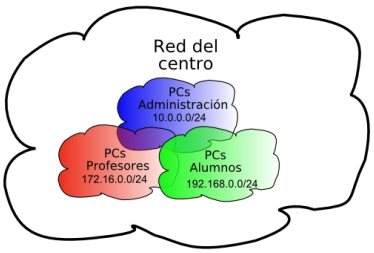


Aprende a diseñar una red local para ofrecer el mejor servicio en optimas condiciones de seguridad.

Diseño de la red del centro

Introducción

En la actualidad, los Centros Educativos disponen de red de ordenadores, pero no todos disponen de una red diseñada para ofrecer el mejor servicio en optimas condiciones de seguridad. A lo largo de este monográfico estableceremos una serie de directrices que ayuden al personal de mantenimiento de la red del centro a acometer los cambios necesarios para su aprovechamiento bajo condiciones de seguridad adecuadas.

¿Cuántas redes necesita mi centro educativo?

Dentro de un centro educativo tenemos distintos tipos de usuarios que podemos clasificar en tres grupos:

- Administración
- Profesores
- Alumnos

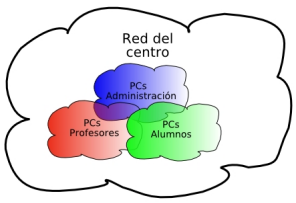
Cada usuario utiliza la red para diferentes cometidos.

La **red administrativa** contiene información de datos personales, matriculación y calificaciones de los alumnos. Debe ser la red más protegida y es evidente que sólo se debe tener acceso a la misma desde la oficina de administración y desde los PCs del equipo directivo del centro.

La **red de profesores** será utilizada por el profesorado para realizar sus tareas habituales de preparación trabajos y exámenes, anotaciones sobre los alumnos, etc... Es conveniente que esté separada de la red de alumnos para evitar que éstos puedan acceder a información confidencial del profesorado.

La **red de alumnos** será la formada por los PCs que utilizan los alumnos durante las horas diarias de clase.

En muchos centros **solo existe una única red** en la que están juntos los PCs de administración, los PCs de profesores y los PCs de alumnos. Esta situación no es recomendable desde el punto de vista de la seguridad.



Por seguridad, es conveniente que exista una separación entre distintos tipos de usuarios. Lo ideal es disponer de tres redes independientes:

- **Red administrativa**: compuesta por los PCs de la oficina y equipo directivo
- **Red de profesores**: compuesta por los PCs de los departamentos y sala de profesores. Los alumnos deberán tener prohibido utilizar estos PCs.
- **Red de alumnos**: compuesta por los PCs de las aulas y la biblioteca. Todos los PCs que se permite utilizar a los alumnos, estarán en esta red.

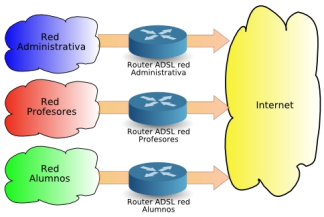
Al crear tres redes totalmente independientes, desde una determinada red no habrá acceso a ninguna de las demás redes. Esto tiene la ventaja de la seguridad que ofrece la separación física de las redes pero tiene la desventaja que para intercambiar datos de una red a otra no podemos hacerlo por la red local, sino que debemos hacerlo a través de Internet o manualmente mediante una memoria USB. Más adelante veremos como resolver esta necesidad.

Conexión a Internet de las redes

Conexión con tres ADSLs

En los tiempos que corren, es imprescindible disponer de conexión a Internet en todos los PCs del centro. Si el centro dispone de redes independientes, una buena decisión es contratar tres conexiones de banda ancha, una para cada red. Ejemplo, contratar tres líneas ADSL:

- ADSL administrativa
- ADSL profesores
- ADSL alumnos



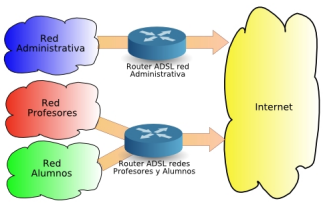
Esto puede suponer al centro un coste importante ya que cada conexión ADSL obliga a contratar una línea telefónica y el ADSL con sus cuotas correspondientes, pero es la solución ideal si cada una de las redes del centro tiene al menos 10 PCs, ya que si el número de PCs del centro es muy grande y solo disponemos de una línea ADSL, el ancho de banda se dividirá entre el número de usuarios, lo que puede llegar a ralentizar excesivamente la conexión a Internet. En cambio, si cada red dispone de su propia conexión ADSL, la velocidad será mayor ya que el ancho de banda se divide solo entre los usuarios de dicha red.

Para que esta separación sea **efectiva**, es necesario que exista una separación física de las redes, es decir, es necesario disponer de diferentes switches para cada red, y que **no estén interconectados entre sí**. Si fuera complicada o muy costosa la separación física de las redes, existe la posibilidad de crear redes virtuales (ver artículo 'Separando la red con VLANes' en este mismo monográfico)

Si el número de PCs del centro es pequeño, quizás sea excesivo contratar tres líneas ADSL. En tal caso, buscaremos otras soluciones.

Conexión con dos ADSLs

Si el centro solamente tiene recursos para contratar dos líneas ADSL, lo ideal es realizar una separación de la red administrativa por un lado y las redes de profesores y alumnos por otro lado:

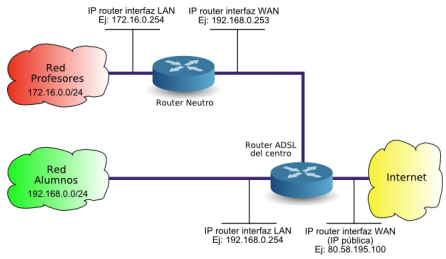


De esta forma tendremos la seguridad de que la red administrativa, que es la que contiene

información más confidencial, esté físicamente separada del resto. Aún así, esta situación no es recomendable ya que desde los PCs de alumnos pueden originarse ataques hacia los PCs de profesores y acceder a información confidencial.

Para separar conveniente la red de profesores de la red de alumnos, se recomienda utilizar **un router neutro**
. Un router neutro es un dispositivo similar a un router ADSL, salvo que la boca que se conecta a la WAN es Ethernet con conector RJ45 en lugar de ser ADSL con conector RJ11, lo que permite conectarle a otra red, interconectando ambas redes. Están diseñados para compartir una conexión monopuesto de banda ancha por NAT. Su precio ronda los 50 euros. Existen modelos que incorporan WIFI e incluso servidor de impresión por USB. La ventaja de este router un tanto especial, es que al igual que los routers ADSL, permite comunicación en la dirección LAN -> WAN pero no al contrario. Veremos cómo sacar provecho de esta cualidad.

El esquema de la conexión sería el siguiente:



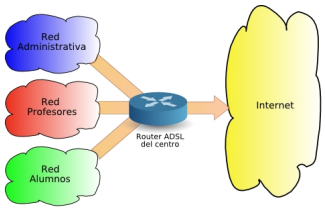
Hay que tener en cuenta que la Interfaz WAN del router neutro deberá ser configurada con IP estática del rango de alumnos y que la puerta de enlace de dicha interfaz WAN, deberá ser la IP LAN del router ADSL.

Para que esta separación con un router neutro sea **efectiva**, es necesario que exista una separación física de los PCs de la red de alumnos y los de la red de profesores en diferentes switches. Si fuera complicada o muy costosa la separación física de las redes, existe la posibilidad de crear redes virtuales (ver artículo 'Separando la red con VLANes' en este mismo monográfico)

Con este conexionado, tenemos la ventaja que desde la red de profesores se puede acceder a la red de alumnos, pero no al contrario.

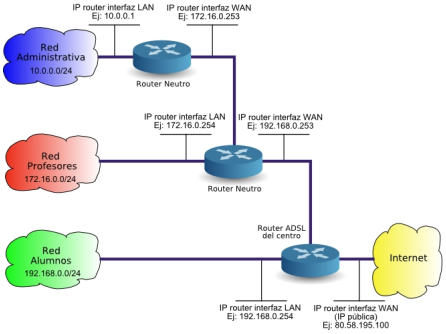
Conexión con una ADSL

Si los recursos del centro solo dan para contratar una única línea ADSL, no tendremos más remedio que tener las tres redes unidas para darlas servicio de Internet:



Esta es la situación más **peligrosa** ya que al estar todos los PCs del centro en la misma red, desde los PCs de alumnos pueden originarse ataques hacia los PCs de profesores o de la red administrativa y acceder a información confidencial.

Para separar conveniente las tres redes, se recomienda utilizar **dos routers neutros**. El esquema de la conexión sería el siguiente:



Para que esta separación con un router neutro sea **efectiva**, es necesario que exista una separación física de los PCs de las distintas redes en diferentes switches. Si fuera complicada o muy costosa la separación física de las redes debido a que implicaría realizar varios tendidos de cableado de red, existe la posibilidad de crear redes virtuales (ver artículo 'Separando la red con VLANes' en este mismo monográfico)

Servidor de Intranet

Este tipo de conexionado mediante dos routers neutros tiene algunas ventajas ya que desde la red administrativa se puede acceder a la red de profesores y a la red de alumnos, pero no al contrario. Así mismo, desde la red de profesores se podrá acceder a la red de alumnos, pero no al revés.

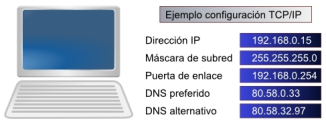
Si necesitamos un servidor de Intranet para dar servicio a todo el centro, se deberá colocar en la red de alumnos. De esa forma, tendrán acceso a él, todos los PCs del centro, incluidos los PCs de la red administrativa y los de la red de profesores.

Si tuviéramos que dar algún acceso desde la red de profesores a la red administrativa, por ejemplo, para que los profesores puedan utilizar alguna aplicación para introducción de calificaciones o faltas de asistencia de los alumnos, existe la posibilidad de abrir algún puerto del interfaz WAN del router neutro de la red administrativa y redirigirlo hacia la IP del PC que preste el servicio en la red administrativa, de igual forma que hacemos cuando abrimos los puertos de un router ADSL.

Direcciones IP

Configuración TCP/IP

La mayoría de personas ya saben que para que los PCs de una red puedan intercomunicarse entre sí, deben disponer de una **dirección IP** y de una máscara de subred. Además, si queremos que disponga de conexión a Internet, es necesario configurar la dirección IP de la puerta de enlace y la dirección IP de dos servidores DNS.



Dentro de una misma red, los PCs deben tener una dirección IP perteneciente al rango de dicha red. Si el rango es desde 192.168.0.0 hasta 192.168.0.255, las IPs de los PCs deberán tener los tres primeros números iguales (192.168.0.X) y el último número podrá cambiar desde 1 hasta 254, porque no se permite la utilización de la primera ni de la última dirección IP del rango ya que quedan reservadas.

Cada PC deberá tener una dirección IP diferente. Si dos PCs tienen la misma IP, habrá un

conflicto de IP y ninguno de ellos podrá comunicarse hasta que no se resuelva el conflicto cambiando la IP a uno de ellos. Si no sabemos qué IP poner, podemos ver la IP de otro PC de nuestra red en el que funcione correctamente la conexión de Internet y por regla general, cambiar el último valor por otro diferente que no tenga ningún otro PC.

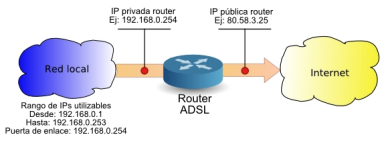
La **Máscara de subred** determina el número de PCs del rango. Casi siempre se suele utilizar la máscara 255.255.255.0 que corresponde a un rango de 256 direcciones IP (suficientes para casi todos los centros educativos) en los que todos los PCs tienen los tres primeros números de la IP iguales y solo cambia el último. Lo normal es que todos los PCs de nuestra red tengan configurada la misma máscara de subred. Si no sabemos cual es la máscara de subred, podemos verla en otro PC que funcione correctamente la conexión de Internet.

La **Puerta de enlace** deberá ser una IP del rango ya que de lo contrario, nuestro PC no será capaz de comunicarse con ella y no tendrá acceso a Internet. Lo normal es que todos los PCs de nuestra red tengan configurada la misma puerta de enlace. Si no sabemos la IP de nuestra puerta de enlace, podemos verla en otro PC que funcione correctamente la conexión de Internet.

Los **DNS preferido y alternativo** nos los debe proporcionar la compañía que presta el servicio. Telefónica usa el 80.58.0.33 y el 80.58.32.97. Lo normal es que todos los PCs de nuestra red tengan configurados los mismos DNSs. Si no sabemos la IP de los DNS preferido y alternativo, podemos verlos en otro PC que funcione correctamente la conexión de Internet.

Direcciones IP públicas y privadas

Las direcciones IP de los PCs de una red local son direcciones privadas ya que los PCs no están directamente conectados a Internet. Solamente el router dispone de conexión directa a Internet y por eso es el único que dispone de una dirección IP pública.



Cuando los PCs de una misma red se quieren comunicar unos con otros, lo hacen directamente, pero si quieren comunicarse con Internet, deben hacerlo a través del router. Es equivalente a una centralitatelefónica. Los teléfonos internos de una empresa utilizan números privados (extensiones) y las llamadas al exterior es necesario hacerlas a través de la centralita,

que es la única que tiene números de teléfono públicos.

Los únicos rangos de direcciones que se pueden utilizar en redes locales son:

Rangos Redes Locales	
Desde	Hasta
10.0.0.0	10.255.255.255
172.16.0.0	172.31.255.255
192.168.0.0	192.168.255.255

Estos rangos de direcciones no están asignados a direcciones públicas de Internet, sino que se han reservado para ser utilizados en las redes locales. Si en lugar de configurar nuestra red con estas direcciones utilizamos otro rango, como seguramente sea un rango utilizado por servidores de Internet, no tendremos acceso a dichos servidores.

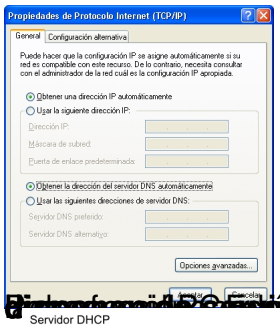
Direccionamiento IP de las diferentes redes

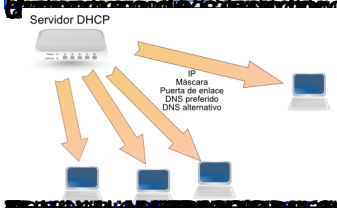
Como ya hemos comentado anteriormente, lo ideal es disponer de tres redes independientes. Al ser diferentes redes, podríamos utilizar los mismos rangos de direcciones en las tres, pero para evitar confusiones, lo mejor es utilizar rangos diferentes, por ejemplo, podríamos utilizar un rango que empiece por 10.0.0.X para la red administrativa, un rango que empiece por 172.16.0.X para la red de profesores y un rango que empiece por 192.168.0.X para la red de alumnos:

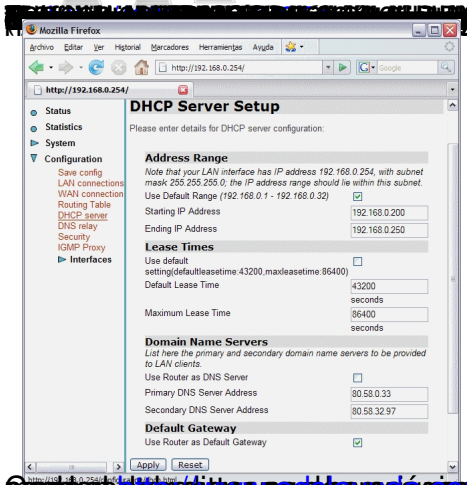
Red	Desde	Hasta	Máscara de subred
Administrativa	10.0.0.0	10.0.0.255	255.255.255.0
Profesores	172.16.0.0	172.16.0.255	255.255.255.0
Alumnos	192.168.0.0	192.168.0.255	255.255.255.0

Asignación automática de direcciones IP

Para que los PCs de la red puedan comunicarse, es necesario configurar uno por uno, la dirección IP, la máscara de subred, la puerta de enlace, el DNS preferido y el DNS alternativo. Si el número de PCs de nuestra red es elevado, existe la posibilidad de configurar las direcciones IP de forma automática:







Máscaras de red

En la configuración TCP/IP, los PCs deben tener una IP y una máscara de red. La máscara de red determina el rango de la red, es decir, el número de direcciones de la red. Dada una IP y una máscara, podemos, mediante unos “sencillos” cálculos, averiguar el rango de la red, la **primera dirección IP** que corresponde con la **dirección de red**, **última dirección IP** que corresponde con la **dirección de difusión** o dirección broadcast y el número de IPs del rango.

La máscara, es un valor que si le pasamos a binario, solamente contiene ‘unos’ y ‘ceros’ consecutivos, es decir, que los ‘unos’ están todos juntos y luego los ‘ceros’ están todos juntos. Los únicos posibles valores de las máscaras son:

Máscara en binario	En decimal	Notación simplif.	IPs totales
11111111.00000000.00000000.00000000	255.0.0.0	/8	16777216
11111111.10000000.00000000.00000000	255.128.0.0	/9	8388608
11111111.11000000.00000000.00000000	255.192.0.0	/10	4194304
11111111.11100000.00000000.00000000	255.224.0.0	/11	2097152
11111111.11110000.00000000.00000000	255.240.0.0	/12	1048576
11111111.11111000.00000000.00000000	255.248.0.0	/13	524288
11111111.11111100.00000000.00000000	255.252.0.0	/14	262144
11111111.11111110.00000000.00000000	255.254.0.0	/15	131072
11111111.11111111.00000000.00000000	255.255.0.0	/16	65536
11111111.11111111.10000000.00000000	255.255.128.0	/17	32768
11111111.11111111.11000000.00000000	255.255.192.0	/18	16384
11111111.11111111.11100000.00000000	255.255.224.0	/19	8192
11111111.11111111.11110000.00000000	255.255.240.0	/20	4096
11111111.11111111.11111000.00000000	255.255.248.0	/21	2048
11111111.11111111.11111100.00000000	255.255.252.0	/22	1024
11111111.11111111.11111110.00000000	255.255.254.0	/23	512
11111111.11111111.11111111.00000000	255.255.255.0	/24	256
11111111.11111111.11111111.10000000	255.255.255.128	/25	128
11111111.11111111.11111111.11000000	255.255.255.192	/26	64
11111111.11111111.11111111.11100000	255.255.255.224	/27	32
11111111.11111111.11111111.11110000	255.255.255.240	/28	16
11111111.11111111.11111111.11111000	255.255.255.248	/29	8

Pasar la máscara de binario a decimal

Hay que convertir byte a byte de binario a decimal, teniendo en cuenta que el bit más significativo está a la izquierda. Ejemplo, supongamos que el último byte de la máscara es 11100000, su valor será 224 porque:

```
Peso del bit: 128 64 32 16  8  4  2  1
Máscara         1  1  1  0  0  0  0  0 => 128 + 64 + 32 = 224.
```

También se puede hacer con Excel, mediante las fórmulas BIN.A.DEC() y DEC.A.BIN()

Averiguar la máscara, dado el número de direcciones IP totales del rango

La máscara de subred es un valor directamente ligado al número de direcciones totales de la red, es decir, dado un número de direcciones, obtenemos la máscara y dada una máscara, obtenemos el número total de direcciones. Si nos dicen que el rango es de X direcciones, podemos consultar la tabla de máscaras y averiguar directamente la máscara de red.

- Ejemplo: si el rango son 64 direcciones, la máscara ha de ser: 255.255.255.192
- Ejemplo: si el rango son 512 direcciones, la máscara ha de ser: 255.255.254.0

Recordar que si el rango son 64 direcciones, solamente se pueden usar 62 para asignar a los PCs y si el rango son 512 direcciones, solamente se pueden utilizar 510 para asignar a PCs. Hay que restar 2 ya que ni la primera ni la última dirección son utilizables porque están reservadas.

Hay que tener en cuenta que el número de direcciones de un rango ha de ser una potencia de 2. Si nos preguntan qué máscara utilizar si necesitamos 200 PCs, usaremos la máscara 255.255.255.0 que admite hasta 256 direcciones. Para no complicarse, lo mejor es utilizar siempre la máscara 255.255.255.0 aunque el número de PCs de la red sea muy pequeño, total, lo que nos sobran son direcciones IP, así que no merece la pena andar utilizando máscaras

'raras'. Si nuestra red tiene solo 5 PCs, lo normal es utilizar el rango 192.168.0.X con máscara 255.255.255.0.

Averiguar direcciones de red y de broadcast dada una IP y una máscara

Si nos dan una IP y una máscara, podemos, mediante unos sencillos cálculos, averiguar el rango de la red, la primera dirección IP (que corresponde con la dirección de red), la última dirección de red (que corresponde con la dirección de broadcast) y el número de IPs del rango.

Si nos dan una IP y nos dan la máscara, es fácil averiguar la dirección de red y la dirección de broadcast si conocemos el **sistema binario** y sabemos realizar **operaciones lógicas**. Debemos pasar la IP y la máscara a binario y hacer dos operaciones lógicas.

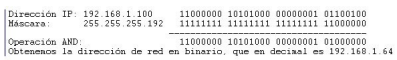
Para calcular la **dirección de red**, debemos hacer una operación lógica **Y (AND)** bit a bit entre la IP y la máscara.

Para obtener la **dirección de broadcast**, debemos hacemos una operación lógica **O (OR)** bit a bit entre la IP y el inverso de la máscara.

Debemos recordar que en una operación AND entre dos bits, el resultado es 1 si los dos bits son 1 y si no, el resultado es 0. En una operación OR, el resultado es 1 si cualquiera de los dos bits son 1 y si los dos son 0, el resultado es 0. Más información: »http://es.wikipedia.org/wiki/AND

Ejemplo: supongamos que nuestro PC tiene la IP 192.168.1.100/26, es decir, máscara 255.255.255.192 (ver tabla de máscaras). ¿Cuáles serán las direcciones de red y de broadcast?

Dirección de red



Dirección de broadcast

```
Dirección IP: 192.168.1.100      11000000 10101000 00000000 01100100
Inverso de la Máscara:           00000000 00000000 00000000 00111111
-------------------------------------------------------------------
Operación OR:                    11000000 10101000 00000000 01111111
Obtenemos la dirección de broadcast, que en decimal es 192.168.1.127
```

Averiguar la máscara a partir de las direcciones de red y de broadcast

Un método seguro para calcular la máscara de red partiendo de la dirección de red y de la dirección de broadcast, es pasar los valores a binario y luego compararlos bit a bit. Los bits que coincidan (sean iguales en la dirección de red y en la dirección de broadcast), corresponden a 'unos' en la máscara y los bits que difieran, corresponden a 'ceros' en la máscara, es lo que en lógica se conoce como operación lógica de equivalencia (operación XNOR) así pues:

```
Dir. de red: 192.168.0.0         11000000 10101000 00000000 00000000
Dir. Broadcast: 192.168.0.255    11000000 10101000 00000000 11111111
-------------------------------------------------------------------
Comparando bits tengo máscara:   11111111 11111111 11111111 00000000
```

Vemos que solo cambian los 8 últimos bits, lo que nos da la máscara. Para calcular la máscara, las posiciones que no cambian, son unos en la máscara y las que cambian, son ceros en la máscara.

Supernetting

Hacer supernetting consiste en utilizar un grupo de redes contiguas como si fueran una única red. Existe la posibilidad de utilizar varias redes de clase C (256 direcciones) contiguas para formar redes mayores. Ejemplo, si dispongo de dos clases C, 192.168.0.0/24 y 192.168.1.0/24, puedo formar una red 192.168.0.0/23 de forma que el espacio de direcciones pasa a ser de 512. Si dispongo de 256 clases C, podría formar una clase B y tendría la red 192.168.0.0/16 de forma que utilizando máscara 255.255.0.0 tendré 65536 IPs en la misma red.

Separando la red con subredes

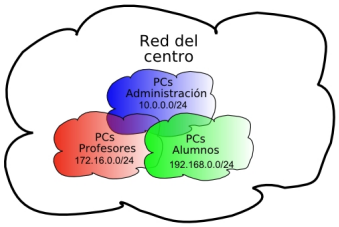
Como ya hemos comentado antes, por motivos de seguridad es conveniente separar las redes del centro. La mejor forma de proceder a la separación de las redes es físicamente, pero si fuera muy costoso por los tendidos de cable que serían necesarios, existe la posibilidad de

adquirir switches que dispongan de VLANes y separar por redes virtuales.

Si los recursos del centro son muy escasos y no llegan para cambiar los switches del centro por otros con VLANes, existe la posibilidad de utilizar rangos de IPs diferentes de forma que, a nivel IP, no se vean unas redes con otras, aunque a nivel ethernet estén interconectadas.

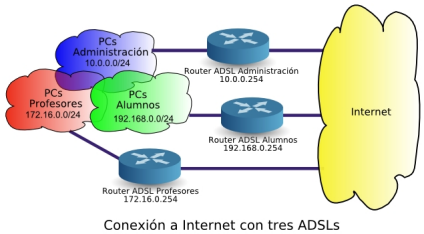
Rangos independientes

Una posibilidad para separar las redes, es utilizar rangos completamente independientes para cada una. Por ejemplo, podríamos utilizar los siguientes rangos:

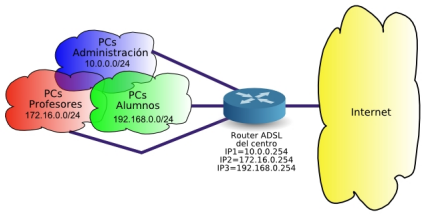


Al ser rangos independientes, desde una red no se puede acceder a la otra, lo que nos permitirá tener separadas las redes. Esta separación es una **separación lógica** pues aunque físicamente las redes están unidas, al tener direcciones IP pertenecientes a redes diferentes, no habrá comunicación entre ellas.

Para conectar a Internet las distintas redes, necesitaremos tres líneas ADSL, una para cada red, o bien necesitamos un router que admita varias IP en la interfaz LAN (IP aliases) para poder configurar una IP en cada rango y puedan todos los PCs alcanzar el router.



Conexión a Internet con tres ADSLs

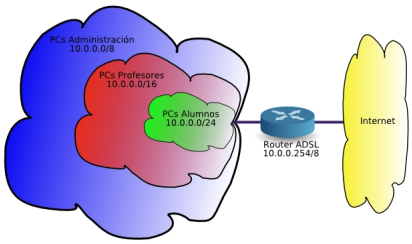


Conexión a Internet con una ADSL y router con IP alias

Rangos incluidos

Otra posibilidad para separar las redes, es utilizar rangos incluidos unos en otros, de forma que la red más exterior sería la red más segura a la que nadie puede acceder y la red más reducida a la que acceden todos. Esto permite utilizar un router normal, siempre y cuando le pongamos una IP que pertenezca al rango más reducido, pero con la máscara del rango más amplio, para que pueda ser accedido desde cualquier rango. La clave en este caso son las máscaras de red a utilizar. Ejemplo, podemos utilizar los siguientes rangos:

- Red administrativa: 10.0.0.0/8
- Red de profesores: 10.0.0.0/16
- Red de alumnos: 10.0.0.0/24
- IP del router: 10.0.0.254/8



Para evitar que PCs de una red se vean con los de otra, hay que utilizar IPs que no pertenezcan al rango de la red incluida. Podríamos por ejemplo, utilizar los siguientes rangos de direcciones para los PCs:

- Red administrativa, por ejemplo desde 10.1.0.1 hasta 10.1.0.254 (no pertenecen ni al rango de profesores ni al rango de alumnos)
- Red de profesores, por ejemplo desde 10.0.1.1 hasta 10.0.1.254 (no pertenecen al rango de alumnos)
- Red de alumnos, desde 10.0.0.1 hasta 10.0.0.253

Con este esquema de direccionamiento, no puede haber intercomunicación entre las distintas redes ya que aunque desde los PCs de rangos exteriores pueda iniciarse una comunicación hacia los PCs de rangos interiores, estos no podrán responder al pertenecer la IP origen a otro rango y no existir un router capaz de encaminar la respuesta.

Igual que en el caso anterior, la separación no es segura ya que si un alumno cambia su dirección IP o su máscara por una del rango de la red administrativa, podrá poner en peligro el sistema.

Separando la red con VLANes

Cableado estructurado

Muchos centros educativos ya disponen de **cableado estructurado** donde las rosetas de las distintas aulas y despachos van directas hacia el panel de parcheo en un armario situado en el cuarto de telecomunicaciones. Este tipo de infraestructura es idónea ya que facilita la reconfiguración de las redes y la localización de averías.

Lo ideal es que todos los centros educativos dispongan de cableado estructurado. Los nuevos edificios ya lo incorporan pero hacer el tendido en un edificio viejo, tiene un coste elevado, que ronda los 300 euros por roseta, es decir, para un centro un poco grande donde sea necesario instalar 100 rosetas, el coste rondaría los 30.000 euros.

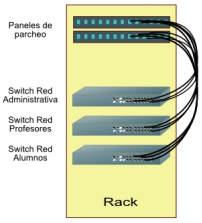
Al armario de telecomunicaciones, también llamado **rack**, llegan los cables provenientes de todas las rosetas y dispuestos en el denominado
panel de parcheo
. Desde el panel de parcheo salen
latiguillos
de red hacia las bocas de los
switches
.

En la siguiente figura podemos observar el panel de parcheo en la parte superior y cómo salen

de él un gran mazo de latiguillos hacia las bocas de los switches en la parte central.

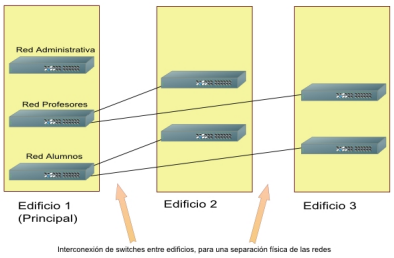
Separación física de las redes

Si nuestro centro educativo tiene un **único edificio** y disponemos de cableado estructurado, tendremos todas las rosetas centralizadas en un armario de telecomunicaciones similar al de la figura anterior. Separar las redes en este caso es muy sencillo, porque bastaría con adquirir tres switches y utilizar **un switch para cada red**, así tendríamos:



Si para alguna de las redes no fuera suficiente con un switch, deberíamos adquirir e interconectar entre sí todos los switches que fueran necesarios.

El problema surge cuando el centro tiene **varios edificios**, cosa bastante habitual ya que las ampliaciones de los centros suelen acometerse construyendo nuevos edificios dentro del recinto. En este caso, cada edificio tendrá su armario de telecomunicaciones y dentro de cada armario tendremos que tener diferentes switches, uno para cada red. Además tendremos que interconectar los switches de cada red de los diferentes edificios entre sí. Ejemplo, si en un centro educativo disponemos de tres edificios, la interconexión podría ser de la siguiente forma:



Ejemplo real: Separación de la red con VLANes

Los switches de gama media-alta permiten la creación de **VLANes**. Las VLANes son **redes virtuales** que se forman dentro de un switch y permiten dividir un switch como si fueran varios switches independientes. También permiten unir varios switches entre sí, formando un **gran switch**, para luego separar dicho gran switch a nuestro antojo, configurando las bocas en las VLANes que necesitemos.

Veámoslo con un **ejemplo real**: Supongamos un centro que está compuesto por cuatro edificios, uno principal y tres edificios más pequeños separados algunos metros. Se dispone de cableado estructurado con un único rack en cada edificio. En total hay 118 PCs:

- 5 PCs en la red administrativa, todos ellos en el edificio 1
- 18 PCs en la red de profesores, repartidos en los edificios 1, 2, 3 y 4
- 95 PCs en la red de alumnos, repartidos en los edificios 1, 2, 3 y 4

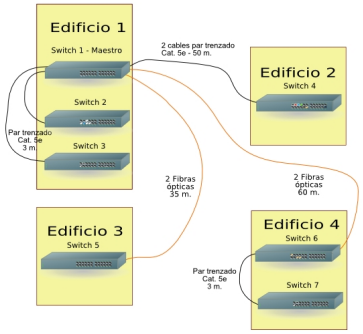
La situación de partida es una única red en la que están **mezclados** los PCs de administración con los PCs de profesores y los PCs de alumnos, aunque con rangos de IPs diferentes. Esto representa un peligro ya que desde los PCs de alumnos se podrían originar ataques hacia la red de profesores y la red de administración. El objetivo es **separar físicamente** la red en tres redes independientes:

- Red administrativa (PCs del equipo directivo y de la oficina)
- Red de profesores (PCs de sala de profesores y departamentos)
- Red de alumnos (Resto de PCs)

La electrónica de red está formada por siete switches modelo 'HP Procurve 2524/J4813A' de 24 bocas con dos slots de doble fibra para interconexión a alta velocidad (1 Gbps) con otros switches. Estos switches admiten la creación de VLANes. La distribución de los switches por los edificios es:

- 3 switches en el edificio 1
- 1 switch en el edificio 2
- 1 switch en el edificio 3
- 2 switch en el edificio 4

Existe interconexión entre el rack del edificio principal y los racks de los otros tres edificios. Desde el edificio 1 hacia el edificio 2, salen 2 cables de par trenzado categoría 5e. Desde el edificio 1 hacia los edificios 3 y 4, salen dos fibras ópticas, una para recepción y otra para transmisión. La interconectividad entre edificios se aprecia en la siguiente figura:



Configuración de la IP de los switches

Originalmente, los switches vienen con los parámetros de fábrica. Al estar interconectados, forman una única red a nivel 2 ó **nivel de enlace** (ethernet) aunque actualmente las redes están separadas a nivel 3 ó **nivel de red**(IP) con diferente direccionamiento IP. Esta situación es insegura ya que si un alumno configurara en su PC una IP libre de la red de profesores, podría comunicarse con los PCs de los profesores. Igualmente podría hacerlo con la red administrativa.

Se propone crear un stack o **pila de switches** para que los siete switches se comporten como un único **gran switch de 168 bocas** y después, crear **tres VLANes** diferentes para separar a nivel 2 las tres redes. La conexión a Internet se hará mediante tres líneas ADSL independientes, aunque se podría hacer con una única línea ADSL y uniendo las redes con dos routers neutros que dispongan de cortafuegos o con un router ADSL con al menos tres interfaces en la parte LAN, como los de la **serie 800 de Cisco** .

Lo primero que necesitamos es poner IPs a los switches, para posteriormente poder configurarles vía web. Inicialmente, los switches no tienen IP, sino que la toman por DHCP. Si disponemos un servidor DHCP, los switches tomarán automáticamente una IP, pero lo mejor es configurarles con una IP fija. Para ello utilizaremos un **cable serie RS-232** con conectores **DB9** hembra en ambos extremos, que nos permitirá conectar el switch con un PC. En el PC ejecutaremos la aplicación **HyperTerminal** . Crearemos una conexión nueva con emulación de terminal VT100 a 9600-N-8-1 sin control de flujo. Tras conectar el cable, pulsamos varias veces **Enter** hasta que veamos la pantalla de bienvenida y el prompt del switch. En este modelo concreto de switch, tenemos que escribir *setup* y pulsar *Enter* . Lo primero, establecemos el nombre del switch: switch1-edificio1 y ponemos una IP de nuestro rango de la red administrativa: 10.0.0.201. Luego guardamos la configuración permanentemente con el comando 'write memory' para que se grabe en la memoria flash del switch. Salimos con 'exit'.

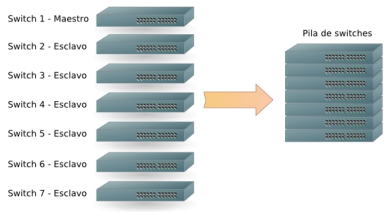
Este paso lo repetiremos en el resto de swithes de forma que todos nuestros switches tengan IP fija:

- switch1-edificio1: 10.0.0.201
- switch2-edificio1: 10.0.0.202
- switch3-edificio1: 10.0.0.203
- switch1-edificio2: 10.0.0.204
- switch1-edificio3: 10.0.0.205
- switch1-edificio4: 10.0.0.206
- switch2-edificio4: 10.0.0.207

Apilando los switches

Después abriremos un navegador de Internet e iremos a »http://10.0.0.201 para entrar en la configuración del switch. Como los swithes están interconectados entre sí, crearemos una pila de switches (switch-stack) para administrarles de forma conjunta. Entramos en el primero > Stacking y le convertimos en Maestro (Commander). Ponemos un nombre al stack, por ejemplo: red-ies. Entramos en el resto de swithes > Stacking y le convertimos en Esclavos (Members) de red-ies.

Ya disponemos de una pila de switches en la cual, el primer switch es el principal y el resto dependerán de él.



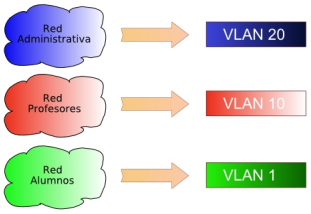
Creando de las VLANes

Por defecto los switches disponen de una VLAN denominada DEFAULT_VLAN e identificada como 'VLAN 1'. Dicha VLAN será la VLAN de alumnos ya que la mayoría de los PCs son PCs de alumnos.

Crearemos dos VLANes nuevas:

- VLAN 10: Red de Profesores
- VLAN 20: Red Administrativa

Para ello debemos entrar en Configuration > VLAN Configuration > Create VLAN.



Recableando los racks

Analizando el cableado en el rack, vemos que los cables están desordenados en los switches. Para simplificar la creación de VLANes, les ordenaremos.

La red administrativa está compuesta por 5 PCs:

- 5 en el switch 1

La red de profesores está compuesta por 18 PCs:

- 6 en el Switch 1
- 3 en el Switch 4
- 3 en el Switch 5
- 6 en el Switch 6

La red de alumnos está compuesta por 95 PCs:

- 5 en el Switch 1
- 20 en el Switch 2
- 20 en el Switch 3
- 10 en el Switch 4
- 10 en el Switch 5
- 10 en el Switch 6
- 20 en el Switch 7

Utilizaremos las **primeras bocas** de cada switch para la red de profesores, por tanto reconectaremos con los patch-coord o latiguillos cortos desde el panel de parcheo al switch de forma que las primeras bocas correspondan a los puntos de la red de profesores.

La red administrativa está compuesta por 8 PCs que están todos en el primer switch. Utilizaremos las **últimas bocas** del switch para dicha red, por tanto reconectaremos con los patch-coord o latiguillos cortos desde el panel de parcheo al switch de forma que las últimas 8 bocas correspondan a la red administrativa.

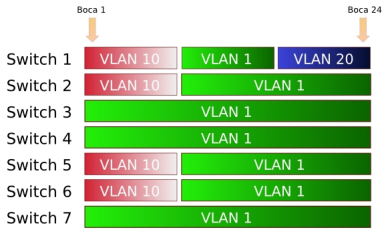
Asignando bocas a las VLANes

Para asignar las bocas de los switches a las VLANes correspondientes, debemos entrar en Configuration > VLAN Configuration > Modify VLAN.

Entraremos en el primer switch y asignaremos las bocas de 1 a 8 a la VLAN 10, seleccionando las 8 primeras bocas y asignándoles la etiqueta *untagged* con lo cual nos aseguramos que solo estarán en la VLAN 10. Lo mismo haremos con los switches 2, 5 y 6.

Después volveremos a entrar en el primer switch y asignaremos las bocas de 17 a 24 a la VLAN 20, seleccionando las 8 últimas bocas y asignándoles la etiqueta 'untagged' con lo cual nos aseguramos que solo estarán en la VLAN 20.

El resto de bocas quedarán en la VLAN 1, que será la VLAN de alumnos. En la siguiente figura podemos ver un esquema de cómo quedarían las VLANes en cada switch:



Como disponemos de un servidor web en la intranet y deseamos que accedan tanto desde la

red de alumnos como desde la red de profesores, a dicha boca le asignamos la VLAN 10 pero con la etiqueta 'tagged' para que siga perteneciendo a la VLAN 1. De ésta forma, si ponemos dos IPs al servidor, una de la red de alumnos y otra de la red de profesores, se podrá acceder al mismo desde ambas redes. Otra solución, quizás más segura, habría sido poner dos tarjetas de red al servidor y conectar por cada tarjeta a cada VLAN utilizando dos bocas.

Ya solo nos queda poner contraseña a los switches para que nadie pueda modificar la configuración. Debemos ir a Security > Set admin user y crear el usuario administrador: usuario 'admin', password 'secreta'. Afectará a todo el stack.

Para que los cambios de configuración se almacenen en la memoria flash del switch y tengan vigencia aunque les apaguemos, debemos entrar en modo consola mediante telnet y escribir el comando 'write memory'.

Ya tenemos la red totalmente separada. Desde la red de alumnos no se podrá acceder a la red de profesores ni a la red administrativa. Es equivalente a tener las redes en switches separados.

Existe la posibilidad de interconectar *switches con VLANes* y switches normales entre sí. El switch normal pertenecerá a la VLAN que pertenezca la boca por donde está interconectado al *switch con VLAN*