konputazio Saila

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

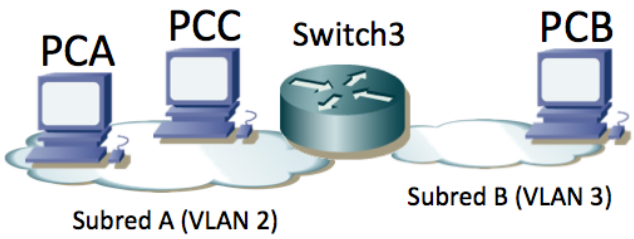


Figura 2 – Topología de capa 3

El conmutador Layer 2/3 es similar a los otros conmutadores Cisco que se han usado hasta ahora. Por defecto trae creada una VLAN, la VLAN 1, y todos los puertos asignados a ella de forma nativa (sin encapsulación 802.1Q). Pueden ver esto con el comando:

```
Switch> show vlan
```

El conmutador Layer 2/3 va a encaminar el tráfico entre la VLAN 2 y la VLAN 3. Primero pongan el conmutador en modo VTP transparente:

```
Switch(config)# vtp mode transparent
```

A continuación creen las VLANs de número 2 y 3 con el comando `vlan`.

```
Switch(config)# vlan 2
```

Ahora ya podrían comunicarse entre los PCs de la misma VLAN, es decir, entre PC A y PC C. Para comunicarse entre PCs de diferentes VLANs es necesario configurar la parte de encaminamiento de paquetes IP del switch3. Hay que darle un interfaz IP en cada una de las subredes IP (tendremos una en cada VLAN).

En primer lugar, como en los routers Cisco hay que activar su capacidad de encaminar:

```
Switch(config)# ip routing
```

A continuación el equipo va a tener un interfaz de nivel 3 (IP) en cada vlan. Este interfaz se llama como la VLAN. Para entrar a configurar este interfaz debe hacer:

```
Switch(config)# interface vlan <ID>
```

Configure las direcciones IP de las interfaces virtuales de las VLANs 2 y 3 del conmutador Layer 2/3. Puede ver la tabla de direcciones IP y la tabla de rutas del conmutador como lo haría en un router Cisco.

Pruebe a hacer ping entre PC A y PC B. ¿Qué sucede? ¿Qué le falta por configurar? Corrija los posibles problemas.

Compruebe mediante tcpdump o wireshark que el tráfico entre el PC A y el PC C se está conmutando, mientras que el tráfico entre PC A y PC B se está encaminando a través del conmutador Layer 2/3.

¿Qué camino físico seguirán los paquetes de un ping del PC A al PC C? ¿Y uno entre PC A y PC B? ¿Y entre PC B y PC C?

Punto de control: Muestre la configuración funcionando y la captura del tráfico a su profesor de prácticas.

Departamento de
Automática y Computación
Automatika eta
Konputazio Saila

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

4- Múltiples VLANs

Esta vez, en vez de dar el diagrama físico y/o lógico de la red e indicar paso-a-paso qué tiene que configurar, simplemente se le va a indicar las conexiones físicas a realizar, su modo de funcionamiento y la puerta de enlace por defecto (siguiente salto) de cada VLAN. **Primero debe dibujar en un papel las topologías físicas y lógicas de la red** y posteriormente realizar la configuración. Es decir, por un lado la topología de conmutadores capa 2 para cada VLAN y por otro lado tal y como lo ve IP, ignorando la estructura de cada LAN y viendo solo los equipos de interconexión entre subredes (los routers). **No se corregirá el punto de control si no se tienen estos esquemas dibujados.**
Hay 3 VLANs y 3 subredes IP, la subred 1 en la VLAN 1, la subred 2 en la VLAN 2 y la subred 3 en la VLAN3. Puede decidir el rango de direcciones de cada subred IP.

- Conecte el eth0 del PC A al puerto 1 del Switch 1. Este puerto estará en la VLAN 1.
- Conecte el eth0 del PC B al puerto 9 del Switch 1. Este puerto estará en la VLAN 3.
- Conecte el puerto 1 del Switch 3 al puerto 17 del Switch 1. Este enlace estará en modo trunk.
- Conecte el puerto 2 del Switch 3 al puerto 17 del Switch 2. Este enlace estará en modo trunk.
- Conecte la interfaz GigabitEthernet0/0/0 del Router 2 al puerto 2 del Switch 1. Este puerto estará en la VLAN 1.
- Conecte la interfaz GigabitEthernet0/0/1 del Router 2 al puerto 2 del Switch 2. Este puerto estará en la VLAN 3.
- Conecte la interfaz GigabitEthernet0/0/0 del Router 3 al puerto 3 del Switch 3. Este puerto estará en la VLAN 3.
- Conecte la interfaz GigabitEthernet0/0/1 del Router 3 al puerto 9 del Switch 2. Este puerto estará en la VLAN 2.
- Asigne en el Switch 3 direcciones IP en los interfaces virtuales correspondientes a las VLAN 1 y 2. El interfaz de la VLAN 1 tendrá dirección IP de la subred 1. El interfaz de la VLAN 2 tendrá dirección IP de la subred 2. No asigne dirección IP al interfaz virtual de la VLAN 3.
- Asigne direcciones IP apropiadas a los eth0 del PC A y PC B, y a los FastEthernet y Ethernet de los Router 2 y 3.

Rutas por defecto:

- El router por defecto para los hosts (los PCs) de la subred 1 es la dirección IP asignada al interfaz virtual del Switch 3 en la subred 1.
- El router por defecto para los hosts (los PCs) de la subred 2 es la dirección IP asignada al interfaz del Router 3 en esa subred. Con lo descrito no hay ningún host en la subred 2 pero puede configurar el PC C en esa subred o en otras para llevar a cabo pruebas de conectividad.
- El router por defecto para los hosts (los PCs) de la subred 3 es la dirección IP asignada al interfaz del Router 2 en esa subred.
- El Switch 3 tiene una ruta por defecto vía la dirección IP del router 3 en la subred 2.
- El router 3 tiene una ruta por defecto vía la dirección IP del router 2 en la subred 3.

Departamento de
Automática y Computación
Automatika eta
Konputazio Saila

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

- El router 2 tiene una ruta por defecto vía la dirección IP del switch 3 en la subred 1.

Una vez completada la configuración estudie el camino que siguen los paquetes entre cada máquinas de cada pareja de subredes. Analice por un lado el camino en capa 3 (saltos entre routers) como el camino físico (saltos entre equipos físicos, sean conmutadores capa 2, capa 3 o capa 2/3). ¿Qué sucede si mandan un paquete a una dirección IP que no pertenece a ninguna de las subredes configuradas?

Punto de control: Muestre esta última configuración funcionando.

5- Switch capa 2/3 + STP

Partiendo de la configuración del apartado anterior conecte mediante un enlace de trunk el switch2 con el switch 1. Modificando las prioridades de los conmutadores puede conseguir diferentes árboles de expansion en cada VLAN. Consiga mediente esto (si es possible) diferentes caminos físicos para el tráfico entre los PCs, aunque los saltos en capa 3 sigan siendo los mismos.

6- Evaluación

Mediante puntos de control

upna Universidad Pública de Navarra Nafarroako Unibertsitate Publikoa

Departamento de
Automática y Computación
Automatika eta
Konputazio Saila

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

Práctica 6: 802.1Q en routers Cisco. Routing y Bridging

1- Objetivos

Con esta práctica completamos los temas alrededor de la configuración de equipos con interfaces Ethernet. Para ello veremos cómo emplear 802.1Q en routers Cisco y finalmente haremos que un router actúe simultáneamente como un puente.

2- Conocimientos previos

- Configuración IP básica de PCs con Linux y de routers Cisco
- VLANs y 802.1Q
- Configuración básica y de VLANs en conmutadores Cisco

3- 802.1Q en router Cisco

Sobre el interfaz físico Ethernet de un router Cisco se pueden configurar interfaces "virtuales", en concreto nos interesan en esta práctica los "subinterfaces". Indica la documentación de Cisco:

"A subinterface is a mechanism that allows a single physical interface to support multiple logical interfaces or networks. That is, several logical interfaces or networks can be associated with a single hardware interface."

Queremos que un interfaz del router pueda enviar tramas ethernet con encapsulado 802.1Q y etiquetas de diferentes VLAN. Si el puerto del conmutador al que está conectado está en "trunk" y acepta tramas de todas esas VLANs entonces podremos conseguir que efectivamente el router tenga un interfaz lógico en cada VLAN.

Conecte un interfaz ethernet del router2 a un puerto del switch1. Active ese interfaz (`no shutdown`) en el router y configure el puerto del switch para que esté en trunk. Cree un par de VLANs en el switch (por ejemplo la VLAN 2 y la 3).

Vamos a crear un subinterfaz en el router para cada VLAN. El subinterfaz representará al interfaz del router en esa LAN. Los subinterfaces se indentifican por un número. Para recordar mejor qué subinterfaz corresponde a cada VLAN los identificaremos con el número de la VLAN (aunque no es obligatorio). Para entrar en el modo de configuración del subinterfaz 2 deberá usar (según cuál sea el interfaz que esté empleando):

```
Router(config)# interface GigabitEthernet0/0/0.2
```

Ahora, en el modo de configuración de ese subinterfaz indique que desea emplear encapsulado 802.1Q y la VLAN 2 (comando `encapsulation`).

Asigne dirección IP a este subinterfaz en una LAN, por ejemplo en la LAN `192.168.1.0/24` (que llamaremos LAN A).

Repita los pasos con el subinterfaz 3, asignándolo a la VLAN 3 y con dirección IP en la LAN B (que debe ser independiente de la LAN A)

Puede ver ahora ambos interfaces por ejemplo con:

```
Router# show ip interface brief
```

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

Y vea también las entradas en la tabla de rutas.

Para probar la configuración colocaremos un PC en cada una de esas VLANs.

Conecte el interfaz 0 del PC A al switch1 y configure ese puerto del switch en modo acceso y en la VLAN 2. Configure la IP del interfaz del PC dentro de la LAN A. Configure la ruta por defecto de este PC con siguiente salto la IP del router en la LAN A.

Conecte el interfaz 0 del PC B al switch1 y configure ese puerto del switch en modo acceso y en la VLAN 3. Configure la IP del interfaz del PC dentro de la LAN B. Configure la ruta por defecto de este PC con siguiente salto la IP del router en la LAN B.

Pruebe a hacer ping y traceroute entre ambos PCs y verifique el correcto funcionamiento de la comunicación y que efectivamente los paquetes están siendo enrutados por router.

Punto de control: Muestre esta última configuración a su profesor de prácticas

4- Router Cisco como puente

Cisco IOS permite que un router actúe también como un puente entre varios interfaces. Es decir, se puede hacer que varios interfaces del router actúen como interfaces enrutados con normalidad mientras que otros se unan para formar un puente. Sería equivalente a lo que se representa en la figura 1. En esta figura tenemos un router con 8 interfaces. Entre 3 de ellos está enrutando IP. Otros 3 están siendo puenteados y los dos restantes forman un puente diferente. Ni las tramas ethernet ni los paquetes IP pueden pasar de un dominio a otro. Es decir, un paquete IP en uno de los dominios de broadcast no será reenviado por el otro dominio ni salir por uno de los interfaces enrutados.

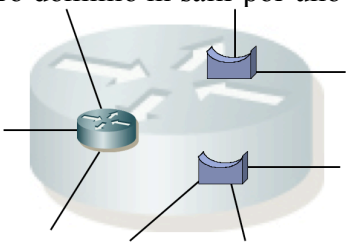


Figura 1.- Router Cisco actuando simultáneamente como puente

Lo que vamos a hacer en este apartado es simplemente configurar los 2 interfaces ethernet de un router (por ejemplo router2) como un puente. Tradicionalmente, Cisco IOS permite que haya unos interfaces enrutados y otros puenteados mediante lo que llama CRB (*Concurrent Routing and Bridging)* o mediante IRB *(Integrated Routing and Bridging)*. En los routers ISR4221 del laboratorio se está empleando Cisco IOS XE. Esta versión permite implementar lo descrito mediante las funcionalidades asociadas a EVCs (Ethernet Virtual Connections).

Conecte un PC a cada interfaz Ethernet del router2. Asigne direcciones IP de la misma subred a los interfaces del PC. Verifique que los interfaces del router están activados pero no configure direcciones en ellos. Compruebe que no hay comunicación entre los PCs (por ejemplo no puede hacer ping de uno a otro, el ARP que envía uno no lo recibe el otro, etc).

Vamos a configurar los dos interfaces Ethernet de router2 en el mismo dominio de broadcast o lo que Cisco llama un "*Bridge Domain*". De esa forma el router estará actuando como un puente (no cambiaremos nada en los PCs). Para ello debe entrar en la configuración de cada interfaz del router y crear un interfaz lógico creando lo que se llama un "Ethernet Flow Point (EFP) service instance".

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

Este interfaz lógico nos permitirá crear la asociación entre el interfaz físico y el *bridge domain*. Al crear esta *service instance* debe asignarle un número que debe ser único *dentro de ese interfaz*; esto es así porque se pueden crear múltiples *service instances* en el mismo interfaz y este número sirve para diferenciarlas (no necesitan ser diferentes de las creadas en otro interfaz).

Una vez dentro de la configuración de la *service instance* debemos indicarle qué tráfico del interfaz queremos que se asigne a la misma. En este caso asignaremos todo el tráfico que venga sin encapsulado 802.1Q (el tráfico *untagged*). Finalmente, crearemos la asociación entre la *service instance* y un bridge domain.

Todo esto se ve en los siguientes comandos:

```
interface GigabitEthernet0/0/0
 service instance 1 ethernet
  encapsulation untagged
  bridge-domain 1
```

Puede repetir estos comandos para el segundo interfaz Ethernet. Es importante que el valor numérico indicado en el comando *bridge-domain* sea el mismo, dado que es lo que hará que ambos interfaces asocien las tramas sin encapsulado 802.1Q al mismo puente. El valor numérico de identificador de la *service instance* podría ser diferente.

Compruebe que ahora sí hay comunicación entre los PCs, siendo puenteadas las tramas que envían.

5- Router Cisco como puente con interfaz virtual enrutado

IOS permite enrutar paquetes IP entre interfaces puenteados e interfaces enrutados. Para ello crea un interfaz lógico asignado al *bridge domain*. Este interfaz se llama un BDI (*Bridge Domain Interface)* Ese interfaz lógico actúa como un interfaz capa 3 del router, conectado a dicho puente como se representa en la figura 2. El icono de conmutador y de router representan esas funcionalidades de capa 2 y capa 3 que está llevando a cabo de forma simultanea el router. Externamente, para los equipos conectados no hay forma de reconocer que el router no es en realidad dos equipos.

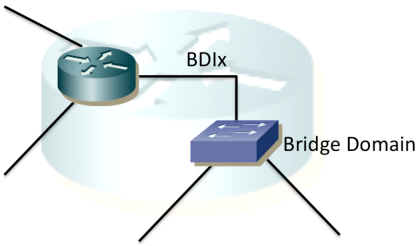


Figura 2.- Router Cisco con 3 interfaces enrutados, de los cuales uno es un BDI

Puede crear el interfaz lógico mediante:

```
Router(config)# interface bdi 1
```

Dentro del modo configuración de este interfaz virtual podremos asignarle dirección IP teniendo en cuenta que como se representa en la figura 2 ese es el interfaz del router en esa LAN.

Vamos a probar una configuración de este estilo creando la topología de capa 3 que se ve en la

figura 3.

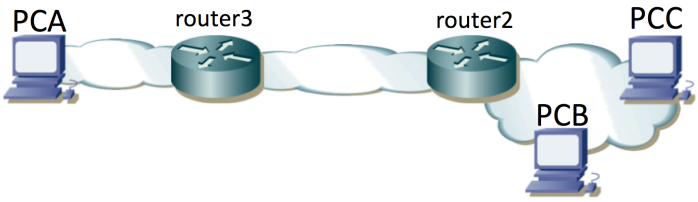


Figura 3 – Topología de red IP objetivo

Como se puede ver, en esa figura los equipos router2, PCB y PCC se encuentran en la misma subred IP. Por ello deben tener un interfaz en el mismo dominio de broadcast. Podríamos crear ese dominio empleando un conmutador Ethernet al cual se conectaran los tres equipos pero lo vamos a hacer con la funcionalidad descrita en esta práctica. La topología física a crear es la que se muestra en la figura 4.

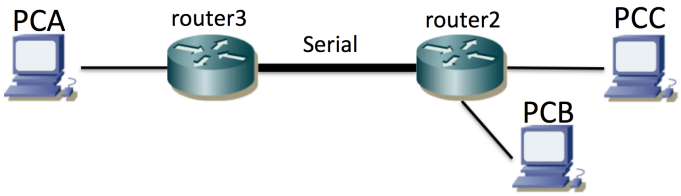


Figura 4 – Topología física

Con este conexionado físico PCB y PCC estarían conectados a diferentes interfaces enrutados de router2, por lo que no estarían en el mismo dominio de broadcast y no podrían comunicarse con una configuración con direcciones IP en la misma subred (un ARP que enviara uno no llegaría al otro). Debemos convencer a router2 de que puentee esos dos interfaces creando un *bridge domain*. El resultado será algo parecido a lo que se muestra en la figura 5, donde hemos representado de nuevo el *bridge domain* con el icono de un conmutador. Los iconos de conmutador y de router son funciones que lleva a cabo el mismo equipo router2 y que hemos separado para entenderlas mejor. El interfaz BDI1 es el interfaz enrutado que tiene el equipo en el dominio de broadcast al que se asigna el tráfico sin tag de los dos interfaces Ethernet del mismo.

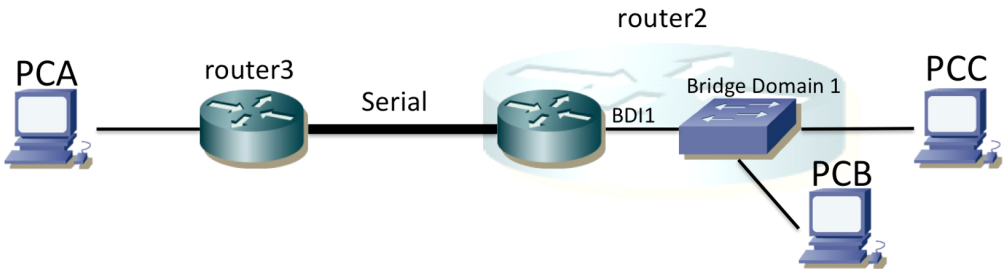


Figura 5 – Topología incluyendo elementos virtuales

Averigüe la dirección MAC que está empleando el router en ese BDI.

Configure las tablas de rutas de PCs y routers para tener conectividad IP entre todos los equipos.

Departamento de
Automática y Computación
Automatika eta
Konputazio Saila

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

Compruebe que la comunicación entre PCB y PCC es puenteada mientras que con PCA es enrutada, siguiendo los saltos que se ven en la topología.

Punto de control: Muestre esta última configuración a su profesor de prácticas

6- Evaluación

Mediante puntos de control

Departamento de
Automática y Computación
Automatika eta
Konputazio Saila

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

Práctica 7- Configuración de VRRP en routers Cisco

1- Objetivos

En esta práctica configuraremos VRRP y veremos su funcionamiento en varios escenarios.

2- Conocimientos previos

- Funcionamiento de VRRP[3]
- Configuración de IP en PCs Linux
- Configuración de interfaces Ethernet y serie en routers Cisco
- Gestión de conmutadores Cisco

3- Escenario con un solo grupo VRRP

Lleve a cabo el interconexionado de la figura 1. Para los conmutadores puede emplear dos switches Cisco o el mismo equipo y dos VLANs.

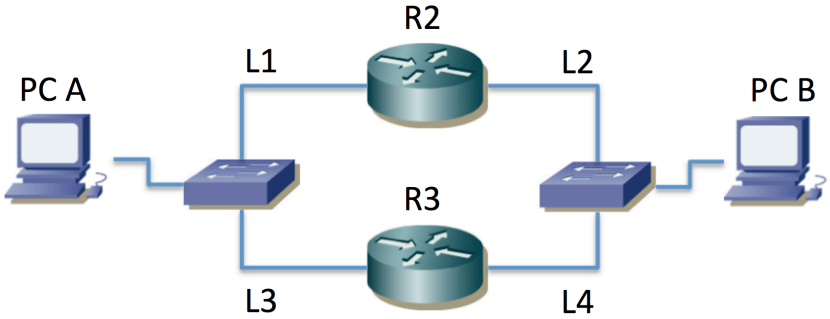


Figura 1 – Topología física

Figura 2 – Topología capa 3

Cree dos subredes IP (A y B). Como no se va a interconectar con el resto del laboratorio puede emplear el rango de direcciones que desee. En la figura 1 se han etiquetado también los enlaces. Al interfaz de R2 en el enlace L1 lo llamremos $R2_{L1}$ y al resto de forma análoga. PCA se configurará en la subred A y PCB en la subred B. Asigne direcciones IP a los interfaces de los PCs y los routers en las correspondientes subredes. Puede probar la configuración añadiendo rutas por defecto a los PCs y probar así la comunicación entre ellos pero tras las pruebas *borre esas rutas por defecto*.
Un interfaz podría formar parte de varios grupos VRRP pero en esta parte trabajaremos solo con un grupo. El grupo VRRP que crearemos estará en la subred A y lo formarán los interfaces $R2_{L1}$ y $R3_{L3}$.
La configuración de un grupo VRRP en un router Cisco se hace dentro de la configuración del interfaz que va a formar parte de dicho grupo. Entre en el modo de configuración del interfaz $R2_{L1}$.

[3] Esta práctica no pretende ser un tutorial sobre el funcionamiento de VRRP. Para entender el protocolo recurra a las clases de teoría o a la RFC 3768 sobre la versión 2 de VRRP.

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

Consulte la ayuda en línea del comando *vrrp*. La configuración básica será indicar la dirección IP y el identificador del router virtual (VRID, Virtual Router IDentifier). Esto lo puede hacer mediante el comando:

```
Router(config-if)# vrrp {VRID} ip {direccionIPvirtual}
```

Como VRID puede elegir un número entre 1 y 255. La dirección IP virtual es la que se va a proteger con varios interfaces. Escoja una dirección IP libre de la subred A[4]. Tras aplicar el comando podrán aparecer mensajes correspondientes a cambios de estado del proceso de VRRP para ese grupo. Dado que hemos configurado de momento solo un interfaz en el grupo debería terminar en pocos segundos ese interfaz como Maestro del mismo. Puede ver el estado de la configuración de VRRP con comandos como:

```
Router# show vrrp
Router# show vrrp brief
```

Repita la configuración en el interfaz $R3_{L3}$. El VRID y la dirección IP virtual deben ser la misma así que el comando a aplicar es el mismo. A continuación vea con los comandos *show* anteriores el estado en cada router. ¿Quién es el maestro? ¿Por qué?
Configure la dirección IP del router virtual como router por defecto de PCA. Configure la dirección IP de $R2_{L2}$ como ruta por defecto de PCB.
Haga ping desde PCA a la dirección IP del router virtual. Capture el tráfico en el propio PCA. ¿Cuál es la dirección MAC destino de los *echo request*? ¿Y la dirección MAC origen de los *echo reply*? Inspeccione la base de datos de filtrado (tabla de direcciones MAC) del conmutador de la LAN A y localice el interfaz físico que está contestando. ¿Qué relación hay entre la dirección IP virtual y las MACs que observa? ¿Qué se observa en el tráfico de la subred B?
Verá también en PCA mensajes del protocolo VRRP. Estudie el formato de los mismos. ¿Qué interfaz o interfaces los envían? En el momento que ha activado la captura ya se había decidido quién era el interfaz maestro y cuál el de backup. Si desconfigura VRRP en los routers (vale con poner "no" delante del comando en cada interfaz del grupo) y pone la captura en PCA antes de hacer la configuración, al hacerla tal vez pueda ver una secuencia diferente de mensajes.
Se puede configurar un valor de prioridad para controlar cuál de los interfaces del grupo es el maestro[5]. Esto se hace mediante el comando:

```
Router(config-if)# vrrp {VRID} priority {valorDePrioridad}
```

¿Qué valor de prioridad se está empleando por defecto?
El interfaz con mayor valor de prioridad se convertirá en el maestro. En caso de que aparezca un nuevo interfaz con mayor prioridad que el maestro pasará este nuevo a ser el maestro si está activada la *preemption*. Por defecto en IOS suele estarlo.
Configure la prioridad para que el maestro sea $R3_{L3}$. ¿Qué camino seguirá el tráfico de ida y de vuelta del ping entre PCA y PCB?

---

[4] La dirección IP virtual podría ser la dirección IP de uno de los interfaces que van a formar el grupo, pero de momento no vamos a optar por ello.
[5] Por simplicidad crearemos en esta práctica solo grupos de 2 interfaces pero el protocolo no está limitado a esta cantidad.

Departamento de
Automática y Computación
Automatika eta
Konputazio Saila

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

A continuación, mientras tiene funcionando el ping de PCA a PCB, desconecte físicamente el cable que va a $R3_{L3}$. Observe los paquetes en PCA. ¿Se recupera la conectividad? ¿Cómo, cuándo? ¿Qué interfaz es ahora el maestro? Reconecte el cable que va a $R3_{L3}$. ¿Qué sucede ahora?
¿Qué hubiera sucedido ante la desconexión anterior si el router por defecto en la subred B hubiera sido $R3_{L4}$?

Punto de control: Muestre a su profesor de prácticas un escenario de desconexión de cable en el que se recupere la conectividad entre los PCs.

Revise el contenido de las bases de datos de filtrado de los conmutadores de las LANs cuando haga cambios de router maestro.
Pruebe un escenario de desconexión del interfaz de backup y compruebe que no tiene efecto sobre el tráfico en curso.

4- Escenario con dos grupos VRRP

Manteniendo la topología de la figura 1 y un grupo VRRP en la subred A, configure ahora un grupo VRRP también en la subred B, entre los interfaces $R2_{L2}$ y $R3_{L4}$.
Configure R2 como maestro en ambas subredes y pruebe los efectos de la desconexión de diferentes cables a interfaces de routers mientras tiene tráfico entre los PCs. Compruebe que el comportamiento se ajusta a lo previsto.
Configure R2 como maestro en la subred A y a R3 como maestro en la subre B y repita el ejercicio.

5- Caminos diferentes

Lleve a cabo el interconexionado de la figura 2. Para los conmutadores puede emplear dos switches Cisco o el mismo equipo y dos VLANs.

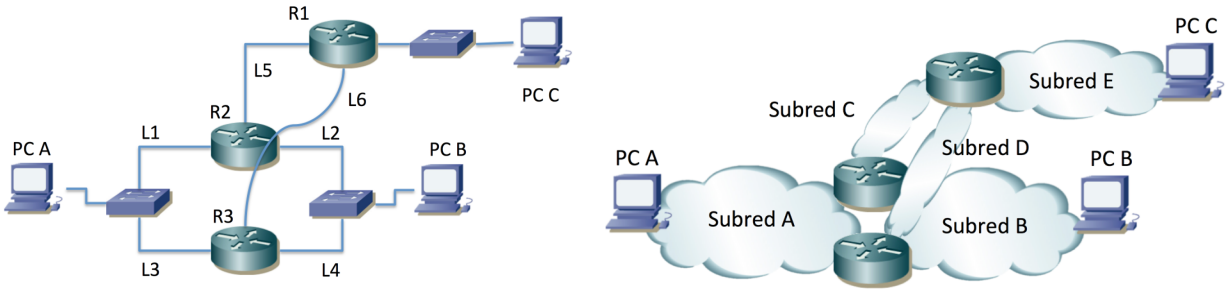


Figura 2 – Topología (a) física y (b) de nivel de red

Los enlaces L5 y L6 emplean interfaces serie. Configure una velocidad mucho más baja en el enlace L6 que en el enlace L5 (así notaremos en el retardo del ping por dónde va el tráfico).
Configure R2 y R3 para que formen un grupo VRRP en la subred A. Asigne la dirección virtual del grupo como router por defecto en PCA. El maestro del grupo será R2.
Configure R2 y R3 para que formen un grupo VRRP en la subred B. Asigne la dirección virtual del grupo como router por defecto en PCB. El maestro del grupo será R3.
El router por defecto de PCC será el interfaz de R1 en la subred E.
En R1 configure una ruta por defecto cuyo siguiente salto sea la dirección del interfaz $R2_{L5}$.
En R2 configure una ruta por defecto cuyo siguiente salto sea la dirección del interfaz $R1_{L5}$.
En R3 configure una ruta por defecto cuyo siguiente salto sea la dirección del interfaz $R1_{L6}$.
¿Qué camino sigue el tráfico entre cada par de hosts?
Desconecte interfaz $R2_{L1}$. Compruebe los cambios en los caminos.

Departamento de
Automática y Computación
Automatika eta
Konputazio Saila

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

Reconecte el interfaz $R2_{L1}$.
Deconecte el interfaz $R3_{L4}$. Compruebe los cambios en los caminos.
Reconecte el interfaz $R3_{L4}$.
Desactive el interfaz $R3_{L6}$. Compruebe los cambios en los caminos.
Reactive el interfaz $R3_{L6}$.
Desactive el interfaz $R2_{L5}$. Compruebe los cambios en los caminos.
Reactive el interfaz $R2_{L5}$.

Punto de control: Avise al profesor de prácticas y responda a preguntas sobre el escenario, las pruebas que ha llevado a cabo y los resultados de las mismas.

6- Varios grupos VRRP en la misma subred

Construya un escenario similar a la figura 2 pero retire de ella la subred B. Conecte PCB en la subred A. Ahora tiene dos poblaciones de usuarios en la subred A, una de las cuales viene representada por PCA y la otra por PCB.
Cree dos grupos VRRP diferentes entre los interfaces de R2 y R3 en la subred A. La dirección IP de uno de ellos la configurará como ruta por defecto de PCA y la del otro para la ruta por defecto de PCB.
Compruebe el correcto funcionamiento de esta configuración y los caminos que usan los flujos entre las diferentes parejas de hosts.

7- Evaluación

Mediante puntos de control.

Departamento de
Automática y Computación
Automatika eta
Konputazio Saila

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

Práctica 8- Configuración de Access Point y cliente WiFi

1- Objetivos

En esta práctica veremos el funcionamiento básico de una red WiFi en la que tenemos un punto de acceso (Access Point, AP) comercial y clientes WiFi PCs con sistema operativo Linux. Configuraremos PCs como clientes de este AP, simultáneamente a PCs en el sistema de distribución cableado. Finalmente, emplearemos las funcionalidades de enrutamiento de los equipos para encaminar el tráfico de la red inalámbrica hacia el laboratorio.

2- Conocimientos previos

- Conocimientos básicos sobre WiFi
- Configuración de IP en PCs Linux

3- Acceso y configuración de un AP/WirelessRouter comercial

En primer lugar vamos a ver un típico interfaz de configuración de un punto de acceso comercial de bajo coste. En el armario de prácticas dispone de un Cisco Linksys WRT54G. Si ha encontrado el manual de configuración sabrá que dispone de un servidor web interno mediante el cual sirve unas páginas que permiten especificar los parámetros de configuración del equipo. El equipo funciona no solo como un AP sino también como un router (si funcionara solo como AP no necesitaría implementar el nivel IP). Por ello tiene dos interfaces, uno es el llamado interfaz WAN y el otro el interfaz LAN. En el interfaz LAN dispone de un switch de 4 puertos FastEthernet. Por defecto está preconfigurado para ser accesible su servidor web de configuración solo através del interfaz LAN. El manual de configuración del equipo especifica la dirección IP y máscara de subred empleada en él. Configure en el PC B una dirección de la misma red, interconéctelos y acceda mediante un navegador a la página web que sirve el equipo. Si tiene problemas pruebe a resetear la configuración del equipo (debería estar indicado cómo hacerlo en su manual).

Si ignoráramos el interfaz WAN y por lo tanto la capacidad de encaminamiento del equipo nos encontraríamos con un AP con su interfaz inalámbrico y 4 puertos ethernet en el sistema de distribución cableado.

Estudie las opciones de configuración del equipo. Localice el método de configuración de las siguientes funcionalidades:

- Dirección IP del interfaz LAN o local
- Configuración de la dirección IP del interfaz WAN
- Servidor de DHCP interno para la red local
- Configuración de la tabla de rutas
- SSID
- Canal WiFi
- Velocidad de transmisión de la WiFi

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

- Parámetros de QoS

4- Configuración de un cliente WiFi

A continuación configuraremos un cliente de la WiFi de este accesspoint. Comience por dar a su AP un SSID que le permita distinguirlo del de sus comañeros. Para ello, emplee como SSID el nombre de su armario (por ejemplo "armario15").

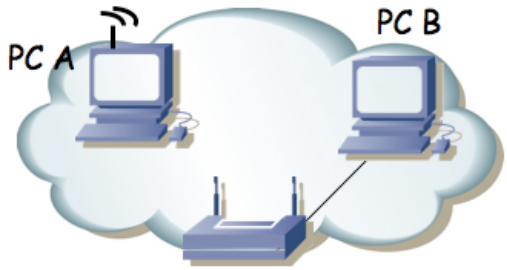


Figura 1.- Accesspoint y cliente

Ahora en PC A configuraremos el intefaz WiFi (`wlan0`). El interfaz puede funcionar en diferentes modos (excluyentes). Los principals son:

- Managed (gestionado): Es el modo en el que se asocia a un punto de acceso.
- Ad-Hoc: Para una WLAN sin punto de acceso (comunicación peer-to-peer entre los terminales inalámbricos).
- Monitor: Permite a aplicaciones (tcpdump, wireshark, tshark, etc) capturar las tramas 802.11. En los otros modos el interfaz y el driver transforman las tramas 802.11 en tramas 802.3 (DIX), además de no entregar al resto del sistema las tramas de gestión de la WLAN.

Para configurar parámetros del protocol IP en el interfaz wlan0 emplearemos *ifconfig* pero para configurar la parte 802.11 usaremos *iwconfig*. Puede ver el estado actual del interfaz con:

```
% iwconfig wlan0
```

Puede ver los canales soportados por su interfaz con:

```
% iwlist wlan0 frequency
```

En primer lugar configure el modo *Managed* si no lo está ya:

```
% sudo iwconfig wlan0 mode managed
```

y active el interfaz (`sudo ifconfig wlan0 up`).

Ahora puede localizar los puntos de acceso a su alrededor con:

```
% sudo iwlist wlan0 scanning
```

Cada WLAN encontrada ha sido por recibir anuncios del punto de acceso. Dichos anuncios (*beacons*) son paquetes 802.11 enviados por la WLAN correspondiente y por lo tanto vienen por uno de los canales de la banda correspondiente (en este caso la de 2.4GHz).

Revise los puntos de acceso que está encontrando. En el listado podrá ver el canal que están empleando. Puede haber varios empleando el mismo canal, en cuyo caso tendrán que compartir la capacidad del mismo (para eso está el control de acceso al medio). Los anuncios le dirán un "nombre" de la WLAN junto a la etiqueta ESSID. Por ejemplo es común que puedan ver el ESSID "UPNA", que es anunciado por los puntos de acceso del Servicio Informático (SI) para acceso a

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

Internet de alumnos. También puede encontrar el ESSID "eduroam". El ESSID es lo que permite distinguir las tramas de un canal si corresponden a una WLAN o a otra que esté empleando el mismo canal.

Debería encontrar en el listado el anuncio el del AP que ha configurado al principio de la práctica. Compruebe la dirección MAC que anuncia ese AP, que es el auténtico identificador de la WLAN en los paquetes. No se confunda entre su punto de acceso y el de otro grupo (si han puesto bien el ESSID deberían ser fáciles de distinguir). ¿Podría intentar adivinar el fabricante de cada AP que ve? Compruebe que el canal es el que ha configurado en su punto de acceso.

Puede que encuentre varios anuncios del ESSID "UPNA", que vendrán con diferente dirección MAC del AP. Esto corresponde a diferentes APs que están anunciando el mismo nombre de WLAN. Aunque empleen el mismo nombre lo que en realidad distingue los paquetes de una WLAN de los de otra del mismo canal es el ESSID (la dirección MAC del AP), el cual no debe coincidir.

En los *beacons* que se reciben como resultado del scan se obtiene también información del tipo de seguridad empleada en la WLAN así como las velocidades soportadas por el AP.

Para asociar el interfaz inalámbrico del PC a un punto de acceso puede hacerlo indicándole al interfaz el ESSID de la WLAN:

```
% sudo iwconfig wlan0 essid NOMBRE
```

Tenga cuidado de no asociarse al AP de otro grupo de prácticas.

A partir de este punto podrá ver con `iwconfig` a qué AP se ha asociado su interfaz WiFi. Confirme la dirección de dicho AP.

Configure una dirección IP de la red local en el interfaz inalámbrico (con *ifconfig*) y compruebe que puede acceder desde PC A al PC B. Si ha dejado activo en su AP un servidor de DHCP podría emplear un cliente de DHCP en el PC ara obtener la configuración IP (esto no es algo particular de WiFi, ni hace falta que el servidor de DHCP esté en el AP, como ya sabrá de otras asignaturas, pero si tiene dudas consulte con el profesor de prácticas). Si tiene interés investigue el programa *dhclient*. En el resto de la práctica se supondrá que ha hecho una configuración manual con *ifconfig*.

Podríamos repetir la configuración del PC A en el PC C y tener con ello dos terminales inalámbricos. Recuerde que la comunicación entre ellos pasa por el punto de acceso (salvo en modo Ad-hoc) y que por lo tanto los paquetes circulan dos veces por el medio aéreo. Además, el control de acceso al medio (CSMA/CA) se emplea en la comunicación de un PC hacia el AP y después desde el AP hacia el otro PC. Reflexione sobre las implicaciones que esto tiene en el throughput que puede obtener una aplicación que intente transferir un fichero de un PC al otro por el medio inalámbrico (suponiendo que los terminales están junto al AP y no hay problemas de interferencias, atenuación, etc).

El driver de estar tarjetas inalámbricas nos permite ver todas las tramas 802.11. Para ello, en lugar de emplear el modo *Managed* y asociarnos a un punto de acceso debemos emplear el modo *Monitor*. En ese modo, las tramas que el driver entregará serán las tramas 802.11 completas, sin ocultarnos además las tramas de gestión (confirmaciones, *probes,* mensajes de autentificación, asociación, etc). Serán las tramas que se reciban por un canal. El interfaz debe sintonizarse a una frecuencia, la de un canal, así que podremos recibir solo las tramas de las WLANs que empleen ese canal y habrá que reconfigurar el interfaz para recibir las tramas de otras WLANs que estén

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

empleando otro canal.

Emplearemos el PC C. Para colocar el interfaz en modo monitor, en primer lugar debe desactivar el interfaz (*sudo ifconfig wlan0 down*) si estaba activo, para a continuación cambiar el modo:

```
% sudo iwconfig wlan0 mode monitor
```

Vuelva a levanter el interfaz.

Configure ahora el interfaz para emplear el canal 1 (probablemente sea el que emplee por defecto):

```
% sudo iwconfig wlan0 channel 1
```

Empiece a capturar del interfaz. Debería ver las tramas 802.11 de todas las WLAN que están empleando ese canal. Si por ejemplo configuró su AP en el canal 5 no verá sus tramas y tendrá que reconfigurar el interfaz para que se sintonice en ese canal.

Empleando `tcpdump` o `wireshark` para ver todas las tramas estudie:

- Los beacons enviados por el AP
- El proceso de asociación del PC A (desactive y vuelva a activar su interfaz para verlo)
- El envío de paquetes entre un host en la red inalámbrica y otro en la LAN cableada
- Si tiene acceso a otro PC con interfaz inalámbrico o a un smartphone, es muy recommendable que lo use para tener dos equipos inalámbricos comunicándose entre ellos mientras ve las tramas con un tercero. Haga ping de un terminal inalámbrico al otro y estudie las tramas 802.11 que viajan y cómo las reenvía el AP.

Emplee las capacidades de filtrado del sniffer para localizar con mayor facilidad las tramas.

Punto de acceso: Muestre a su profesor de prácticas el escenario con el cliente asociado al AP

5- Router WiFi

Ahora emplearemos ambos interfaces enrutados del Linksys WRT54G. En primer lugar en la sección de configuración del mismo *"Setup – Advanced Routing"* asegúrese de que tiene seleccionado el modo de operación *"Router"*. Si tuviera seleccionado *"Gateway"* entonces el equipo actuaría también como un NAT, lo cual en el siguiente escenario no nos interesa. También es recomandable que en la sección *"Security – Firewall"* desactive la protección del Firewall así como desactive la opción *"Block Anonymous Internet Requests"* (averigüe qué hace esa opción).

A continuación lleve a cabo la configuración de la figura 2. Tenemos 2 redes. En el lado LAN del WRT54G tenemos conectados a PC A y PC B. En el lado WAN tenemos a PC C. Seleccione las subredes que desee para esta configuración y compruebe que funciona la comunicación entre las máquinas de diferentes redes. Vea las tramas 802.11.

Departamento de
Automática y Computación
Automatika eta
Konputazio Saila

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

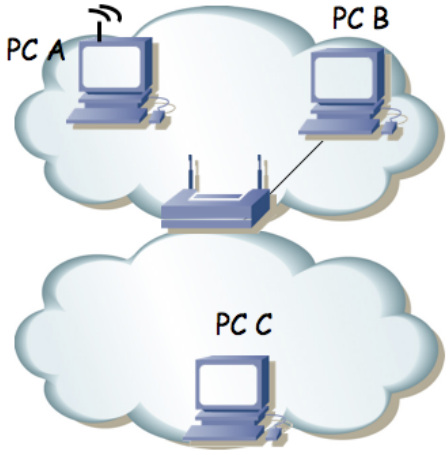


Figura 2.- Router WiFi en funcionamiento

Finalmente lleve a cabo la configuración de la figura 3. En el interfaz LAN empleará una red que depende de su armario de prácticas y será:

`00001010 . 00000011 . 0010 ABCD . XXXXXXXX / 24`

Donde ABCD forma el número de su armario. Por ejemplo en el armario 15 sería: `10.3.47.0/24`.

En el interfaz WAN (conectado al punto C de su puesto de prácticas en la mesa) empleará la configuración IP:

`00001010 . 00000011 . 00010001 . 0000 ABCD / 20`

Donde ABCD forma el número de armario. Por ejemplo en el armario 15 sería: `10.3.17.15/20`. Y el router por defecto en el WRT54G será `10.3.16.1`.

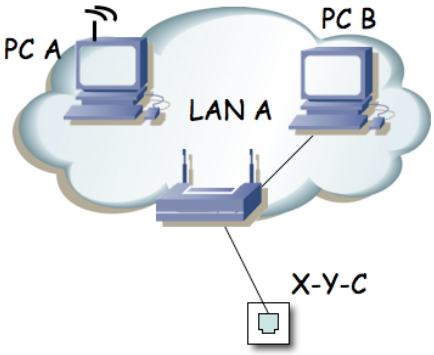


Figura 3.- Acceso de la red WiFi al laboratorio

Punto de control: Muestre el resultado de la configuración anterior

6- Evaluación

Mediante puntos de control

Departamento de
Automática y Computación
Automatika eta
Konputazio Saila

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

Práctica 9- Configuración de accesos ADSL

1- Objetivos

En esta práctica vamos a ver algunos escenarios de configuración del acceso de una LAN a otra red o Internet a través de un enlace ADSL. Empezaremos por los escenarios más simples en los que el equipo de cliente actúa como un puente e iremos pasando a escenarios de mayor complejidad tanto en el equipamiento como en la configuración.

2- Conocimientos previos

- PVCs ATM
- Transporte de IP y Ethernet sobre ATM

4- Escenario bridged

En la figura 1 se muestra la topología física que se va a crear. El equipo routerADSL hace referencia al modem-router que se va a configurar. El equipo C3660 es un router Cisco 3660 que está preconfigurado. Tiene varios interfaces Ethernet y dos interfaces ATM a 155Mbps (sobre un STM-1 SDH; solo entra en juego uno de sus interfaces ATM en esta práctica). En este caso, el enlace que tiene C3660 a DSLAM1 es uno de esos interfaces ATM de fibra. Una de las direcciones IP de este equipo es la 10.4.0.1; puede emplear `telnet` para conectar con ese equipo desde un PC de la red de laboratorio y hacer login en el mismo con usuario tlm y la misma password que las cuentas de los PCs A, B y C. Podrá ver así sus interfaces, direcciones, tabla de rutas, etc (no tiene permiso para subir privilegios con `enable`).

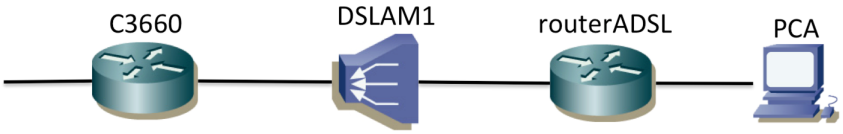


Figura 1 – Topología física a crear

El equipo DSLAM1 es un DSLAM ATM, es decir, tiene interfaces ADSL (de ahí la parte de DSLAM) y lleva a cabo conmutación de celdas ATM. De cara a las celdas se comporta como un conmutador ATM con interfaces ADSL y un interfaz STM-1, el cual va directo a C3660.

En realidad, entre el DSLAM y el router podría haber toda una WAN ATM, por ejemplo una WAN nacional que permita llevar el tráfico de abonados ADSL repartidos por todo el país. Recuerde que los bucles ADSL son cortos (unos pocos kilómetros), así que los DSLAM deben estar cerca de los usuarios. Tendrá que haber múltiples DSLAMs repartidos por las poblaciones (incluso varios en la misma población, si es extensa) y la WAN ATM podría conducir todo el tráfico ATM hasta el mismo agregador (en este caso C3660) o hasta un número reducido de agregadores. Esto se intenta representar en la figura 2.

Departamento de
Automática y Computación
Automatika eta
Konputazio Saila

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

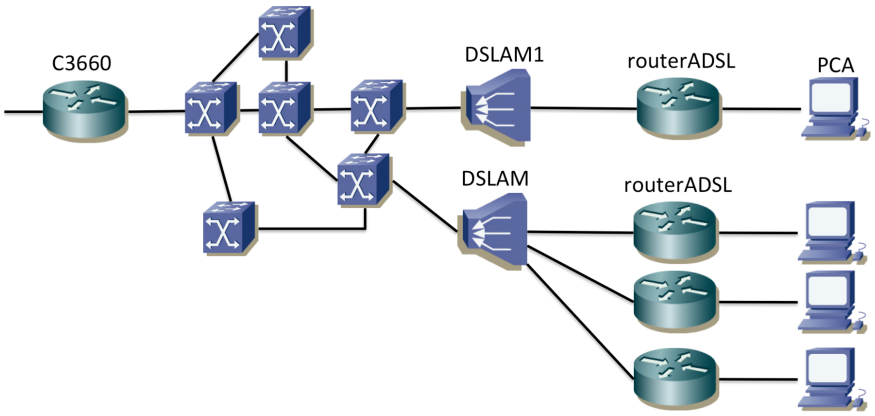


Figura 2 – Posible topología física en un escenario de cobertura nacional

A todos los armarios llega una línea de par telefónico desde el DSLAM1, por lo que en realidad, al haber varios grupos haciendo la práctica, lo que tendremos es lo que se ve en la figura 3.

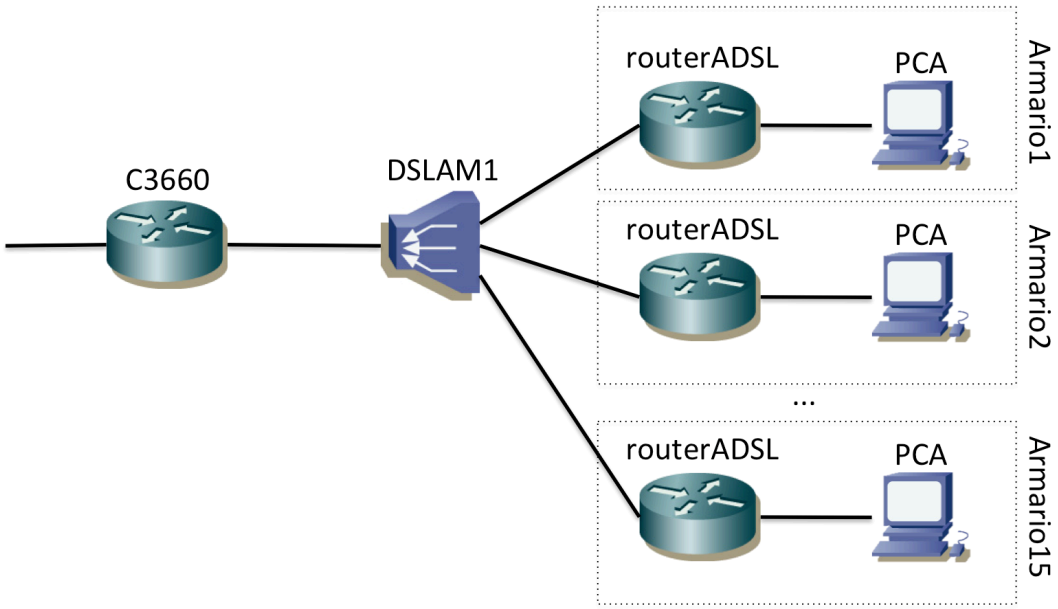


Figura 3 – Topología física en la práctica teniendo en cuenta los grupos de prácticas

Uno de los escenarios más sencillos para la interconexión de redes a través de un enlace ADSL se basa en que el equipo del cliente con el interfaz ADSL actúe como un bridge entre ese interfaz y un interfaz Ethernet del mismo. En nuestro caso el equipo es un router (TP-Link, Linksys o Cisco) que deberá ser configurado para actuar como un puente. En este modo de funcionamiento se enviarán las tramas Ethernet completas que se reciben por el interfaz Ethernet hacia un PVC del interfaz ATM empleado en la línea ADSL.

Lo que queremos obtener es una topología de capa 3 como se ve en la figura 4. En esta ocasión hemos representado el dominio de broadcast con un cilindro en lugar de con una nube.

Departamento de
Automática y Computación
Automatika eta
Konputazio Saila

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

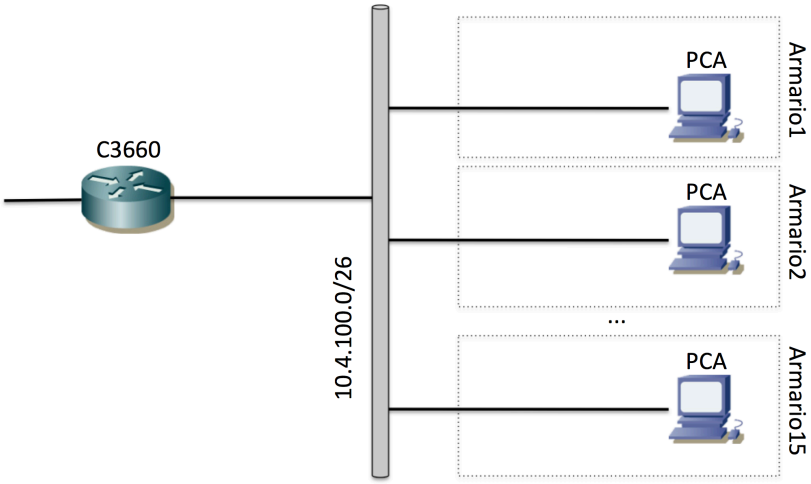


Figura 4 – Topología de capa 3 a obtener. Todos los PCs A y C3660 están en la misma LAN Ethernet puenteada

Es decir, C3660 los PCA de todos los armarios se encontrarán en la misma LAN capa 2 y si les configuramos direcciones IP de la misma subred deberían poder comunicarse entre ellos sin saltos enrutados (solo con saltos puenteados).

Para lograr esto necesitamos en primer lugar que los router ADSL actúen como puentes, pero estos puentes no unen solo interfaces Ethernet sino que deben puentear también hacia el interfaz ADSL. Recuerde que el interfaz ADSL transporta ATM, luego en realidad lo que deben hacer es puentear entre el interfaz Ethernet y algún PVC ATM que emplee en su interfaz ADSL. Esos PVCs ATM terminan en el equipo C3660, pero si queremos un camino puenteado entre los PCs no pueden terminar los PVC en interfaces enrutados de C3660 sino que deben ser puenteados entre ellos. Esto nos lleva a que C3660 deba también puentear entre esos PVCs. Todo esto intenta mostrarse en la figura 5.

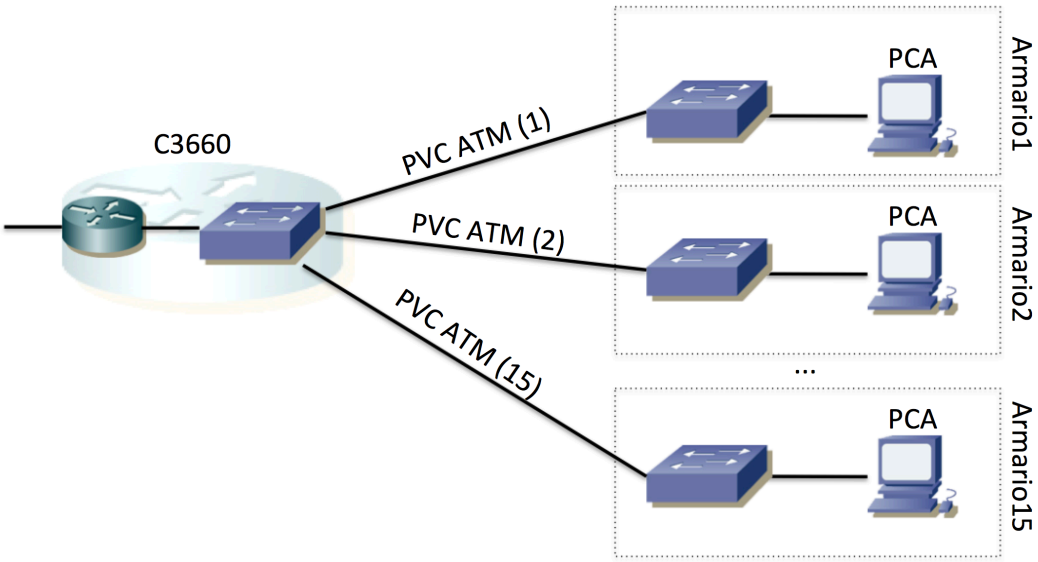


Figura 5 – Topología con visibilidad del equipamiento Ethernet

Departamento de
Automática y Computación
Automatika eta
Konputazio Saila

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

En la figura 5 los conmutadores de los armarios son los routers ADSL actuando como puentes. Los PVC son circuitos virtuales ATM, entidades lógicas que permiten que el paquete que se introduce en el circuito por un extremo aparezca en el otro extremo. En este caso se envían tramas Ethernet. Para los puentes que se muestran en la figura 5 los PVCs actúan como cables punto a punto (a fin de cuenta eso es lo que intentan emular los circuitos y los circuitos virtuales). El router C3660 lo hemos dividido en sus dos funciones lógicas de puente y de router. El interfaz del router al puente es un interfaz lógico; en el caso de este equipo es un BVI en lugar de un BDI debido a la versión de Cisco IOS que corre (en concreto es el BVI1 que puede ver si hace `telnet` al equipo).

El DSLAM (y una potencial WAN ATM) no aparece en la figura 5 dado que no es visible para los equipos Ethernet, pero es el equipo que está conmutando las celdas ATM que envían los routers ADSL y el C3660 para crear esos PVCs. Es decir, si nos fijamos en los PVCs en la red ATM podríamos dibujar algo parecido a la figura 6.

En la figura 6 hemos ocultado todos los enlaces que no transportan celdas ATM. Las líneas rojas representan los PVCs, cuyos extremos como se puede ver están en los routers ADSL y en C3660. Eso quiere decir que la capa de adaptación (AAL5 en este caso) solo es procesada en esos equipos. Aunque todos los routers ADSL generen las celdas como se va a indicar en la práctica con VPI/VCI 8/36, entran en el DSLAM por cables (puertos) diferentes, por lo que la funcionalidad de conmutación ATM del DSLAM puede distinguirlos para conmutarlas todas hacia el interfaz óptico pero con diferente VPI/VCI para cada una, de forma que no se mezclen hacia C3660, que es lo que pasaría si salieran todas las celdas con el mismo VPI/VCI independientemente del PVC. En C3660 los PVCs aparecen identificados con los interfaces lógicos ATM5/0.2xxxxx. Puede ver los interfaces lógicos que están en el puente de C3660 haciendo "`show bridge 1 verbose`" o con "`show bridge 1 group`". Puede ver los valores de VPI/VCI que espera C3660 en esos PVC con el comando "`show atm pvc`". También se le indica ahí el tipo de encapsulación que se espera sobre AAL5. Si pudiéramos ver la tabla de conmutación de DSLAM1 veríamos el mapeo entre los valores de VPI/VCI en el lado hacia C3660 y los valores 8/36 y el interfaz con el par de cobre a cada usuario concreto.

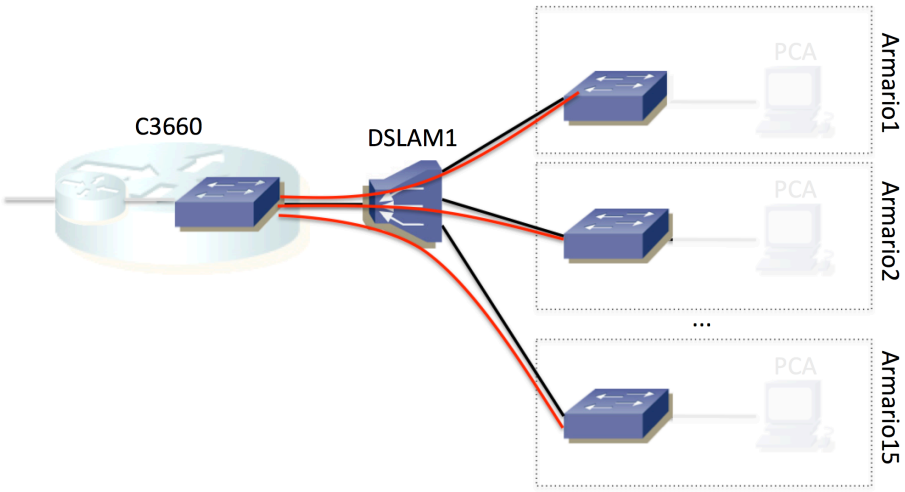


Figura 6 – Topología y PVCs de la sección ATM

En el lado del usuario (en los routers ADSL) emplearemos como hemos comentado el **VPI/VCI 8/36** en todos ellos. El circuito usa AAL5 (para el transporte de paquetes) con encapsulado

LLC/SNAP (se ha decidido esta opción en vez de VC multiplexing de forma arbitraria, pero dado que eso está esperando C3660 es lo que debemos enviar desde los routerADSL). La subred IP común para todos los PCs de los diferentes grupos de prácticas es la red `10.4.100.0/26` y para que no haya conflictos entre los diferentes grupos de prácticas se reparte el bloque de direcciones de esta red de la siguiente forma:

```
00001010 . 00000100 . 01100100 . 00 ABCD XX
```

donde ABCD es el número de armario y XX quedan a disposición de cada grupo de prácticas. Por ejemplo el rango para el armario 15 sería:

```
00001010 . 00000100 . 01100100 . 00 1111 XX = 10.4.100.60 a 10.4.100.63
```

Tenga en cuenta que NO estamos creando subredes, simplemente estamos haciendo un reparto administrativo de las direcciones IP de una red por lo que no hay limitaciones en las IPs a utilizar salvo en el caso del armario 0 (0000) que no podría emplear la que termina en 00 y el armario 15 (1111) que no podría emplear la que termina en 11 (pero como no hay armario 0 ni 15 no tenemos problemas). Eso quiere decir que la máscara siempre es de 26 bits. Podría configurar más PCs en esta red sin más que conectando un conmutador al interfaz LAN de su router (hasta agotar las direcciones que se le han asignado). Esto por ejemplo se ve en la figura 7. En esa figura, para el armario 1 hemos conectado el switch1 al puerto Ethernet del router ADSL en el que antes estaba el PC A. En el caso del armario 2 hemos conectado el segundo PC a otro puerto Ethernet del router ADSL; esto último es posible gracias a que por defecto el router ADSL puentea entre todos los puertos Ethernet.

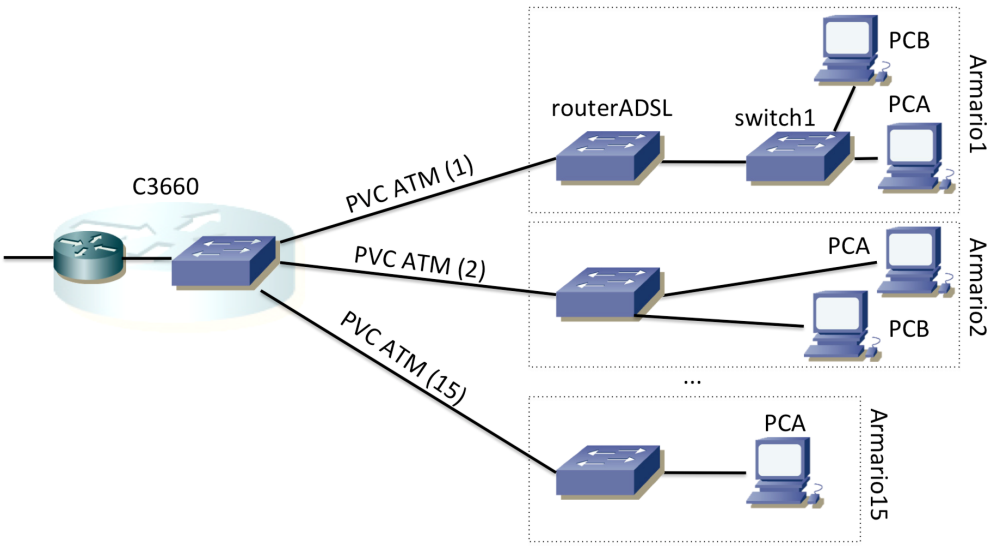


Figura 7 – Escenario con varios PCs de cada armario en la subred IP

Empiece creando este escenario con el Router TP-Link. Verá que éste se configura mediante una página web en la que puede indicar este modo de funcionamiento (Bridge Mode o similar) y el PVC del circuito. Si emplea `10.4.100.1` como router por defecto podrá comunicarse con el resto de las redes del laboratorio (e Internet). Esa es la dirección del inerfaz virtual de C3660 en esa LAN.

Nota: emplee la línea telefónica del armario, que es la que va al DSLAM1, el cual está configurado tal y como se espera para esta práctica y las siguientes sobre ADSL. Busque "DSLAM1" en la documentación de los armarios para saber qué conector del panel de parcheo trae

esa línea.

Una vez tenga sincronizada la línea ADSL en el routerADSL inspeccione la información que éste le ofrezca sobre la misma. ¿A qué velocidad ha sincronizado cada sentido del enlace?

Punto de control: Muestre a su profesor de prácticas el escenario en funcionamiento

5- Escenario 1483 bridged

A continuación vamos a hacer que el router TP-Link enrute, en vez de actuar como un simple puente. En caso de que le ofrezca funcionalidades de NAT desactívelas. Nuestro objetivo es una topología de capa 3 como la que se muestra en la figura 8. En este caso todos los routers ADSL y C3660 tienen un interfaz en la red 10.4.100.0/26. Los PCA están en subredes IP diferentes, al otro lado de los routers ADSL. La red que debe configurar en el lado interno de su routerADSL depende del armario de la siguiente forma:

```
00001010 . 00000100 . 011001 AB . CD XXXXXX / 26
```

donde ABCD corresponde al número de armario. Por ejemplo, en el caso del armario 15 sería:

```
00001010 . 00000100 . 011001 11 . 11 XXXXXX = 10.4.103.192/26
```

Si mira la tabla de rutas de C3660 verá que tiene una ruta a cada una de esas redes con siguiente salto una dirección IP de la subred 10.4.100.0/26. Para que el encaminamiento hacia su subred funcione correctamente debe configurar en el interfaz externo de su routerADSL la dirección IP que tiene como siguiente salto C3660 en la ruta hacia la subred de su armario. Puede ver la tabla de rutas accediendo al interfaz de gestión de C3660. La dirección IP que está configurada para cada ruta es la segunda dirección IP del rango asignado al armario dentro de la red `10.4.100.0/26`. Es decir, en el caso por ejemplo del armario 15 sería la dirección `10.4.100.61` porque `61 = 00 1111 01`, es decir 1111=”armario 15” y 01=”segunda dirección de ese bloque”. Esta puede que fuera la dirección IP que empleó en alguno de sus PCs en el apartado anterior.

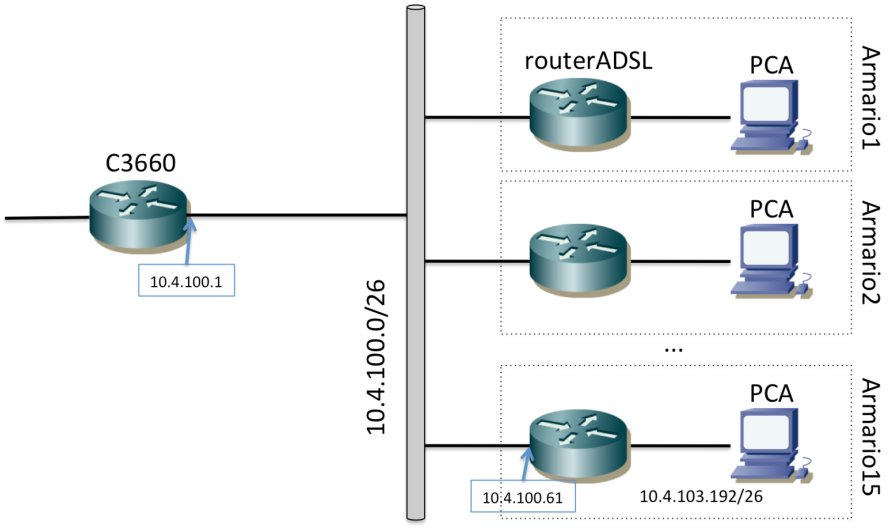


Figura 8 – Topología de nivel IP con enrutamiento en los routers ADSL

Departamento de
Automática y Computación
Automatika eta
Konputazio Saila

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

Emplearemos el mismo PVC de acceso al C3660. Por este PVC (nada ha cambiado en la configuración de C3660) el C3660 espera un encapsulado AAL5 con LLC/SNAP y dentro tramas Ethernet. Debe configurar el router ADSL para que emplee esa encapsulación en el cirtuito virtual. Tenga en cuenta que las tramas Ethernet que envía el PCA ahora no pasan transparentemente el routerADSL pues no actúa como puente. Ahora el routerADSL debe ser el router por defecto de PCA y las tramas Ethernet irán a la dirección MAC de su interfaz Ethernet. Cuando routerADSL quiera reenviar ese paquete IP por el PVC deberá añadirle una nueva cabecera Ethernet, donde la dirección MAC origen deberá ser una dirección que tenga el router ADSL, igual que tendrá que hacer ARPs para resolver la dirección MAC del interfaz Ethernet de C3660 (que es también un interfaz lógico, sobre el puente que hace la unión en capa 2 de los PVCs que veíamos en la figura 6).

En la figura 9 mostramos una representación lógica que algunos fabricantes implementan para estos escenarios. En el caso de la configuración del router TP-Link no va a ver la necesidad de crear estos puentes pero por ejemplo en la configuración de un router Cisco para esa misma funcionalidad tendríamos que crear los dominios de puente y tendríamos un interfaz lógico enrutado que sería el que tendría la dirección MAC Ethernet en el lado WAN del router ADSL.

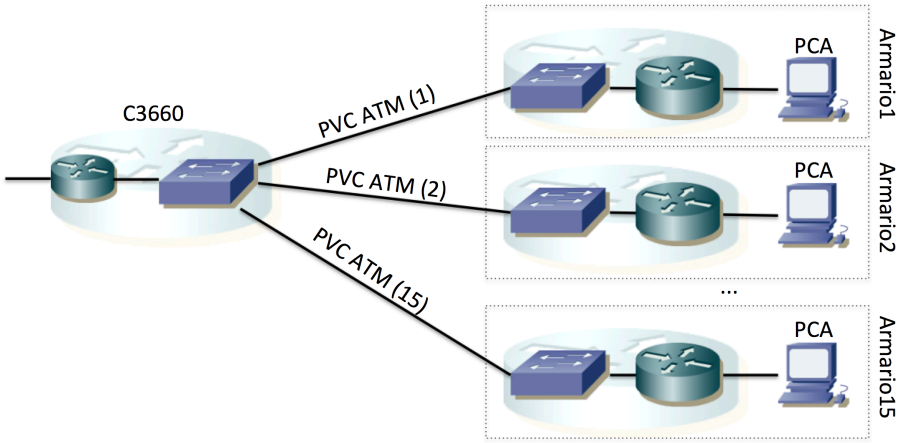


Figura 9 – Escenario 1483 bridged con separación de funciones lógicas

Punto de control: Muestre a su profesor de prácticas el escenario en funcionamiento.

6- Escenario 1483 routed

En este escenario reutilizamos los equipos con una configuración ligeramente diferente. En un escenario 1483 routed se envían los paquetes IP por el PVC ATM sin un encapsulado Ethernet. En nuestro caso emplearán LLC/SNAP y por supuesto AAL5. El otro extremo del PVC sigue teniendo que ser C3660. En el lado del abonado (el lado de los armarios) el **PVC viene identificado con VPI/VCI 8/35**. Esos PVCs, en el lado de C3660 están asignados a unos interfaces lógicos que son directamente interfaces de la funcionalidad de router, como se ve en la figura 10. En la figura hemos mantenido sombreada la parte anterior para recordar que esos PVCs siguen existiendo, y de hecho los emplearemos de nuevo más adelante.

Departamento de
Automática y Computación
Automatika eta
Konputazio Saila

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

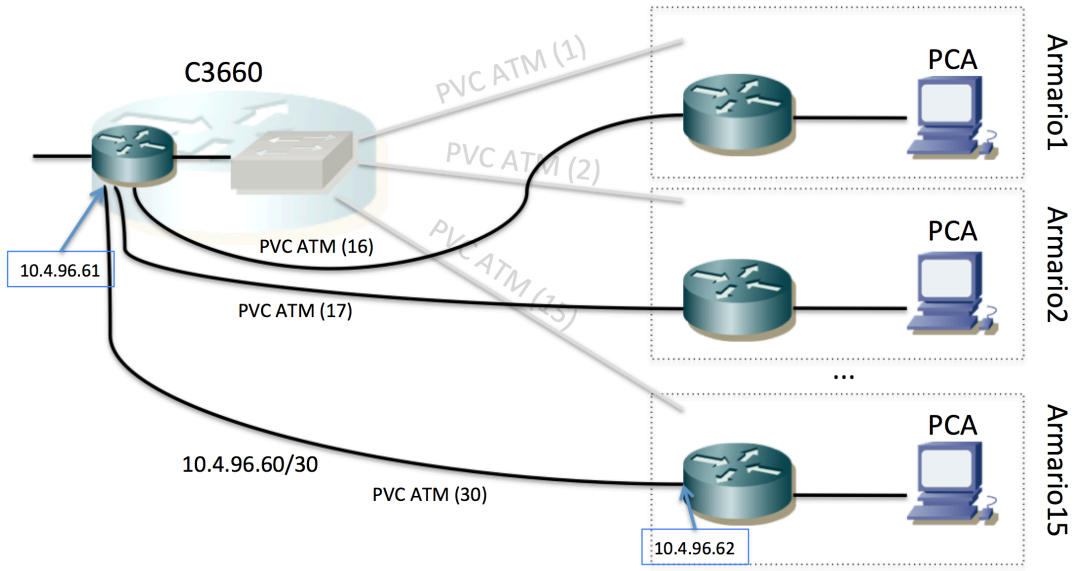


Figura 10 – PVCs del escenario 1483 routed

Este tipo de conexionado implica que habrá una subred IP independiente entre C3660 y cada uno de los routers ADSL. C3660 ya tiene configurados sus interfaces sobre estos PVCs e igualmente tiene introducidas rutas estáticas para poder enviar paquetes a las subredes que se deben configurar en cada uno de los armarios.

La red de uno de estos enlaces punto-a-punto eso:

```
00001010 . 00000100 . 01100000 . 00 ABCD XX / 30
```

donde ABCD es el número de armario. Por ejemplo el rango para el armario 15 sería:

```
00001010 . 00000100 . 01100000 . 00 1111 XX = 10.4.96.60 / 30
```

La primera de las direcciones utilizables en cada una de estas redes la emplea un interfaz del router C3660 y la segunda queda para el router del grupo de prácticas. Es decir, en el caso del armario 15 la dirección IP empleada por el interfaz del C3660 sería `10.4.96.61` y la reservada para el router de prácticas `10.4.96.62`.

Para la red local de cada grupo de prácticas se ha reservado:

```
00001010 . 00000100 . 011000 AB . CD XXXXXX / 26
```

donde ABCD corresponde al número de armario. Por ejemplo, en el caso del armario 15 sería:

```
00001010 . 00000100 . 011000 11 . 11 XXXXXX = 10.4.99.192/26
```

Punto de control: Muestre a su profesor de prácticas el escenario en funcionamiento

7- Múltiples escenarios simultáneos

A continuación vamos a configurar simultáneamente dos de los escenarios anteriores, aprovechando las capacidades de multiplexación de ATM. En concreto vamos a configurar simultáneamente los escenarios de las secciones 5 y 6. Con eso el resultado en capa 3 sería algo similar a lo que se muestra en la figura 11.

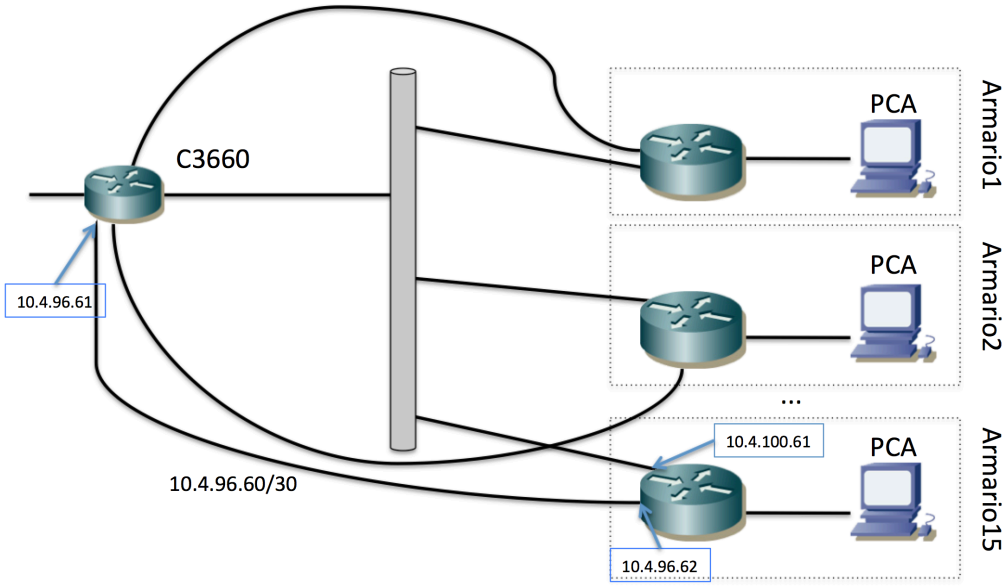


Figura 11 – Topología de capa 3 del escenario con dos PVCs

Como se puede ver, cada router ADSL tiene ahora 3 interfaces enrutados. El interfaz Ethernet se encuentra en la LAN interna del armario. En esa LAN puede haber un solo PC (conectado por ejemplo a un puerto Ethernet del router) o podemos tener más equipos empleando conmutadores Ethernet de los armarios; en cualquier caso se supone que todo ello será una misma subred IP (un mismo dominio capa 2). El router ADSL tiene un interfaz en otra LAN Ethernet, la cual está compartida por todos los routers ADSL y el C3660. Esta LAN está creada mediante los PVCs que se describieron en el apartado 5. El tercer interfaz enrutado de estos equipos corresponde a un enlace punto a punto con C3660 tal y como se describió en la sección 6.

Para el direccionamiento en la LAN interna del armario se puede emplear el direccionamiento mencionado en el apartado 5 o en el 6. Tenga en cuenta las rutas que hay en C3660. Si por ejemplo la subred IP que se configura en la LAN interna es la indicada en el apartado 5 entonces el tráfico que vuelva desde el exterior hacia los PCs lo hará por el PVC 8/36. Si se emplea el direccionamiento indicado en el apartado 6 entonces el tráfico de vuelta empleará el enlace punto-a-punto sobre el PVC 8/35.

Emplee el direccionamiento LAN del escenario 1483 routed (apartado 6).

Para finalizar, nos quedaría configurar la tabla de rutas del router ADSL para poder acceder al laboratorio y/o Internet. La versión simple es añadir una ruta por defecto, sin embargo, eso nos obliga a seleccionar un siguiente salto que emplee uno u otro de los enlaces. Podríamos estudiar la posibilidad de balancear la carga. Podríamos cursar diferente tipo de tráfico por cada uno de los PVCs y éstos podrían tener contratada diferente QoS en la red (por ejemplo uno ser un CBR de 1Mbps y otro un UBR). En esas situaciones podríamos cursar por ejemplo el tráfico de unos usuarios por un interfaz y el de los demás por el otro, según la calidad que necesitaran. O podríamos cursar el tráfico de ciertas aplicaciones por el interfaz de mayor calidad. Por simplicidad, lo que vamos a hacer es que el acceso a ciertos ordenadores se haga por un PVC y a otros por el otro. Esto se puede llevar a cabo introduciendo varias rutas con diferente siguiente salto. Configure una ruta en routerADSL a todas las máquinas del laboratorio (red `10.0.0.0/8`) por el PVC 8/35 y a Internet

Departamento de
Automática y Computación
Automatika eta
Konputazio Saila

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

(una ruta por defecto) por el PVC 8/36.

Ahora estudie el camino (de ida y de vuelta) que sigue el tráfico entre los PCs de la LAN y los del laboratorio o de Internet.

Punto de control: Muestre al profesor de prácticas la configuración en funcionamiento

8- Evaluación

Mediante puntos de control

Departamento de
Automática y Computación
Automatika eta
Konputazio Saila

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

Repaso: Configuración de interfaces IP en equipos con sistema operativo GNU/Linux

1- Objetivos

Para llevar a cabo las configuraciones planteadas en este asignatura necesitaremos PCs que colocaremos en las diferentes LANs. Por ello en esta práctica se repasarán los comandos básicos para configurar un interfaz de red Ethernet con IP en Linux y conectarlo a una LAN con un router de acceso. Igualmente, una técnica básica para el *troubleshooting* en redes es la captura y análisis de tráfico, por ello se verá el procedimiento básico para el mismo empleando sniffers en Linux.

2- Conocimientos previos

Es necesario un conocimiento básico sobre IP: direcciones, redes y subredes, máscaras de red, tablas de rutas, ICMP (ping)...
Esta es una práctica de repaso para todo aquel que haya cursado *Redes de Ordenadores*.

3- Configuración manual de IP sobre el interfaz Ethernet

Los PCs A, B y C disponen cada uno de 4 interfaces Ethernet. Analizaremos previamente dichos interfaces. Para loguearse en estos PCs use el usuario `ftpr` con password `telemat`.
Lea la página del manual del comando `ifconfig` (localizado normalmente en el directorio `/sbin`). Este comando permite configurar los interfaces de red de una máquina. Si ejecuta el comando sin opciones podrá ver los interfaces que se encuentran activos. Si no ha configurado ninguna de las tarjetas Ethernet lo normal es que solo aparezca el interfaz de loopback que suele ser el `lo0`. Este interfaz no corresponde a ninguna tarjeta de red física sino que es parte del software del sistema y puede servir para que programas ejecutándose en la misma máquina se comuniquen empleando protocolos de red.
Ejecute el comando `ifconfig` con la opción `-a`. Esta opción muestra todos los interfaces de red reconocidos por el kernel. Aquí podremos ver los interfaces Ethernet aunque no estén configurados, siempre que hayan sido detectadas por el sistema operativo.
Averigüe la dirección MAC (o dirección hardware) de cada uno de los interfaces Ethernet del PC A.

A continuación procederemos a crear una pequeña red con un par de PCs en la misma que se podrán comunicar empleando la familia de protocolos TCP/IP.

- Conecte mediante un cable recto el puerto del panel de parcheo correspondiente al primer interfaz de red (`eth0`) del PC A con uno de los puertos del concentrador que también están en el panel de parcheo.
- Haga lo mismo con el primer interfaz del PC B.
- Busque en la página del manual del comando `ifconfig` cómo configurar la dirección IP de un interfaz.
- Configure el interfaz `eth0` del PC A para que su dirección IP siga el siguiente esquema:
  `00001010 . 00000011 . 0000 ABCD . 00000001 /24`
  Donde ABCD representa el número de armario en que está realizando prácticas. Es decir `10.3.armario.1`.
- Compruebe que el PC A puede hacer ping a su propia dirección IP.

Departamento de
Automática y Computación
Automatika eta
Konputazio Saila

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

- Configure el interfaz `eth0` del PC B para que su dirección IP sea `10.3.armario.2/24` donde debe substituir "armario" por el número del armario donde realiza las prácticas.
- Compruebe que el PC B puede hacer ping a su propia dirección IP
- Compruebe que el PC A puede hacer ping a la dirección IP del PC B
- Compruebe que el PC B puede hacer ping a la dirección IP del PC A

4- Viendo el tráfico con `tcpdump` *y* `wireshark`

Vamos a ver los paquetes IP que los PCs se envían como resultado de la aplicación `ping`. Para ello en primer lugar emplearemos el programa `tcpdump`.
El programa `tcpdump` nos permite observar los paquetes de red que son recibidos o transmitidos por un interfaz de red. Para ello lee del interfaz de red y muestra de una forma sencilla de entender el contenido principal de las cabeceras del paquete. Además, si el interfaz está en modo promiscuo (vea el manual de `ifconfig`) permite ver también todos aquellos paquetes que circulen por el dominio de colisión al que se esté conectado. Tiene bastantes opciones, entre ellas se pueden especificar filtros para que solo muestre los paquetes que cumplan ciertas condiciones (por ejemplo ser paquetes TCP dirigidos al puerto 80) o indicar el interfaz por el que leer. Opciones útiles son por ejemplo la combinación `-nl`, la opción `l` hace que los paquetes aparezcan por pantalla nada más recibirse y `n` que las direcciones (o los puertos) no se conviertan en nombres DNS (o en nombres del servicio) (salvo que se indique lo contrario emplee siempre ambas opciones).
Manteniendo la configuración anterior de los PCs A y B siga los siguientes pasos:

- Ejecute en PC A el programa `ping` enviando paquetes al interfaz del PC B y déjelo ejecutándose.
- En el PC A (en otro terminal) ejecute el programa `tcpdump` para ver los paquetes que se están enviando y recibiendo. El ping envía paquetes del protocolo ICMP que se transporta dentro de datagramas IP. Para hacer que `tcpdump` nos muestre solo estos paquetes podemos ejecutar:

```
%> tcpdump -nl icmp
```

A continuación emplearemos `wireshark`. Éste es un programa similar a `tcpdump` pero con interfaz gráfico:

- Ejecute en PC A el programa `ping` enviando paquetes al interfaz del PC B y déjelo ejecutándose (o si ya lo tenía corriendo no lo pare).
- Para variar, ejecute en el PC B el programa `wireshark` para ver los paquetes que se están enviando. El ping envía paquetes del protocolo ICMP que se transporta dentro de datagramas IP. Puede indicarle al programa `wireshark` que filtre el tráfico que muestra de forma que solo se vean los paquetes ICMP. Para ello en la casilla de texto junto al botón *Filter* escriba "icmp". En el menún *Capture* escoja la opción *Start...*, asegúrese de que va a leer del interfaz correcto (probablemente `eth0`) y dele al botón de "OK". Debería ver en una ventana cómo `wireshark` está recogiendo paquetes de diferentes tipos, cuando vea que tiene varios de tipo ICMP dele al botón "Stop".
- Analice el contenido de esos paquetes ICMP gracias a la decodificación de sus campos ofrecida por `wireshark`.

Hasta aquí hemos visto los paquetes IP bien en la máquina que envía el ping (y recibe la respuesta) o en la que recibe el ping (y envía la respuesta). Sin embargo, dado que ambas máquinas se encuentran conectadas al mismo Hub o concentrador Ethernet cualquier otra máquina que conectemos al mismo debería ser capaz de ver esos paquetes siempre que configure su interfaz de

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

red para recibir todo el tráfico. Para ver esto siga los siguientes pasos:

- Conecte mediante un cable recto el puerto del panel de parcheo correspondiente al primer interfaz de red (`eth0`) del PC C con uno de los puertos del mismo concentrador
- Active dicho interfaz de red del PC C. Para ello no necesita darle una dirección IP (aunque podría hacerlo), basta con que ejecute:
  ```
  %> sudo ifconfig eth0 up
  ```
- Ejecute en PC C el programa `tcpdump` y vea los paquetes IP del ping entre PC A y PC B

5- Acceso al laboratorio

A continuación vamos a configurar uno de los PCs para que pueda acceder a la red del Laboratorio de Telemática (Fig. 1). Para ello se ha dispuesto un router que interconecta una LAN dedicada para las prácticas de esta asignatura con la LAN del laboratorio. Cada puesto de prácticas tiene un punto de red colocado en la LAN de la asignatura, que es el punto C. Todos estos puntos C van a un conmutador Ethernet al cual también está conectado un router. Con otro de sus interfaces este router se conecta a la red del laboratorio. En el interfaz conectado a la red de esta asignatura tiene la dirección IP `10.3.16.1`.

Procedan de la siguiente forma:

- Escojan uno de los puntos externos del armario y conéctenlo al punto C de su puesto de prácticas. Si por ejemplo han escogido el R-9 eso quiere decir que ahora en la primera fila de su panel de parcheo, en el punto 9, tienen un punto de red del conmutador de la LAN de prácticas
- Conecten ese punto con el punto del panel de parcheo correspondiente al interfaz `eth0` del PC A. ¿Qué necesitarán, un cable recto o uno cruzado? ¿Por qué?
- Configure en PC A la IP `10.3.17.armario/20`
- Denle un tiempo (aproximadamente 1min) al conmutador para que descubra que tienen un nuevo ordenador conectado (más adelante veremos que este tiempo es debido a la configuración del Spanning Tree Protocol)
- Prueben a hacerle ping a la IP del router (`10.3.16.1`)

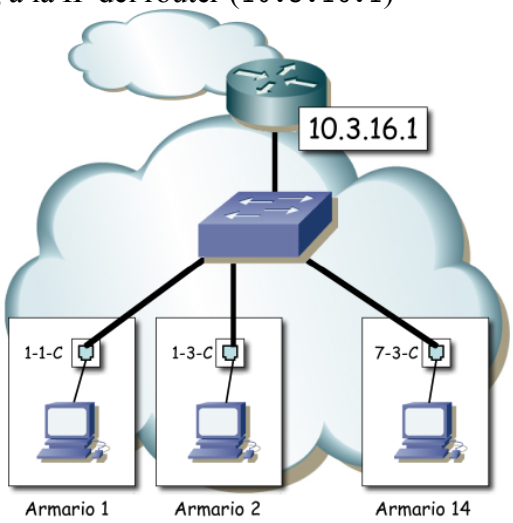


Figura 1: LAN de prácticas

Ahora ya podemos acceder al router y de hecho debería poder acceder al PC A de cualquiera de sus compañeros de prácticas que hayan alcanzado este punto. Sin embargo, para poder comunicarse con

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

otras LANs, como por ejemplo la del laboratorio, hemos de indicarle al PC cuál es el router que debe emplear como intermediario. Para ello vamos a introducir lo que se llama una ruta por defecto, es decir, una ruta o regla que indica a dónde enviar todo el tráfico IP que no se sabe hacer llegar a su destino de otra forma. En nuestro caso el único tráfico que ahora mismo el PC sabe hacer llegar a su destino es el dirigido a máquinas de su misma red.

- Compruebe que desde PC A no puede hacer ping a la máquina `10.1.1.230` que se encuentra en la red del laboratorio.
- Consulte el manual del comando `route`. Averigüe cómo añadir una ruta por defecto (`default gateway`). La página del manual trae ejemplos.
- Introduzca la ruta por defecto empleando el comando `route`. Dicha ruta debe tener como gateway a la dirección `10.3.16.1`.
- Compruebe que puede hacer ahora ping a la máquina `10.1.1.230` que se encuentra en la red del laboratorio.

Para poder acceder a recursos mediante nombres de dominios necesita configurar el servidor DNS del PC. Prueba a hacer ping o acceder mediante el navegador a un nombre de dominio. ¿Puede?

Mire si el fichero `/etc/resolv.conf` tiene una línea especificando el servidor DNS, sino la tiene añada una con `nameserver 10.1.1.193`. Prueba ahora. A continuación borre esa línea para dejar el fichero tal cual estaba.

6- PC como router IP

Vamos a emplear el PC C como router IP. Nuestro primer objetivo es crear una topología como la de la figura 2.

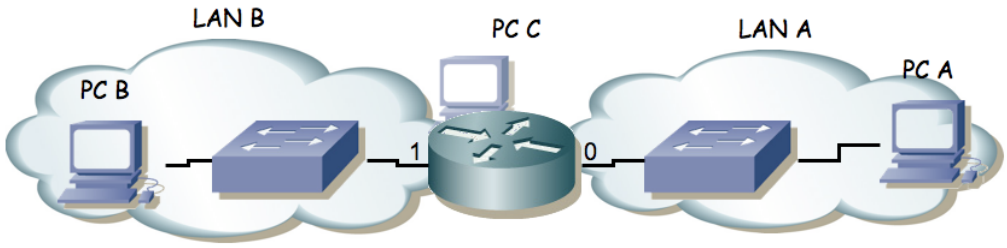


Figura 2.- Router conectado a dos redes

Para ello:

- Dividan su espacio de direcciones (`10.3.armario.0/24`) en al menos dos bloques que no se solapen.
- Configuren las IPs de los dos primeros interfaces ethernet del PC C para que cada uno esté en una de esas redes.
- Configuren un interfaz de PC A para que tenga dirección IP de la Red A y un interfaz del PC B para que la tenga de la Red B.
- Conecten el interfaz del PC C con IP en la Red A en un conmutador (switch0 funciona como 3 conmutadores independientes) y ahí también el PC A.
- Conecten el otro interfaz del PC C en otro conmutador.
- Conecten ahí el PC B.
- Configuren la ruta por defecto de cada PC para que cada uno la tenga haciendo referencia al interfaz del PC C conectado en su misma red.

Departamento de
Automática y Computación
Automatika eta
Konputazio Saila

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

- Prueben a hacer ping desde el PC C a PC A y PC B.
- Prueben a hacer ping desde PC A a PC C y desde PC B a PC C.
- Prueben a hacer ping desde PC A a PC B. ¿Qué sucede?
- Empleen `wireshark` para averiguar qué es lo que está fallando

El PC C tiene ahora dos interfaces IP en funcionamiento. Tal y como está, se dice que este PC está *multihomed* porque tiene interfaces en redes diferentes. Ahora mismo, si recibe por uno de sus interfaces un paquete que se dirige a una IP destino que no es ninguna de las suyas lo descarta. Para que funcione como un router tenemos que convencerle de que cuando reciba un paquete con esas características no lo tire sino que lo reenvíe aplicando las reglas que tiene en su tabla de rutas. Esta funcionalidad es lo que se conoce como IP *forwarding* o reenvío de paquetes IP. Si el kernel tiene compilada esta funcionalidad (y en nuestro caso la tiene) podemos activarla sin más que escribir un 1 en el fichero `/proc/sys/net/ipv4/ip_forward` (recuerde que en Linux los ficheros en `/proc` en realidad hacen referencias a variables dentro del kernel), o equivalentemente empleando el comando `sysctl` para modificar esa variable del kernel.
Ambas acciones requieren privilegios de superusuario. Para resolver el problemas se les ha dejado un programa muy simple que tan solo ejecuta un comando `sysctl` para activar o desactivar el forwarding según se le indique.
Para activarlo:

```
%> sudo /usr/local/sbin/forwarding si
```

Para desactivarlo:

```
%> sudo /usr/local/sbin/forwarding no
```

Y pueden ver el comando que se está ejecutando porque lo muestra por pantalla.
Con solo activar el forwarding el PC empezará a reenviar paquetes. También se podría activar esta funcionalidad para que reenviara paquetes solo entre ciertos interfaces, lo cual sería útil si tuviéramos más de dos y no quisiéramos que reenviará entre todos ellos (ficheros `/proc/sys/net/ipv4/conf/*/forwarding`).
Y ya está. El PC ya se comporta como un router. Si activáramos más interfaces (Ethernet, PPP, WLAN, etc) podría reenviar tráfico entre todos ellos. De hecho esta es una solución bastante barata para tener un router. Coloque ahora un `wireshark` o `tcpdump` en el servidor y observe que sí reenvía los paquetes ICMP.
Una vez que el PC funciona como un router debemos mirar con más cuidado el contenido de su tabla de rutas dado que ahora no solo la empleará para todos los paquetes que él quiera enviar sino también para todos los que decida reenviar.

Departamento de
Automática y Computación
Automatika eta
Konputazio Saila

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

Repaso: Configuración básica de routers Cisco

1- Objetivos

En esta práctica veremos los métodos básicos de acceso a un equipo con Cisco IOS, cómo configurar las direcciones IP de interfaces Ethernet y Serie de routers Cisco, su tabla de rutas y el acceso por telnet al mismo.

2- Conocimientos previos

Es necesario un conocimiento básico sobre IP: direcciones, redes y subredes, máscaras de red, tablas de rutas, ICMP (ping)...
Esta es una práctica de repaso para todo aquel que haya cursado *Redes de Ordenadores*.

3- Acceso al router a través del puerto de consola

Cada grupo de prácticas dispone de tres routers Cisco. Consulten la documentación de los armarios. Verán que el servidor de consola tiene un cable desde el puerto serie al puerto de consola de cada uno de ellos (y tiene varios puertos serie). Estos cables tienen por un extremo un conector DB9 y es el conectado al PC. El otro extremo, que pueden ver en los routers, es un conector RJ45 (sigue siendo una conexión serie, NO es Ethernet) (Fig. 1).

- Apaguen el router2 (con el interruptor de alimentación)
- Ejecuten la aplicación `minicom` en el PC-SC para que abra el puerto serie que le comunica con el router2. La comunicación debe ser a 9600 bps, 8 bits de datos, 1 de parada, sin paridad, comprueben que el puerto está bien configurado.
- Ahora enciendan el router. Deberían poder ver el proceso de arranque del mismo.

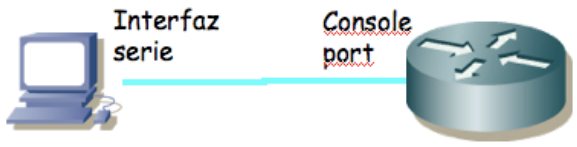


Figura 1.- Conexión al puerto de consola

La primera configuración del router es necesario hacerla a través de este puerto de consola dado que al no tener el router aún una configuración de red no podemos acceder a él por ninguno de sus interfaces de red.
El Cisco IOS CLI ofrece diferentes modos de comandos. Cada modo de comandos ofrece un conjunto de comandos diferentes y con diferente objetivo (configuración, mantenimiento, monitorización...). Los comandos disponibles en cada momento dependen del modo en el cual se encuentre el usuario. En cualquiera de estos modos se puede emplear el interrogante (?) para obtener una lista de los comandos disponibles en ese modo.
Lo mejor es que se acostumbre a la documentación oficial de Cisco. En el siguiente URL tiene una introducción a los diferentes modos existentes:
`http://www.cisco.com/en/US/docs/ios/11_0/router/configuration/guide/cui.html`
Lea de la sección *Understanding the User Interface* de dicho documento las subsecciones: *Understanding the User Interface, User EXEC Mode, Priviledged EXEC Mode, Global Configuration Mode* e *Interface Configuration Mode* (en total unas 5 páginas). Explica las diferencias entre los modos, cómo cambiar de uno a otro y cómo ver la ayuda en línea disponible.

upna Universidad Pública de Navarra Nafarroako Unibertsitate Publikoa

Departamento de
Automática y Computación

Automatika eta
Konputazio Saila

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

Al finalizar el arranque del router seguramente se encontrarán (a través de `minicom`) con algo como:

```
Router>
```

Este es el prompt de CLI (en este caso con el nombre del router). En este punto estamos en modo de comandos de usuario (User EXEC Mode) que es el de menos privilegios y con el que no vamos a poder cambiar la configuración del router.

Puede ver los comandos disponibles desde este modo con el interrogante:

```
Router> ?
Exec commands:
  <1-99>           Session number to resume
  access-enable    Create a temporary Access-List entry
  access-profile   Apply user-profile to interface
  clear            Reset functions
  connect          Open a terminal connection
  disable          Turn off privileged commands
  disconnect       Disconnect an existing network connection
  enable           Turn on privileged commands
...
```

Podemos obtener ayuda de cada comando e incluso de las opciones del comando terminándolo con un interrogante. Por ejemplo:

```
Router> show ?
  backup          Backup status
  clock           Display the system clock
  compress        Show compression statistics
  dialer          Dialer parameters and statistics
  flash:          display information about flash: file system
  history         Display the session command history
  hosts           IP domain-name, lookup style, nameservers, and host table
  location        Display the system location
  modemcap        Show Modem Capabilities database
  ppp             PPP parameters and statistics
  rmon            rmon statistics
  rtr             Response Time Reporter (RTR)
  sessions        Information about Telnet connections
  snmp            snmp statistics
  tacacs          Shows tacacs+ server statistics
  terminal        Display terminal configuration parameters
  traffic-shape   traffic rate shaping configuration
  users           Display information about terminal lines
  version         System hardware and software status
```

Podemos ver la versión del sistema operativo y el hardware disponible (RAM, interfaces...) mediante el comando `show version`.

- ¿Qué versión del sistema operativo tiene su router?
- ¿Cuánta RAM tiene instalada?
- ¿De cuántos interfaces dispone su router?
- ¿De qué tipo son? Identifíquelos físicamente en el router.

Con el comando `show interfaces` pueden ver los interfaces de red de los que dispone el router y muchas características de estos. Averigüe la dirección MAC de cada uno de sus interfaces Ethernet.

Averigüe cómo ver los ficheros que existen en la flash con el comando `show`.

Podemos acceder a información referente a IP con las opciones de `show ip` (vea un poco las opciones existentes). Por ejemplo podemos ver información referente a IP de cada interfaz con `show ip interface`, especificar un solo interfaz u obtener información muy resumida de la configuración ip de los interfaces (pruebe `show ip interface brief`). También podemos ver la

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

tabla de rutas con `show ip route`. Lo más probable es que ahora vea que ningún interfaz tiene asignada dirección IP y que no hay ninguna entrada en la tabla de rutas. Podremos remedio a todo esto en breve.

4- Configuración IP básica de un interfaz Ethernet del router

Para hacer cualquier cambio en la configuración del router lo primero que debemos hacer es pasar al modo de comandos privilegiado (*priviledged EXEC mode*). Para ello ejecute:

```
Router> enable
```

En este punto el router podría (y debería) solicitar una password. De momento esa password está quitada. Si el comando se ejecuta con éxito el prompt debería cambiar a algo como:

```
Router#
```

para indicarnos que estamos en modo privilegiado.

Si ahora pide de nuevo ayuda (?) podrá ver que hay un nuevo conjunto de comandos disponible. Por ejemplo, pruebe el comando `reload` que sirve para reiniciar el router y aprenda a programar que el router se reinicie dentro de 1 minuto. Aproveche para ver de nuevo los mensajes del arranque del router.

Tras terminar el reinicio vuelva a entrar en modo privilegiado. De ahí pasamos al modo de configuración con el comando:

```
Router# configure terminal
```

Si pide ayuda de nuevo verá otro conjunto de comandos. Lo primero que vamos a hacer es activar que el equipo actúe como un router. Para ello emplearemos el comando `ip`. Vea las opciones de este comando con:

```
Router(config)# ip ?
```

Lo activamos escribiendo:

```
Router(config)# ip routing
```

Nota: Muchos alumnos se acostumbran a escribir este comando (y otros) cada vez que entran en modo configuración. Esto no es en absoluto necesario. Una vez que activemos el reenvío de paquetes se queda activado (salvo que lo desactivemos expresamente o rebotemos y no hayamos guardado la configuración), al igual que con los demás comandos (como por ejemplo activar un interfaz).

A continuación vamos configurar la dirección IP de uno de los interfaces Ethernet. Para ello hemos de pasar al modo de configuración de ese interfaz. Esto se hace con el comando interface especificando a continuación el nombre del interfaz (recuerde que siempre puede usar ? para pedir ayuda). Entre en modo configuración del interfaz FastEthernet de su router. El prompt debería ser ahora:

```
Router(config-if)#
```

Una vez en este modo primero le indicamos al IOS que active el interfaz con:

```
Router(config-if)# no shutdown
```

A continuación especificamos la dirección IP del interfaz empleando el comando `ip`. Investigue las opciones del comando lo suficiente para darle a ese interfaz la direcció IP `10.3.armario.1` con máscara `255.255.255.0`.

Conecte ese interfaz del router al hub (si el interfaz no está conectado a ningún dispositvo entonces el Cisco IOS lo desactiva) (Fig. 2). Vuelva al modo usuario y revise la configuración IP de los interfaces. Debe aparecer *up* tanto en la columna *Status* como en la columna *Protocol* de un interfaz para que este reenvíe paquetes. Revise también la tabla de rutas. Ahora debería ver una ruta a la red a la que está conectado ese interfaz.

Conecte uno de los interfaces Ethernet del PC A al mismo hub y configúrele la dirección

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

`10.3.armario.2` con máscara `255.255.255.0`. Ahora debería poder hacer ping a ese interfaz del router desde el PC.

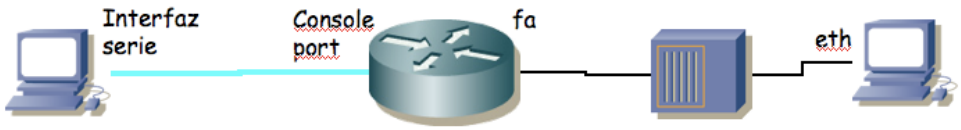


Figura 2.- Conexión a hub

5- Interfaces serie

Los routers se pueden emplear para conectar tanto LANs como WANs, así que suelen tener disponibles interfaces de ambos tipos. A los efectos de nuestros interfaces de red una WAN opera a nivel físico y de enlace y nos permite interconectar LANs.
Generalmente los enlaces WAN utilizan servicios de operadoras (carriers) de comunicaciones, ofreciendo conectividad a nivel de enlace entre los dos extremos. El router (DTE, Data Terminal Equipment) se conecta a la WAN a través de un DCE (Data Communication Equipment) (Fig. 3).

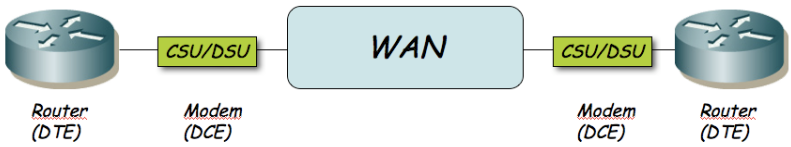


Figura 3.- Routers conectados por un enlace WAN

El DTE se conecta al DCE con un Cable DTE. El conector libre de un cable DTE (en nuestro caso un V.35) normalmente es macho. El DCE ofrece un conector hembra. El router Cisco puede actuar tanto como DTE o como DCE. En las prácticas no vamos a emplear unidades CSU/DSU para conectar los routers entre sí a través de los interfaces WAN serie. Lo que vamos a hacer es conectarlos con un cable tipo *NULL modem*. Para ello juntaremos dos cables, uno un cable DTE y el otro un cable DCE (Fig. 4). El cable DCE tienen un extremo V.35 hembra. Posteriormente, en la configuración de los dos routers, deberemos configurar que uno de ellos actúe como DCE.

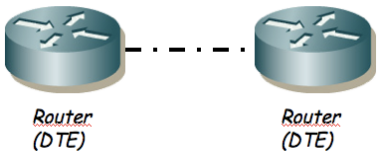


Figura 4.- Routers conectados por cable NULL modem

Las tarjetas WAN de los routers de los que disponen tienen dos puertos serie cada una. Tienen ya conectados cables DTE y DCE.

- Conecten uno de los puertos serie de router2 con uno de router3

Uno de los dos extremos actuará como el DTE y el otro como el DCE, según el cable que le hayamos conectado. La diferencia principal es que normalmente el DCE genera la señal de sincronismo necesaria en el cable.

- Entren en modo de configuración de cada interfaz serie que hayan conectado y asignen una dirección IP y una máscara de red a ese interfaz (empleen a su gusto la red asignada a su armario: `10.3.armario.0/24`)
- En el router que vaya a ser el DCE (el del cable de conector V.35 hembra) deben especificar la velocidad a la que se empleará la línea serie (comando `clock rate`). Los interfaces serie de estos routers son de baja velocidad y normalmente estarán limitados en torno a unos 100-120Kbps.

Departamento de
Automática y Computación
Automatika eta
Konputazio Saila

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

- Y por supuesto activen los interfaces

Con esto deberían poder hacer ping desde un router al otro a través de la línea serie. La línea serie estará empleando como nivel de enlace el encapsulado HDLC. Se puede configurar para que se emplee otro encapsulado como por ejemplo PPP.

- A continuación conecten uno de los interfaces Ethernet de cada router a un conmutador diferente del switch0 (Fig. 5)
- Conecten un PC a cada una de esas LANs
- Configuren 3 redes: una para cada LAN y una tercera para el enlace serie, empleando el espacio de direcciones que tienen asignado
- Configuren en cada PC la dirección IP y el router por defecto. El comando para añadir rutas en el Cisco IOS es (en modo configuración) `ip route`
- Configuren en cada router una ruta por defecto al otro router por el interfaz serie
- Prueben a hacer ping entre los PCs
- Prueben a cambiar la velocidad del enlace serie y vean cómo cambia el retardo indicado por el ping

Figura 5.- Topología en serie

6- Topología con 2 routers

A continuación vamos a crear la topología que se ve en la figura 6.

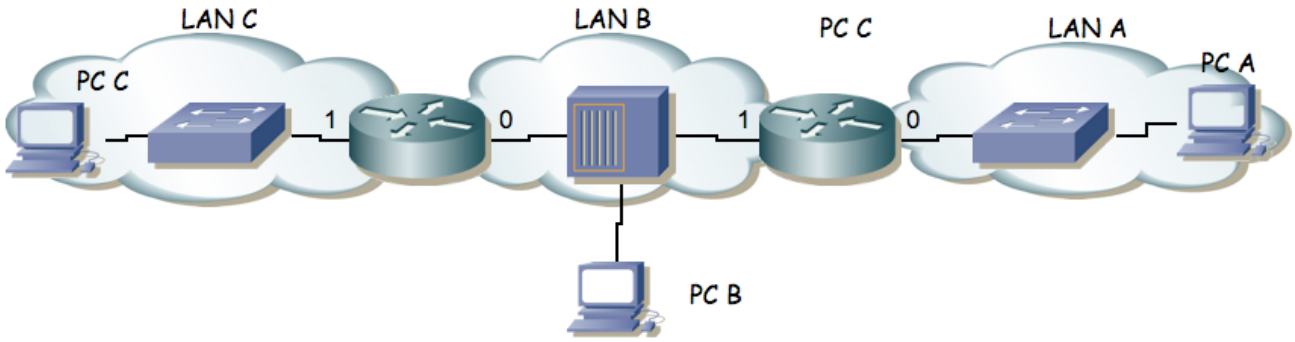


Figura 6.- 2 routers conectando 3 redes

Para ello emplearemos los routers router2 y router3.

- La red que tiene asignada el grupo de prácticas (`10.3.armario.0/24`) divídanla en al menos 3 redes que no se solapen.
- Configuren los interfaces de los routers para que tengan la dirección IP en la red que les corresponde.
- Configuren PC A, B y C para que cada uno esté conectado a una de las redes.
- Configuren la ruta por defecto de cada PC. Recuerde que debe apuntar a un router que esté en su misma red. Con el PC B tiene dos para elegir!
- Compruebe que cada PC puede comunicarse con otro que esté a un router de distancia pero los dos de los extremos (PC A y PC C) no pueden comunicarse entre si.
- Para resolver esto introduzcan una ruta por defecto en cada uno de los routers que tenga al

otro router como siguiente salto. El comando para añadir rutas en el Cisco IOS es (en modo configuración) `ip route`

- ¿Ahora qué camino siguen los paquetes que van de la Red A a la Red C?
- Coloque un `tcpdump` o `wireshark` en PC B.
- ¿Puede ver los paquetes que van de PC A a PC C? ¿Y los que van de PC C a PC A?
- Si pone un ping entre PC A y PC C y ve los paquetes con wireshark en PC B ¿Qué direcciones IP origen y destino tienen? ¿Qué direcciones MAC tienen? ¿De qué interfaces son?
- ¿Qué camino siguen los paquetes que van de PC B a PC A? ¿Y los que van de PC B a PC C?

Uno de los campos de la cabecera de todos los paquetes IP es el TTL o *Time To Live*. El origen del paquete le da un valor y cada router que reenvía el paquete lo decrementa al menos en una unidad. Si un router va a reenviar un paquete y después de decrementar este campo de la cabecera el resultado es 0 o menos que 0 descarta el paquete sin reenviarlo. Podemos ver el valor de este campo de los paquetes IP con el programa `tcpdump` si le pedimos que saque más información de cada paquete. Pueden emplear para ello la opción `-v`.

- ¿Con qué valor de TTL generan estos PCs los paquetes IP normalmente?
- Vean cómo el TTL se decrementa al ser reenviado por cada uno de los routers
- En esta topología, ¿Qué valor mínimo de TTL se debe emplear para que todos los paquetes puedan llegar a su destino?

Ahora vamos a añadir unas rutas a las tablas de los Cisco. Para ello

- Consulten la ayuda del comando `ip route` en modo configuración con el que pueden añadir rutas estáticas a un router Cisco
- Añadan al router de la izquierda una ruta hacia la red A apuntando al otro router
- Añadan al router de la derecha una ruta hacia la red C apuntando al otro router
- Prueben a hacer ping entre todos los PCs

7- Gestión de configuración

Los cambios que hemos hecho hasta el momento en la configuración del router se perderán en el momento que lo reiniciemos. Para que los cambios sean permanentes lo que se hace es guardar la configuración actual con el nombre del fichero de configuración que lee en el arranque el router y que se encuentra en la NVRAM. En general en estas prácticas NO utilizaremos este commando, para evitar modificar la configuración en el arranque del router, dado que daría problemas al siguiente grupo de prácticas, que esperará una configuración "limpia". Puede buscar en la documentación de Cisco cómo se haría este paso, si tiene interés. El nombre del fichero que carga en el arranque es "startup.config".

Para ver la configuración que tiene en el momento actual el router puede ejecutar desde modo privilegiado:

```
Router# show running-config
```

Ahí están todos los comandos que se han ejecutado y están en efecto en este momento. Como se ha comentado, si en algún momento deseamos deshacer un comando lo único que hace falta es ejecutarlo de nuevo poniendo delante `no`. Por ejemplo, para desactivar el routing podríamos desde modo configuración:

```
Router(config)# no ip routing
```

En un escenario real es frecuente que la configuración total sea un fichero bastante grande, por lo que hay formas de visualizar solo partes del mismo. Para el tipo de escenarios que se configuran en

Departamento de
Automática y Computación
Automatika eta
Konputazio Saila

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

estas prácticas es un ejercicio interesante y recomendado acostumbrarse a ver la configuración completa del router (o conmutador), la cual nunca es muy grande.