

TEMA 4

INDICE

1.- Direccionamiento IP.....	3
1.1.- Clases de direcciones.....	3
1.2.- Direcciones específicas.....	5
1.3.- Direcciones privadas.....	5
1.4.- Subredes.....	6
Ejemplo 1. División básica.....	7
Ejemplo 2. Varias subredes.....	8
1ª DIVISIÓN: 3 redes de 50 ordenadores.....	8
2ª DIVISIÓN 4 redes de 12 ordenadores.....	8
2.- Seguridad.....	10
2.1.- Esquema de red básico.....	10
2.2.- Esquema de red con una zona neutra.....	11
2.3.- Redes inalámbricas.....	12
3.- Configuración de routers.....	14
3.1.- Tablas de enrutado.....	14
3.2.- Elementos de configuración de un router.....	15
3.3.- Ejemplo de creación de una tabla de enrutado.....	16
4.- Servicios de red.....	18
4.1.- Servicio DHCP.....	18
4.2.- Servicio DNS.....	19
4.2.1.- Espacio de nombres de dominio.....	20
4.2.2.- Registrar un dominio.....	21
4.2.3.- Tipos de registro.....	21
4.3.- Servicio FTP.....	22
4.4.- Servicio Web.....	23
4.5.- Servicio de correo electrónico.....	24
4.6.- Servicio de acceso remoto.....	25

Direccionamiento IP y servicios de red

Caso práctico

María y Antonio se encuentran en la sala de reuniones de la empresa BK porque Ada les ha solicitado la puesta en marcha de la infraestructura de una empresa y cuento con vosotros para realizar este proyecto. En el diseño de la red hay que prestar especial cuidado en la seguridad del sistema.

María:— *Hola Antonio, esta es la primera red que vas a diseñar y para que te sea más fácil lo vamos a realizar juntos.*

Antonio: — *¡Muy bien, tengo muchas ganas de aprender!*

María: — *Para diseñar la red tenemos que hacerlo desde tres puntos de vista: nivel físico, lógico y la configuración de routers para asegurar la empresa.*

1.- Direccionamiento IP.

Caso práctico

María: — Antonio, como el diseño físico de la red ya esta listo ahora tenemos que establecer el direccionamiento IP de la red. Es decir, tenemos que indicar la dirección IP que van a utilizar los diferentes equipos.

Antonio: — ¿Para qué vale la IP?

María: — Es fácil, las direcciones IP se utilizan para que los equipos se puedan comunicar correctamente entre ellos, pero mejor vamos a verlo en profundidad.

Sin duda alguna Internet se ha convertido en la red más grande y con mayor crecimiento de la historia. Cada vez se ofrecen más servicios a través de Internet como comercio electrónico, banca electrónica, formación,... Por lo que se hace necesario que cualquier empresa disponga de una red y que pueda conectarse a Internet.

Los pasos que hay que realizar para la puesta en marcha de una red son:

- ✓ **Creación de la red a nivel físico.** Se crea la infraestructura necesaria para poner la red en funcionamiento. Para ello se instala el cableado de la red y luego se ponen en marcha los dispositivos de interconexión (hub, switch, routers...). Esta parte ya se ha visto en la unidad anterior por lo que en esta unidad vamos a realizar los siguientes pasos.
- ✓ **Creación de la red a nivel lógico.** Se crean las diferentes redes lógicas y se asignan las direcciones IP a los diferentes equipos de la red.
- ✓ **Configuración de los routers.** Se configuran los routers para permitir aceptar o denegar la comunicación que se realizan a través de él.

Además, veremos los conceptos más importantes sobre los servicios más utilizados en las redes de ordenadores e Internet.

Sin duda alguna la red más importante es Internet. En el siguiente enlace podrás ver la Historia de Internet.

http://es.wikipedia.org/wiki/Historia_de_Internet

Para poder trabajar en red, cada interfaz de red de un equipo (host o router) necesita una dirección IP, esta dirección identifica al equipo mediante una dirección única de 32 bits. Las direcciones IP se suelen representar por cuatro números decimales separados por puntos, que equivalen al valor de cada uno de los cuatro bytes que componen la dirección. Por ejemplo, una dirección IP válida sería 147.156.23.208.

El direccionamiento IP es la parte encargada de asignar de forma correcta a cada equipo una dirección IP, de forma que los equipos puedan comunicarse correctamente entre sí.

Para realizar correctamente la unidad primero debes ver todos sus contenidos y después puedes realizar ejercicios de redes. En el siguiente enlace puedes ver una relación de ejercicios de redes en el que tienes resuelto el primer ejercicio de cada tipo.

[Ejercicios de redes resueltos](#)

1.1.- Clases de direcciones.

Las direcciones IP tienen una estructura jerárquica. Una parte de la dirección corresponde a la red (netid), y la otra al host dentro de la red (hostid). Cuando un router recibe un datagrama (mensaje) por una de sus interfaces compara la parte de red de la dirección con las entradas contenidas en sus tablas

150.200	18.231
Netid	Hostid
Partes de una dirección IP	

(que normalmente sólo contienen direcciones de red, no de host) y envía el datagrama por la interfaz correspondiente.

Dependiendo del número de bits que se utiliza para indicar la red (netid) o el equipo (hostid) se definen varios tipos de direcciones de red. Los diferentes tipos de direcciones IP dan una mayor flexibilidad y permiten definir direcciones IP para grandes, medianas y pequeñas redes, conocidas como redes de clase A, B y C, respectivamente:

- ✓ Una red de clase A (que corresponde a las redes originalmente diseñadas) se caracteriza por tener a 0 el primer bit de dirección; el campo red ocupa los 7 bits siguientes y el campo host los últimos 24 bits. Puede haber hasta 126 redes de clase A con 16 millones de hosts cada una.
- ✓ Una red de clase B tiene el primer bit a 1 y el segundo a 0; el campo red ocupa los 14 bits siguientes, y el campo host los 16 últimos bits. Puede haber 16382 redes clase B con 65534 hosts cada una.
- ✓ Una red clase C tiene los primeros tres bits a 110; el campo red ocupa los siguientes 21 bits, y el campo host los 8 últimos. Puede haber hasta dos millones de redes de clase C con 254 hosts cada una.

Para indicar qué parte de la dirección corresponde a la red y qué parte al host, se suele utilizar una notación denominada “máscara de red”, consistente en poner a 1 los bits que corresponden a la parte de red y a 0 los que corresponden a la parte host. Así, por ejemplo, diremos que una red clase A tiene una máscara 255.0.0.0, lo cual equivale a decir que los ocho primeros bits especifican la red y los 24 restantes el host. Análogamente decimos que una red clase B tiene una máscara 255.255.0.0 y una clase C una máscara 255.255.255.0. Otra notación utilizada en muchos sistemas es expresar de forma conjunta con la dirección IP el número de bits de la máscara de red. Así por ejemplo, para expresar una dirección de clase A sería 12.15.19.1/8, 172.16.0.1/16 de clase B y 192.168.1.1/24 de clase C.

Además existen direcciones de clase D (no redes) cuyos primeros cuatro bits valen 1110, que se utilizan para definir grupos multicast (el grupo viene definido por los 28 bits siguientes).

Por último, la clase E, que corresponde al valor 11110 en los primeros cinco bits, está reservada para usos futuros. A partir de los valores de los primeros bits de cada una de las clases mencionadas anteriormente, se puede deducir el rango de direcciones que corresponde a cada una de ellas. Así pues, en la práctica es inmediato saber a qué clase pertenece una dirección determinada sin más que leer el primer byte de su dirección. La siguiente tabla resume toda la información esencial sobre los tipos de direcciones de Internet.

Clase	0xxxxxxx	HOSTS		
Tipo: Locales	Valores:	0, (255-2 ⁷)	0, (255-128)	0,127
Clase B	10xxxxxx	HOSTS		
Tipo: Medias	Valores:	2 ⁷ , (255-2 ⁶)	128, (255-64)	128, 191
Clase C	110xxxxx	HOSTS		
Tipo: Internet	Valores:	2 ⁷ +2 ⁶ , (255-2 ⁵)	192, (255-32)	192, 223
Clase D	1110xxxx			
Tipo: Multicast	Valores:	2 ⁷ +2 ⁶ +2 ⁵ , (255-2 ⁴)	224, (255-16)	224, 239
Clase E	1111xxxx			
Tipo: Futuro	Valores:	2 ⁷ +2 ⁶ +2 ⁵ +2 ⁴ , (255)	240, (255)	240, 255

A modo de resumen, a continuación puedes ver un esquema de las diferentes clases de direcciones y en la tabla puedes ver las características principales de las clases de direcciones.

Características principales de las clases de direcciones.					
Clase	Bits Reservados	Bits red/host	Número de redes	Número de ordenadores	Rango
A	0---	7/24	126	16777214	1.0.0.0 127.255.255.255
B	10--	14/16	16384	65334	128.0.0.0 191.255.255.255
C	110-	21/8	2097152	254	192.0.0.0 223.255.255.255
D	1110				224.0.0.0 239.255.255.255
E	111				240.0.0.0 255.255.255.255

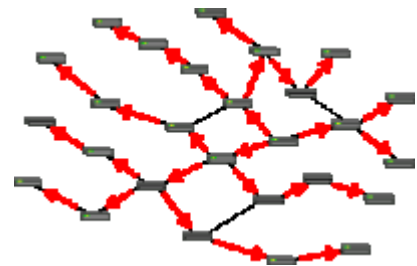
Indica la clase de dirección a la que pertenece la red 150.214.0.0/16.

- ☐ Clase A.
- ☒ **Clase B.**
- ☐ Clase C.
- ☐ Clase D.

1.2.- Direcciones específicas.

Existen unas reglas y convenios en cuanto a determinadas direcciones IP que es importante conocer:

- ✓ La dirección broadcast **255.255.255.255** se utiliza para enviar un mensaje a la propia red, cualquiera que sea (y sea del tipo que sea).
- ✓ La dirección **0.0.0.0** identifica al host actual.
- ✓ La dirección con el campo **host todo a ceros** se utiliza para indicar la red misma, y por tanto no se utiliza para ningún host. Por ejemplo, la dirección **193.147.7.0** identifica la red clase B que pertenece a la Universidad de Valencia.
- ✓ La dirección con el **campo host todo a unos** se utiliza como la dirección broadcast de la red indicada, y por tanto no se utiliza para ningún host. Por ejemplo, para enviar un mensaje broadcast en la red anterior, utilizaríamos la dirección **193.147.7.255**.
- ✓ La dirección con el **campo red todo a ceros** identifica a un host en la propia red, cualquiera que sea; por ejemplo, si queremos enviar un datagrama al primer host (1) de una red clase B podemos utilizar la dirección **0.0.0.1**. Esto permite enviar datagramas sin saber en qué red nos encontramos, aunque es preciso conocer si es clase A, B o C para saber qué parte de la dirección es red y qué parte es host.
- ✓ La dirección **127.0.0.1** se utiliza para pruebas loopback; todas las implementaciones de IP devuelven a la dirección de origen los datagramas enviados a esta dirección sin intentar enviarlos a ninguna parte.



Como consecuencia de las reglas 3 y 4 siempre hay dos direcciones no asignables a hosts en una red. Por ejemplo, si tenemos la red 200.200.200.0 (clase C) tendremos que reservar la dirección 200.200.200.0 para denotar la red misma, y la dirección 200.200.200.255 para envíos broadcast a toda la red; dispondremos pues de 254 direcciones para hosts, no de 256.

A modo de resumen, en la tabla puedes ver un ejemplo de las diferentes direcciones específicas.

Direcciones específicas.			
Dirección especial	Netid	Hostid	Ejemplo (193.147.7.32/24)
Dirección de red	Específica	Todo a 0	193.147.7.0
Dirección directa de broadcast	Específica	Todo a 1	193.147.7.255
Dirección broadcast limitada	Todo a 1	Todo a 1	255.255.255.255
Host específico en esta red	Todo a 0	Específica	0.0.0.325
Dirección loopback	127	Cualquiera	127.0.0.1

1.3.- Direcciones privadas.

La tabla de direcciones privadas, nos muestra que las direcciones de red **10.0.0.0**, **172.16.0.0** a **172.31.0.0**, y **192.168.0.0** a **192.168.255.0** están reservadas para redes privadas (intranets) por el RFC1918. Estos números no se asignan a ninguna dirección válida en Internet y por tanto pueden utilizarse para construir redes privadas. Por ejemplo, detrás de un firewall o cortafuegos, sin riesgo de entrar en conflicto de acceso a redes válidas de Internet.

Direcciones privadas		
Clase	Rango	Número de redes
A	10.x.x.x	1
B	De 172.16.x.x A 172.31.x.x	16
C	De 192.168.x.x a 192.168.255.x	256

Indica las direcciones de red que se consideran como privadas.

- ☒ 10.9.8.0/24.
- ☐ 193.168.0.0/24.
- ☒ 172.25.0.0/24.
- ☒ 192.168.0.0/24.

1.4.- Subredes.

A la hora de diseñar la red de una empresa uno de los aspectos que hay que tener en cuenta es optimizar el uso de redes públicas. Por ejemplo, es posible que tenga dos redes de servidores con 100 servidores cada una y desea que estén visibles en Internet.

Si se utilizan dos redes públicas de clase C se están desaprovechando los recursos de la empresa ya que una red pública de clase C puede tener 254 equipos y en el ejemplo se requieren 100. De esta forma se están desaprovechando más de la mitad de las direcciones IP disponibles en cada red pública. Hay que tener en cuenta que las direcciones IP públicas tienen un coste y que son limitadas.

En el ejemplo planteado es lógico que en vez de tener dos redes de clase C se utilice una única red para las dos redes de 100 servidores de cada una. Por lo tanto, resulta útil disponer de algún mecanismo que permita **dividir una red IP en trozos o subredes**.



Al realizar la división de redes se va creando así un nivel jerárquico intermedio entre la red y el host; de esa forma la empresa puede, por ejemplo, solicitar una red de clase B e ir asignando fragmentos de dicha red a cada oficina a medida de que vayan creándose. Supongamos que a la empresa se le asigna la clase B 156.134.0.0; de los 16 bits que en principio corresponden al host podría reservar los primeros 8 para la subred y dejar los 8 siguientes para el host, con lo que habría 256 subredes de 256 direcciones cada una. Desde fuera la red de la empresa seguiría siendo 156.134.0.0, ya que la estructura de subred no sería visible.

Para **dividir la red en subredes** se define una máscara en la que están a 1 los bits de la dirección que corresponden a la red-subred, y a 0 los que corresponden al host. Por ejemplo, la máscara 255.255.255.0 divide una red clase B en 256 subredes de 256 hosts pues tiene puestos a 1 los primeros 24 bits (los 16 de la clase B más los 8 de la subred). Se pueden hacer divisiones que no correspondan con bytes enteros, por ejemplo, si la máscara fuera 255.255.252.0 se estarían reservando los primeros 6 bits del campo host para la subred y dejando 10 para el host; con lo que podría haber hasta 64 redes con 1024 hosts cada una.

Al crear subredes hay **dos direcciones de cada subred que quedan automáticamente reservadas**: las que corresponden al **campo host todo a 0 y todo a 1**; éstas se emplean para la designación de la subred y para la dirección broadcast, respectivamente. Así si la red 156.134.0.0 se subdivide con la máscara 255.255.255.0 se crean 256 subredes del tipo 156.134.subred.host, siendo 156.134.subred.0 la dirección que identifica a toda la subred y 156.134.subred.255 la dirección broadcast de la subred. Por tanto, el número de hosts de una subred es siempre dos menos que el número de direcciones

que abarca; por lo que no tiene sentido crear subredes con la máscara 255.255.255.254 en las que el campo host tendría un bit, pues no dispondría de direcciones útiles.

Del mismo modo que los valores todo ceros o todo unos del campo host están reservados con un significado especial, los **valores todo ceros y todo unos del campo subred también son especiales**. El valor todo ceros se utiliza para representar la subred misma; por ejemplo si a la red 156.134.0.0 le aplicamos la máscara 255.255.255.0 el campo subred todo a ceros no debería utilizarse, pues resultaría ambiguo el significado de la dirección 156.134.0.0, que representaría tanto a dicha subred como a la red entera. Por otro lado, el campo subred todo a unos tampoco debería utilizarse porque de lo contrario el significado de la dirección 156.134.255.255 sería ambiguo, significaría tanto broadcast en la subred como en la red entera. Por consiguiente, en el campo subred también se pierden siempre dos direcciones, y tampoco tendría sentido crear máscaras con el campo subred de un bit.

A continuación veremos varios ejemplos de cómo se hacen las divisiones en subredes.

Ejemplo 1. División básica

Realiza la división de la dirección de red 193.147.12.0/24 en 4 redes de 50 ordenadores

¿Cuántas direcciones IP se pierden? $4 \times 2 = 8$

Para realizar la división correctamente se realizan los siguientes pasos:

Calculo la dirección de red

193.147.12.0/24

128 64 32 16 8 4 2 1
1 1 0 0 0 0 0 0 Mascara

Paso la parte hostid de la red a binario

193.147.12.00000000/24

Red1: 00 000000 - 00 111111 / 0 - 63/ 0 y 63 reservadas
Red2: 01 000000 - 01 111111 / 64 - 127/ 64 y 127 reservadas
Red3: 10 000000 - 10 111111 / 128-191/ 128 y 191 reservadas
Red4: 11 000000 - 11 111111 / 192 - 255/ 192 y 255 reservadas
8 reservadas 62 hosts por red

Calculo el número de bits que necesito para dividir ($2^n \geq n^\circ$ de divisiones)

$2^2 \geq 4 \rightarrow$ Utilizo 2 bits

Calculo el número de ordenadores que puede tener cada subred

La nueva máscara de red es de 26 bits (24 + 2) luego el número de equipos de cada red es $2^{(32-26)} = 2^6 = 64$ equipos. Realmente son 62 equipos ya que por cada red se pierden 2 direcciones IPs (la dirección de red y la de broadcast).

Realizo las divisiones

193.147.12.00000000/24

193.147.12.00000000/26 = 193.147.12.0/26 { 0 \rightarrow Dirección de red
1..62 \rightarrow IPs para equipos
63 \rightarrow Dirección broadcast

{
193.147.12.01000000/26 = 193.147.12.64/26 { 64 \rightarrow Dirección de red
65 ... 126 \rightarrow IPs para equipos
127 \rightarrow Dirección broadcast

193.147.12.10000000/26 = 193.147.12.128/26 { 128 \rightarrow Dirección de red
129..190 \rightarrow IPs para equipos
191 \rightarrow Dirección broadcast

$$193.147.12.11000000/26 = 193.147.12.192/26 \begin{cases} 192 \rightarrow \text{Dirección de red} \\ 193..254 \rightarrow \text{IPs para equipos} \\ 255 \rightarrow \text{Dirección broadcast} \end{cases}$$

Como tengo 4 redes y se pierden 2 direcciones IP por cada red, en total pierdo 8 IPs (antes se perdían únicamente 2 IPs).

Ejemplo 2. Varias subredes

Realiza la división de la dirección de red 193.147.12.0/24 en 3 redes de 50 ordenadores y 4 redes de 12 ordenadores. ¿Cuántas direcciones IP se pierden? $(3+4)*2=14$

En este caso la división de la red hay que hacerla en dos pasos. Primero se realiza la división de la red con un mayor número de ordenadores y luego el resto.

1ª DIVISIÓN: 3 redes de 50 ordenadores

Calculo la dirección de red

193.147.12.0/24

255 direcciones
3 subredes >50
4 subredes >12 = 48
255/4: 0-63/64-127/128-191
Hueco 192-255
64/4 = (192+0)-(192+15)=192-207
208-223/224-239/240-255

Paso la parte hostid de la red a binario

193.147.12.00000000/24

Calculo el número de bits que necesito para dividir ($2^n \geq n^{\circ}$ de divisiones)

$2^2 \geq 4 \rightarrow$ Utilizo 2 bits

Calculo el número de ordenadores que puede tener cada subred

La nueva máscara de red es de 26 bits (24 + 2) luego el número de equipos de cada red es $2^{(32-26)}=2^6=64$ equipos. Realmente son 62 equipos ya que por cada red se pierden 2 direcciones IPs (la dirección de red y la de broadcast).

Realizo las divisiones

193.147.12.00000000/24

$$193.147.12.00000000/26 = 193.147.12.0/26 \begin{cases} 0 \rightarrow \text{Dirección de red} \\ 1..62 \rightarrow \text{IPs para equipos} \\ 63 \rightarrow \text{Dirección broadcast} \end{cases}$$

$$193.147.12.01000000/26 = 193.147.12.64/26 \begin{cases} 64 \rightarrow \text{Dirección de red} \\ 65..126 \rightarrow \text{IPs para equipos} \\ 127 \rightarrow \text{Dirección broadcast} \end{cases}$$

$$193.147.12.10000000/26 = 193.147.12.128/26 \begin{cases} 128 \rightarrow \text{Dirección de red} \\ 129..190 \rightarrow \text{IPs para equipos} \\ 191 \rightarrow \text{Dirección broadcast} \end{cases}$$

$$193.147.12.11000000/26 = 193.147.12.192/26 \{ \text{Red libre para seguir dividiendo} \}$$

En este momento ya tengo las 3 redes de 50 equipos y una red libre. Ahora, voy a seguir dividiendo la dirección de red que queda libre.

2ª DIVISIÓN 4 redes de 12 ordenadores

Calculo la dirección de red

193.147.12.192/26

Paso la parte hostid de la red a binario

193.147.12.11000000/26

Calculo el número de bits que necesito para dividir ($2^n \geq \text{nº de divisiones}$)

$2^2 \geq 4 \rightarrow$ Utilizo 2 bits

Calculo el número de ordenadores que puede tener cada subred

La nueva máscara de red es de 28 bits (26 + 2) luego el número de equipos de cada red es $2^{(32-28)} = 2^4 = 16$ equipos. Realmente son 14 equipos ya que por cada red se pierden 2 direcciones IPs (la dirección de red y la de broadcast).

Realizo las divisiones

193.147.12.11000000/26

193.147.12.11000000/26 = 193.147.12.192/28 $\left\{ \begin{array}{l} 192 \rightarrow \text{Dirección de red} \\ 193..206 \rightarrow \text{IPs para equipos} \\ 207 \rightarrow \text{Dirección broadcast} \end{array} \right.$

193.147.12.11010000/26 = 193.147.12.208/28 $\left\{ \begin{array}{l} 208 \rightarrow \text{Dirección de red} \\ 209..222 \rightarrow \text{IPs para equipos} \\ 223 \rightarrow \text{Dirección broadcast} \end{array} \right.$

193.147.12.11100000/26 = 193.147.12.224/28 $\left\{ \begin{array}{l} 224 \rightarrow \text{Dirección de red} \\ 225..238 \rightarrow \text{IPs para equipos} \\ 239 \rightarrow \text{Dirección broadcast} \end{array} \right.$

193.147.12.11110000/26 = 193.147.12.240/28 $\left\{ \begin{array}{l} 240 \rightarrow \text{Dirección de red} \\ 241..254 \rightarrow \text{IPs para equipos} \\ 255 \rightarrow \text{Dirección broadcast} \end{array} \right.$

Resultado final

El resultado final sería:

- ✓ 193.147.12.00000000/24
 - ➔ 193.147.12.0/26 (red de 50 equipos)
 - ➔ 193.147.12.64/26 (red de 50 equipos)
 - ➔ 193.147.12.128/26 (red de 50 equipos)
 - ➔ 193.147.12.192/26
 - ➔ _ 193.147.12.192/28 (red de 12 equipos)
 - ➔ _ 193.147.12.208/28 (red de 12 equipos)
 - ➔ _ 193.147.12.224/28 (red de 12 equipos)
 - ➔ _ 193.147.12.240/28 (red de 12 equipos)

Como tengo un total de 7 redes y se pierden 2 direcciones IP por cada red, en total se pierden 14 IPs (antes se perdían únicamente 2 IPs).

Existen programas que nos ayudan a dividir redes, en el siguiente enlace podrás acceder a [ipcalculator](http://www.wildpackets.com/resources/free_utilities/ipsubnetcalc).

http://www.wildpackets.com/resources/free_utilities/ipsubnetcalc

Existen páginas web que te permiten realizar divisiones de redes. Un ejemplo de este tipo de páginas lo puedes encontrar en el siguiente enlace.

<http://www.aprendaredes.com/cgi-bin/ipcalc/ipcalc.cgi>

2.- Seguridad.

Caso práctico

Antonio: —He estado documentándome y he visto que no es recomendable poner todos los equipos en la misma red. ¿Puedes explicármelo mejor?

María: —Si ponemos todos los equipos en la misma red y se produce un ataque de seguridad entonces toda la red se verá comprometida. Las arquitecturas de seguridad se utilizan para que en caso de que haya una intrusión, se pueda limitar el acceso del intruso. Por eso, ahora vamos a definir la arquitectura de red y luego vamos a ver cómo configurar la tabla de enrutado de los routers de la empresa.

Uno de los aspectos más importantes a la hora de asegurar la red correctamente es la arquitectura de red. Una **arquitectura de red es el diseño de la red** en el que se emplean unos determinados componentes, cuya finalidad es la de canalizar, permitir o denegar el tráfico con los elementos apropiados.

Existen **varias arquitecturas de red**, desde la más sencilla, que utiliza simplemente un router, hasta otras más complejas, basadas en varios routers, proxys y redes perimetrales (o zonas neutras).

Antes de entrar en detalle con las arquitecturas de cortafuegos, se van a describir **tres elementos básicos** que intervienen en ella:

- ✓ **Router.** Equipo que permite o deniega las comunicaciones entre dos o más redes. Al ser el intermediario entre varias redes debe estar especialmente protegido ya que puede ser objeto de un ataque. Un router puede ser un dispositivo específico o un servidor que actúe como router.
- ✓ **Red interna.** Es la red interna de la empresa y, por lo tanto, es **donde se encuentran los equipos y servidores internos**. Dependiendo del nivel de seguridad que necesite la red interna se puede dividir en varias redes para permitir o denegar el tráfico de una red a otra.
- ✓ **Zona neutra.(o red perimetral).** Red añadida entre dos redes para proporcionar mayor protección a una de ellas. En esta red suelen estar ubicados los servidores de la empresa. Su principal objetivo es que ante una posible intrusión en unos de los servidores, se aíse la intrusión y no se permita el acceso a la red interna de la empresa.

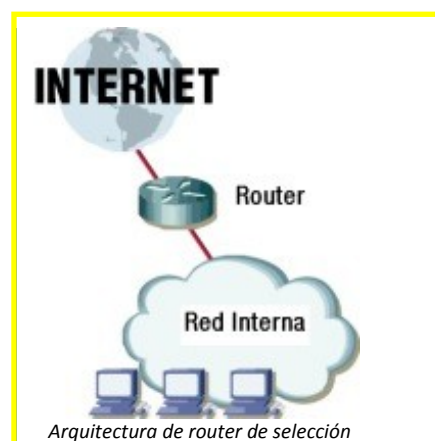
A continuación se va a ver el esquema de red básico que se puede utilizar cuando desea crear una red interna pero no hay servidores que ofrezcan servicios a Internet. En el caso de tener servidores públicos entonces se recomienda tener una zona neutra.

A partir del esquema de red con una zona neutra se pueden realizar todas las modificaciones que estimes oportunas dependiendo de la seguridad que quieras tener en la red interna, si quieres más zonas neutras, varias conexiones a Internet, etcétera. En este caso lo importante es adaptar el esquema de red a las necesidades de la empresa.

2.1.- Esquema de red básico.

Es la **configuración más simple** y consiste en el empleo de un router para comunicar la red interna de la empresa con Internet. Como el router es el encargado de comunicar ambas redes es ideal para permitir o denegar el tráfico.

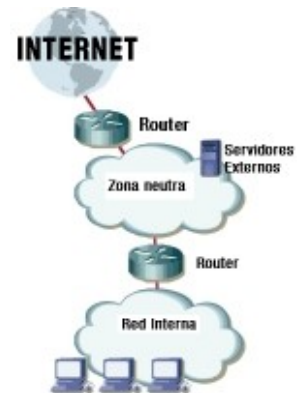
Esta arquitectura de red, aunque es **la más sencilla** de configurar es **la más insegura** de todas ya que toda la seguridad reside en un único punto: el router. En caso de que se produzca un fallo de seguridad en el router el atacante tiene acceso a toda la red interna.



Otro aspecto muy importante es que si se desea tener un servidor que ofrezca servicios a Internet hay que ubicarlo en la red interna. Es peligroso poner el servidor en la red interna ya que el router permite el tráfico al servidor y, en el caso de que se produzca un fallo de seguridad el atacante tiene acceso completo a la red interna. Para solucionar este problema se añade una nueva red a la empresa que se denomina **zona neutra o zona demilitarizada**.

2.2.- Esquema de red con una zona neutra.

Este esquema de red es considerado como el **esquema base** cuando quiere ofrecer servicios a Internet manteniendo un nivel adecuado de seguridad en la red interna. Como puede ver en la siguiente figura, esta arquitectura utiliza **dos routers** que permiten crear un perímetro de seguridad (red perimetral o **zona neutra**), en la que se pueden ubicar **los servidores accesibles desde el exterior**, protegiendo así a la red local de los atacantes externos.

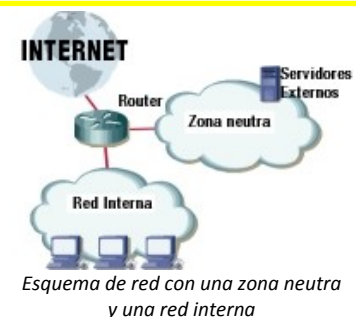


Esquema de red con una zona neutra y una red interna

Al tener dos redes independientes se puede indicar a través de los routers el tráfico que se permite entre Internet y la zona neutra, o el tráfico entre la zona neutra y la red interna. Lo normal es que el **router exterior** esté configurado para **permitir el acceso desde Internet** a los servidores de la zona neutra, especificando los puertos utilizados, mientras que el **router interior** **permite únicamente el tráfico saliente de la red interna** al exterior. De esta forma si se produce un fallo de seguridad y se accede a los servidores de la zona neutra, el atacante nunca podrá tener acceso a la red interna de la empresa.

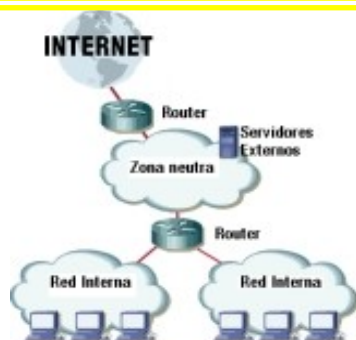
A partir del esquema de red con una red interna y una zona neutra puedes realizar las modificaciones que estimes oportunas para adaptarlo a tus necesidades. A continuación, a modo del ejemplo, se muestran algunas de las configuraciones más utilizadas:

- ✓ **Esquema de red con una zona neutra y una red interna utilizando un único router.** Aunque lo recomendable es utilizar dos routers para separar las redes también puede crear el esquema de red con un único router. En este caso el **router** tiene **tres interfaces de red** que le permiten crear la red interna, la zona neutra y conectarse a Internet. Aunque este esquema **no es tan fiable** como el anterior resulta más aconsejable que el modelo básico que no tiene ninguna zona neutra.



Esquema de red con una zona neutra y una red interna

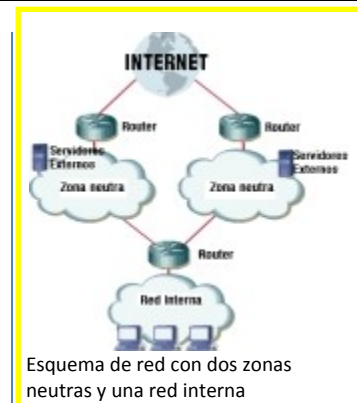
- ✓ **Esquema de red con una zona neutra y varias redes internas.** En los esquemas de red anteriores se ha creado una única red interna y por lo tanto todos los equipos y servidores internos están en la misma red dificultando así su seguridad. En el caso de que se tengan **equipos con diferentes tipos de seguridad o servidores internos**, resulta aconsejable crear varias redes internas para mejorar así la seguridad de la red. En la siguiente figura puede ver un esquema de red que tiene dos redes internas.



Esquema de red con una zona neutra y dos redes internas utilizando dos routers

- ✓ **Esquema de red con varias zonas neutras.** En el caso de que la empresa necesite dar servicios bien diferenciados al exterior puede optar por tener **dos zonas neutras**, o incluso **dos salidas diferentes a Internet**. Por ejemplo, en el esquema de red de la figura tiene dos zonas neutras y dos salidas a Internet. En este caso una de las zonas neutras se puede utilizar para ubicar los servidores públicos (por ejemplo, un servidor web o ftp) y la otra zona neutra se puede utilizar

para que los clientes se conecten por VPN a la red interna de la empresa. De esta forma, los clientes en la VPN estarán en una zona neutra que se encuentra aislada de la red de servidores públicos y la red interna.



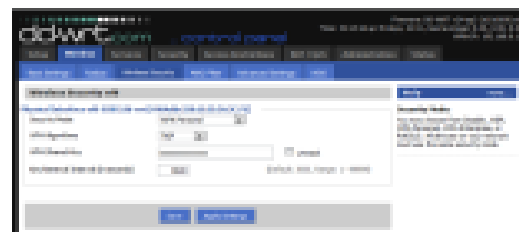
2.3.- Redes inalámbricas.

Las **redes de área local inalámbricas (WLAN, Wireless Local Area Networks)** permiten que varios dispositivos puedan transmitir información entre ellos a través de **ondas de radio** sin necesidad de cables. Las **ventajas** saltan a la vista. La principal es la **libertad** que proporcionan a los usuarios de red, que pueden llevar su ordenador (especialmente si es portátil) a cualquier sitio sin perder la conexión a Internet.

El acceso sin necesidad de cables es la razón por la que son tan populares las redes inalámbricas, y es a la vez el **problema** más grande de este tipo de redes en cuanto a la **seguridad** se refiere. Cualquier equipo que se encuentre cerca del punto de acceso podrá tener acceso a la red inalámbrica.

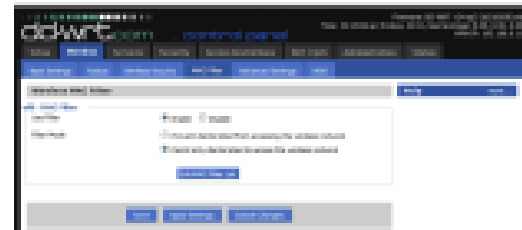
Para poder considerar una **red inalámbrica** como **segura** debería cumplir los siguientes requisitos:

- ✓ **Aislar la red inalámbrica de la red interna de la empresa creando una zona neutra.** Al utilizar una zona neutra es posible limitar el acceso desde la red inalámbrica a los servicios y/o equipos que estime oportunos. Por ejemplo, una opción muy útil es permitir el acceso de la red inalámbrica únicamente a Internet o algún determinado servicio de la red interna.
- ✓ Las **ondas de radio** deben **confinarse** tanto como sea posible.
- ✓ Los **datos** deben **viajar cifrados** para impedir que sean capturados por otro equipo. Como ya has estudiado en la unidad anterior, para que los datos vayan cifrados existen dos **protocolos de encriptación**:
 - **WEP (Wired Equivalent Privacy).** WEP fue el primer protocolo de encriptación introducido en el primer estándar 802.11 en el año 1999. Está basado en algoritmo RC4 con una clave secreta de 40 ó 104 bits, combinado con un vector de inicialización (IV: initialization vector) de 24 bits.
 - **WPA (WiFi Protected Access).** Es un estándar creado para corregir los fallos de seguridad del protocolo WEP. Fue diseñado para utilizar un servidor de autenticación (normalmente un servidor RADIUS), que distribuye claves diferentes a cada usuario (a través del protocolo 802.1x); sin embargo, también se puede utilizar en un modo menos seguro de clave pre-compartida (PSK: Pre-Shared Key). La información es cifrada utilizando el algoritmo RC4, con una clave de 128 bits y un vector de inicialización de 48 bits.
- ✓ Debe existir algún **mecanismo de autenticación en doble vía** que permita al **cliente** conectarse realmente a su **punto de acceso**, y que permita verificar que al **punto de acceso** sólo se conectan los **clientes legítimos**. Para permitir la autenticación de los clientes es posible utilizar un **servidor de autenticación Radius**.



Seguridad red inalámbrica

- ✓ **Filtrado de dirección MAC.** Un mecanismo adicional de seguridad es permitir el acceso a la red inalámbrica únicamente a unos determinados equipos. Para indicar los equipos que pueden acceder a la red inalámbrica se utiliza la dirección física (MAC) del adaptador de red.



Filtrado de direcciones MAC

Indica la medida de seguridad que NO permite proteger una red inalámbrica.

- ☐ Seguridad WEP.
- ☐ Seguridad WPA.
- ☐ Utilizar una correcta arquitectura de cortafuegos.
- ☒ Que cada usuario de la red utilice en su equipo Linux.

3.- Configuración de routers.

Caso práctico

Antonio: — *María, ya hemos terminado de configurar la red, los ordenadores se comunican entre sí pero no tenemos Internet ¿qué falta por configurar?*

María: — *Falta uno de los puntos más importantes, los routers. Los routers son los encargados de comunicar varias redes y además, permiten asegurar la red de la empresa. Veamos cómo se configuran.*

Como hemos visto anteriormente, un router es un dispositivo de interconexión que permite regular el tráfico que pasa entre varias redes. Un router es muy útil a la hora de defendernos de posibles intrusiones o ataques externos. Pero como desventaja es que un router no se configura por sí sólo. Mientras que un router bien configurado puede ser muy útil, un router mal configurado no nos proporciona ningún tipo de protección o, simplemente, no llega a comunicar dos redes.

Si quieres obtener más información, puedes consultar la correspondiente entrada de la wikipedia.

<http://es.wikipedia.org/wiki/Enrutador>

3.1.- Tablas de enrutado.

Para configurar un router debemos crear lo que se denomina “tabla de enrutado” o “directivas de firewall”. En ella se guardan las acciones que hay que realizar sobre los mensajes que recibe el router para redirigirlos a su destino. Existen dos tipos de encaminamiento: **encaminamiento clásico** y **encaminamiento regulado**.

Con el **encaminamiento clásico**, las reglas utilizadas para encaminar los paquetes se basan, exclusivamente, en la dirección destino que aparece en la cabecera del paquete. Así se distinguen las siguientes reglas:

- ✓ Permitir un equipo de nuestra red.
- ✓ Permitir cualquier equipo de nuestra red.
- ✓ Permitir un equipo de otra red.
- ✓ Permitir cualquier equipo de otra red.

La última regla (por defecto) se aplica en el caso de que no se cumpla ninguna de las anteriores y se suele utilizar para poder enviar los mensajes a la puerta de enlace de la red.

Sin embargo, en la actualidad, con la explosión del uso de Internet y la llegada del concepto de calidad de servicio (QoS) y la seguridad, los routers utilizan el llamado **encaminamiento regulado**, con el que, a la hora de escribir la tabla de enrutado, se pueden utilizar los siguientes elementos:

- ✓ **Interfaz:** interfaz de red por donde se recibe la información.
- ✓ **Origen / Destino:** origen y destino del mensaje. Normalmente el origen y el destino de un mensaje es una dirección IP, pero algunos routers permiten utilizar como dirección origen y destino usuarios o grupos de usuarios.
- ✓ **Protocolo:** permitir o denegar el acceso a los puertos es importante porque las aplicaciones servidoras (que aceptan conexiones originadas en otro ordenador) deben 'escuchar' en un puerto para que un cliente (que inicia la conexión) pueda conectarse. Por ejemplo un servidor web trabaja en el puerto 80, un servidor de FTP en el puerto 21, etcétera.
- ✓ **Seguimiento:** indica si el router debe de realizar un seguimiento de los lugares por los que pasa un mensaje.
- ✓ **Tiempo:** espacio temporal en el que es válida la regla.
- ✓ **Autenticación de usuarios:** indica si el usuario debe de estar autenticado para utilizar la regla.
- ✓ **Acción:** especifica la acción que debe realizar el router. Un router puede realizar las siguientes acciones:

- **Aceptar:** dejar pasar la información.
- **Denegar:** no deja pasar la información.
- **Reenviar:** envía el paquete a una determinada dirección IP.

```
[root@redhatserver root]# iptables -F
Chain INPUT (policy DROP)
target    prot opt source                destination
ACCEPT    all  --  anywhere                anywhere

Chain FORWARD (policy DROP)
target    prot opt source                destination
ACCEPT    tcp  --  10.0.0.0/24             anywhere
ACCEPT    udp  --  10.0.0.0/24             anywhere
ACCEPT    all  --  anywhere                anywhere

Chain OUTPUT (policy DROP)
target    prot opt source                destination
ACCEPT    all  --  anywhere                anywhere
[root@redhatserver root]#
```

Ejemplo de configuración de iptables

Si quieres obtener más información, puedes consultar los siguientes enlaces:

http://es.wikipedia.org/wiki/Tabla_de_enrutamiento

<http://technet.microsoft.com/es-es/library/cc779122%28WS.10%29.aspx>

3.2.- Elementos de configuración de un router.

Existen diferentes tipos de routers por lo que en un principio podemos caer en la tentación de pensar que el proceso de configuración para cada router es totalmente diferente a los demás. Pero entre los router más utilizados, ya sean hardware o software, tenemos:

- ✓ FireWall 1 de CheckPoint.
- ✓ Private Internet Exchange (PIX) de Cisco System.
- ✓ IOS Firewall Feature Set de Cisco System.
- ✓ Firewall del núcleo de Linux, Iptables.
- ✓ Enterprise Firewall de Symantec.
- ✓ Internet Security and Acelerador (ISA Server) de Microsoft.

Si se comparan los elementos que utilizan los diferentes routers (ver tabla) puede ver cómo los más utilizados a la hora de realizar una tabla de enrutado son la **interfaz**, la **dirección origen y destino**, el **puerto** y la **acción** que debe realizar el router.

Comparativa sobre los elementos de las tablas de enrutado.

Modelo	Interfaz	Origen/destino	Protocolo	Seguimiento	Tiempo	Autenticación de usuarios	Acción
FireWall 1		**					
PIX			*				
IOS Firewall							
Firewall Linux							
Enterprise Firewall		**					
ISA Server		**	*				

*Distingue entre puerto de origen y destino.

**Permiten especificar como origen o destino direcciones IPs o usuarios.

A la hora de indicar la **dirección de origen** o la **dirección de destino** es importante utilizar la **máscara de red** para indicar un mayor o menor número de ordenadores. Así por ejemplo, si en la dirección destino utiliza la dirección de clase B 142.165.2.0/16 se hace referencia a todas las direcciones IP del tipo 142.165.x.x. Si utiliza la dirección de clase C 192.165.2.0/24, hace referencia a las direcciones del tipo 192.165.2.x. Por lo tanto, si aumentamos la máscara de red, estamos disminuyendo el número de direcciones IP a las que se hace referencia y si disminuimos la máscara de red, entonces se hace referencia a un mayor número de direcciones IP. En la tabla siguiente, puedes ver algunas de las posibilidades más habituales.

Ejemplos de utilización de la máscara de red en la configuración de routers	
Ejemplo	Comentario
192.165.2.23/32	Representa a un único ordenador (por ejemplo, un servidor web)
192.165.2.0./24	Representa a todas las direcciones IP del tipo 192.165.2.X
192.165.0.0/16	Representa a todas las direcciones IP del tipo 192.165.X.X
192.0.0.0/8	Representa a todas las direcciones IP del tipo 192.X.X.X
0.0.0.0/0	Representa a todas las direcciones IP del tipo X.X.X.X

Si quiero indicar que el equipo 15.2.7.8 no tiene acceso a Internet, ¿cuál es la mejor forma de indicar la dirección?

- ☐ 15.2.7.8/0.
- ☐ 15.2.7.8/8.
- ☐ 15.2.7.8/24.
- ☒ 15.2.7.8/32.

Durante el filtrado de paquetes se aplica la regla de "coincidencia total". Todos los criterios de la regla tienen que coincidir con el paquete entrante; en caso contrario, no se aplica la regla. Esto no significa que se rechace el paquete o que se elimine, sino que la regla no entra en vigor. Normalmente, las reglas se aplican en orden secuencial, de arriba hacia abajo. Aunque hay varias estrategias para implementar filtros de paquetes, las dos que se describen a continuación son las más utilizadas por los especialistas de seguridad:

- ✓ **Construir reglas desde la más específica a la más general.** Esto se hace así para que una regla general no "omita" a otra más específica, pero conflictiva, que entra dentro del ámbito de la regla general.
- ✓ **Las reglas deberían ordenarse de tal forma que las que más se utilizan estén en la parte superior de la lista.** Esto se hace por cuestiones de rendimiento. Normalmente un router detiene el procesamiento de una lista cuando encuentra una coincidencia total.



Ejemplo de interfaz de un router: ISA Server

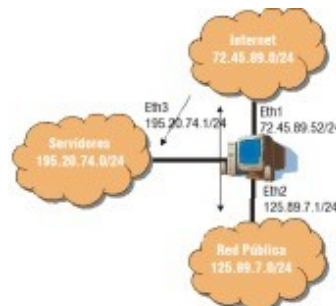
3.3.- Ejemplo de creación de una tabla de enrutado.

La figura muestra un router conectado a tres redes diferentes. Debemos crear el conjunto de reglas para permitir que: la red pública se conecte a Internet y que los servidores sean accesibles desde Internet; el servidor web se encuentra en la dirección 195.20.74.5 y el servidor de correo se encuentra en la dirección 195.20.74.7.

La tabla de enrutado representa el conjunto de reglas que actúan como medida de seguridad para determinar si se permite que un paquete pase o no.

El conjunto de reglas está formado por seis reglas sencillas. La complejidad de las reglas tiene propósitos educativos para mostrar los conceptos del procesamiento de reglas (directiva) del filtrado de paquetes. Las notas acerca de la implementación se incluyen siguiendo la descripción de cada línea del conjunto de reglas.

Las reglas están agrupadas en tres grandes grupos: las primeras tres reglas se aplican al tráfico que tiene como origen Internet y como destino la red de servidores. Las reglas 4 y 5 permiten la comunicación entre Internet y la red pública. Y la última regla, se utiliza siempre para indicar que el tráfico que no cumpla las reglas anteriores debe ser denegado.



Ejemplo de red

Tabla de enrutamiento					
Reglas	Interfaz	Origen	Destino	Puerto	Acción

1: Conexión de internet (Eth1) de cualquier host (0.0.0.0/0) entrando al servidor web (195.20.74.5/32) por el puerto 80->Aceptar

2: Conexión de internet (Eth1) de cualquier host (0.0.0.0/0) entrando al servidor de correo (195.20.74.5/32) por el puerto 25/110->Aceptar

3: Conexión de internet (Eth1) de cualquier host (0.0.0.0/0) entrando a cualquier servidor(195.20.74.5/32) cualquier puerto ->Denegar

1	Eth1	0.0.0.0/0	195.20.74.5/32	80	Aceptar
2	Eth1	0.0.0.0/0	195.20.74.7/32	25, 110	Aceptar
3	Eth1	0.0.0.0/0	195.20.74.0/24	-	Denegar
4	Eth1	0.0.0.0/0	125.89.7.0/24	-	Aceptar
5	Eth2	125.89.7.0/24	0.0.0.0/0	-	Aceptar
6	-	-	-	-	Denegar

4 y 5: Conexión de/a internet (Eth1) de/a cualquier host (0.0.0.0/0) a/de la red pública (125.89.7.0/24)->Aceptar

6: Denegar todo lo que no esté en anteriores reglas

- ✓ **Regla 1.** Esta regla permite el acceso entrante en el puerto 80, que normalmente se utiliza para el tráfico http. El host que está en 195.20.74.5 es el servidor web. La organización no puede predecir quién va a tener acceso a su sitio Web, por lo que no hay restricción en las direcciones IP de origen.
- ✓ **Regla 2.** Esta regla permite el acceso entrante a los puertos 25 y 110, que normalmente se utiliza para correo electrónico (el puerto 25 es el servidor smtp o correo saliente y el puerto 110 es el servidor pop3 o correo entrante). El servidor de correo está en la dirección 195.20.74.7. Al igual que en la regla anterior, como no se puede predecir quién va a tener acceso al servidor de correo no se restringen las direcciones IP de origen.
- ✓ **Regla 3.** Esta regla elimina todos los paquetes que tienen como destino la red donde se encuentran los servidores. Como la **regla 1 y 2, se ejecutan antes, sí se permite el tráfico que va dirigido a los servidores web y correo electrónico.** Si se pone esta regla al principio de la tabla de enrutado, no se podrá acceder a ningún servidor.
- ✓ **Reglas 4 y 5.** La cuarta regla deja pasar el tráfico que va desde Internet a la red pública. Y la quinta regla deja pasar el tráfico que va desde la red pública a la red de Internet.
- ✓ **Regla 6.** Esta regla bloquea explícitamente todos los paquetes que no han coincidido con ningún criterio de las reglas anteriores. La mayoría de los dispositivos de análisis realizan este paso de forma predeterminada, pero es útil incluir esta última regla de limpieza. Incluirla aclara la aplicación de la directiva predeterminada y, en la mayoría de los casos, permite registrar los paquetes que coinciden con ella. Esto es útil por motivos jurídicos y administrativos.

4.- Servicios de red.

Caso práctico

María: — Ahora ya tenemos lista la red y ahora tenemos que empezar a ver los servicios que va ofrecer la red.

Antonio: — ¿Servicios? ¿Qué es un servicio?

María: — Los servicios permiten que la red y sus usuarios dispongan de un determinado recurso o información. Existen muchos servicios, pero sin duda alguna el servicio más utilizado es el servidor Web. Un servidor Web es un servicio que permite que los usuarios puedan ver las páginas web. Existen muchos servicios importantes que vamos a ver ahora y tenemos que decidir cómo los vamos a utilizar.

Aunque los servicios más conocidos en Internet son el servidor Web y el de correo electrónico, también existen otros servicios necesarios y menos conocidos que permiten crear la infraestructura de una red. Estos servicios son los siguientes:

- ✓ **Encaminamiento.** Permite a un servidor actuar como router para permitir la comunicación entre dos o más redes.
- ✓ **Servidor DHCP.** Permite asignar automáticamente la configuración IP de los equipos clientes de la red. Este servicio es muy importante ya que facilita la conexión de los equipos a la red. Por ejemplo, cuando un portátil se conecta a una red obtiene su configuración IP a través de un servidor DHCP.
- ✓ **Servidor DNS.** Permite mantener una equivalencia entre un nombre y su dirección IP. Por ejemplo, el nombre www.adminso.es equivale a 150.214.150.30.

Además de los servicios ya comentados existen otros muchos servicios como por ejemplo, compartir datos, acceso remoto a sistema, monitorización de equipos, etcétera. A continuación se van a ver los servicios más utilizados.

Posteriormente, veremos los dominios de Internet y los servicios de Internet más importantes.

Si quieres obtener más información, puedes ver el siguiente enlace

http://es.wikipedia.org/wiki/Servicio_de_red

4.1.- Servicio DHCP.

El mantenimiento y la configuración de la red de los equipos de una red pequeña es relativamente fácil. Sin embargo, cuando se dispone de una red grande con equipos heterogéneos, la administración y asignación de direcciones IPs, así como la configuración de los equipos, se convierte en una tarea compleja de difícil mantenimiento y gestión. Cualquier cambio en la configuración de red, el servidor de nombres, la dirección IP asignada, la puerta de enlace...conlleva un excesivo tiempo para ejecutar la tarea.

Por otra parte, en entornos con equipos móviles, la gestión y asignación de direcciones supone una tarea compleja que, aunque puede resolverse con la asignación de direcciones IP estáticas, conlleva la asociación fija de una dirección IP al mismo equipo, para evitar conflictos, y la imposibilidad de su reutilización si un portátil no está conectado a la red local en un momento determinado.

Éste es el mismo problema que se presenta en el entorno de trabajo de un ISP; o se dispone de un sistema de asignación dinámica y flexible que permita reutilizar las direcciones de tal forma que sólo los equipos conectados en un momento determinado a la red tienen asignada una dirección IP, o se dispone de una dirección IP distinta por cada cliente que tenemos, algo inviable con el número de usuario conectados a Internet. El servidor DHCP surge ante la necesidad de realizar la asignación dinámica y automática de las direcciones IP de una red.

El servidor DHCP se encarga de gestionar la asignación de direcciones IP y de la información de configuración de la red en general. Para ello, necesita de un proceso (dhcpd) y un fichero de configuración (/etc/dhcpd.conf)

Los datos mínimos que un servidor de DHCP proporciona a un cliente son:

- ✓ Dirección IP.
- ✓ Máscara de red.
- ✓ Puerta de enlace o gateway.
- ✓ Dirección IP del servidor DNS.

El protocolo DHCP incluye dos métodos de asignación de direcciones IP:

- ✓ **Asignación dinámica.** Asigna direcciones IPs libres de un rango de direcciones establecido por el administrador en el fichero/etc/dhcpd.conf. Es el único método que permite la reutilización dinámica de las direcciones IP.
- ✓ **Reserva por dirección IP.** Si queremos que un dispositivo o equipo tenga siempre la misma dirección IP entonces la mejor forma es establecer una reserva. Para ello, en el fichero de configuración, para una determinada dirección MAC, se asignará una dirección IP. Este método es muy útil para aquellos dispositivos que no queramos que cambien de dirección IP. Por ejemplo, es deseable que una impresora en red tenga siempre la misma dirección IP ya que si cambia de dirección IP deberemos configurar nuevamente la impresora en todos los equipos clientes que la utilicen.



Interfaz web para configurar el servicio DHCP en el punto de acceso dd-wrt

Si quieres obtener más información, puedes ver más información sobre el servicio DHCP. http://es.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol

4.2.- Servicio DNS.

Los equipos informáticos se comunican entre sí mediante una dirección IP como 193.147.0.29. Sin embargo nosotros preferimos utilizar nombres como www.mec.es porque son más fáciles de recordar y porque ofrecen la flexibilidad de poder cambiar la máquina en la que están alojados (cambiaría entonces la dirección IP) sin necesidad de cambiar las referencias a él.

Inicialmente la asociación de nombres con su respectiva dirección IP se realizaba de forma local a través del fichero /etc/hosts (Linux) o \winnt\system32\driver\etc\hosts (Windows) en los que se guarda cada nombre junto a su respectiva dirección IP. Con todo, esta opción presenta varios problemas.

Por un lado, todos los equipos de la red están obligados a conocer cualquier cambio para actualizar sus ficheros apropiadamente. Es decir, ante, por ejemplo, la inserción de un nuevo elemento en la red, debe añadirse en los ficheros locales de cada equipo los datos referentes a su nombre y dirección IP. Este hecho indica la poca escalabilidad y manejabilidad de esta opción, sobre todo si hablamos de Internet o, sin llegar a este extremo, de cualquier red local que tenga, por ejemplo, más de veinte ordenadores. Además, el mantenimiento tan descentralizado y dependiente de ficheros locales conlleva un alto riesgo de falta de sincronización y descoordinación entre los equipos de la red y, por tanto, de la información que manejan.

Para paliar estos problemas se ideó el sistema de resolución de nombres (DNS) basado en dominios, en el que se dispone de



Empresa de registro de dominios www.arsys.es

uno o más servidores encargados de resolver los nombres de los equipos pertenecientes a su ámbito, consiguiendo, por un lado, la centralización necesaria para la correcta sincronización de los equipos, un sistema jerárquico que permite una administración focalizada y, también, descentralizada y un mecanismo de resolución eficiente. En la actualidad, Google también nos ofrece un servicio de resolución de nombres, a través de

En la actualidad, Google también nos ofrece un servicio de resolución de nombres, a través de Google Public DNS. Este servicio es accesible a través de las siguientes IPs siguientes:

Direcciones IPv4: 8.8.8.8 y 8.8.4.4 Direcciones IPv6: 2001:4860:4860::8888 y 2001:4860:4860::8844

4.2.1.- Espacio de nombres de dominio.

Al igual que los sistemas de fichero se organizan en árboles jerárquicos y el nombre absoluto de un fichero es el formado por los distintos directorios que recorremos hasta encontrar el fichero, separados por el carácter '/' (o '\' en sistemas Windows). El sistema de nombres de dominios también se estructura con un árbol jerárquico en el que las distintas ramas que encontramos reciben el nombre de dominio y el nombre completo de un equipo (el equivalente al nombre de un fichero) o FQDN (path absoluto) es el nombre resultante de recorrer todos los dominios por los que pasamos, desde las hojas hasta la raíz del árbol utilizando, en este caso, el carácter '.' (punto) como separador.

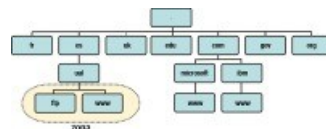


El sistema de nombres de Internet presenta, por tanto, una estructura jerárquica en árbol, en el que cada rama constituye lo que se denomina un dominio de Internet, y dependiendo de la profundidad del árbol, hablaremos de dominios de primer, segundo o tercer nivel –pudiendo existir más, aunque no es habitual-.

En el primer nivel del árbol encontramos que los nombres de los nodos ya están establecidos de antemano, existiendo dos tipos de divisiones: geográfica y organizativa. Con la primera se distingue una rama -dominio- por país: **.es** para España; **.uk** para Gran Bretaña; **.de** para Alemania,... Con la segunda se establece una rama por tipo de organización: **.com** para empresas, independientemente del país en el que se encuentren; **.int** para organizaciones establecidas mediante tratados internacionales; **.org** para organizaciones no gubernamentales y, por último, **.edu**, **.gov** y **.mil** para organizaciones educativas, del gobierno y el ejército de EEUU. Posteriormente, se han introducido nuevos dominios de primer nivel como **.name** para nombres de personas; **.info** para proveedores de servicios de información; **.web** para empresas relativas a servicios web; etcétera.

Cada rama del árbol jerárquico en el que se estructura el sistema de nombres de dominio, recibe el nombre de dominio y, para la resolución global de nombres no es determinante quién se encarga de mantener la información asociada a cada dominio. Con esta estructura, la asignación de nombres de una rama del árbol de primer nivel se delega en un responsable -la empresa pública REDES para España- el cual puede decidir, a su vez, delegar la autoridad de resolución de los nombres de las distintas ramas en las que se divide, en otras corporaciones.

Un servidor DNS puede encargarse de gestionar los datos de un dominio completo o parte de un dominio. El conjunto de datos que puede administrar un servidor de nombres recibe el nombre de zona. En la siguiente figura puede ver que el servidor DNS será el encargado de gestionar los datos del dominio **ual.es**



Representación de una zona gestionada por un servidor

Por otra parte, con la importancia que ha adquirido la resolución de nombres -nadie usa ya las direcciones IP, sino los nombres asociados- una característica crucial es la máxima disponibilidad del servicio. Para ello, una buena solución es que existan varios servidores independientes capaces de realizar el mismo servicio de tal forma que la autoridad de resolución de zona siga recayendo en un servidor aunque éste puede permitir que otros puedan responder a requerimientos de los clientes. Los servidores que tienen asignada la autoridad de resolución de nombres y que gestionan la base de datos de la zona, reciben el nombre de servidores primarios. Los servidores que pueden resolver

requerimientos para una zona, pero que la fuente de información la obtienen de otro servidor, reciben el nombre de servidores secundarios.

Para que no existan problemas de sincronización entre servidores, los secundarios deben conseguir sus datos del servidor primario mediante el proceso llamado “transferencia de zona” que no es más que el traspaso de todas los pares dirección IP-nombre simbólico que gestiona el servidor. Cada vez que se modifique un dato del servidor primario debe transmitirse a todos los secundarios que estén declarados para el correcto funcionamiento del sistema.

De esta forma, no sólo se consigue aumentar la disponibilidad del servicio, sino hacerlo más eficiente ya que la carga de trabajo puede repartirse entre distintos servidores. Si el objetivo es exclusivamente éste, existe otro tipo de servidores llamados caché cuya finalidad es la de responder a peticiones de resolución, consultando, previamente, las peticiones almacenadas en memoria y, si no se corresponde con ninguna de ellas, iniciar el proceso de resolución de nombres recursivo visto anteriormente. Los servidores caché sólo son útiles si el número de usuarios es suficientemente elevado para sacar provecho de la caché de direcciones.

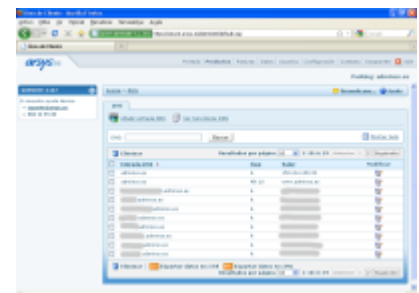
4.2.2.- Registrar un dominio.

Cualquier persona física con residencia en España, así como empresas constituidas según la legislación española, puede solicitar el registro de dominios a través de la página nic.es o bien, por medio de los agentes registradores acreditados. Los nombres de dominio se deben, según la reglamentación española, corresponder con:

- ✓ Nombre (o abreviatura) de una empresa que la identifique de forma inequívoca.
- ✓ Nombres comerciales o de marcas.
- ✓ Nombre de personas tal y como aparecen en su DNI, con un máximo de 60 caracteres.
- ✓ Nombres de profesiones y el apellido o nombre del profesional que se dedica a dicha labor o del nombre del establecimiento.
- ✓ Denominaciones de origen, en cuyo caso debe solicitarlo el órgano regulador de dicha denominación.

Una vez registrado el dominio podremos acceder a una web que nos permitirá gestionar los distintos registros del dominio. Por ejemplo, a continuación se muestra la interfaz de gestión del dominio adminso.es.

Los cambios que realices en un registro estarán visibles en Internet antes de 24 horas.



Gestión del dominio adminso.es

4.2.3.- Tipos de registro.

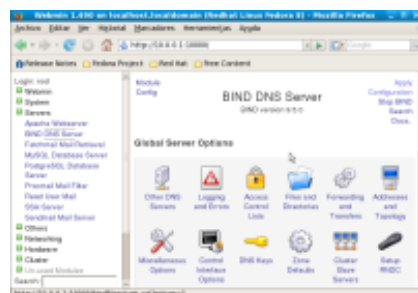
Tal y como hemos visto anteriormente, un servidor de nombres es el encargado de gestionar un dominio o parte de un dominio. El conjunto de datos que administra el servidor recibe el nombre de zona. Por ejemplo, el servidor de nombres del Ministerio de Educación es el encargado de gestionar la zona **mec.es**.

Para administrar una zona existe un servidor DNS primario y normalmente, además del servidor primario se dispone de uno o más servidores secundarios que únicamente realizan una copia de la zona.

La comunicación entre los servidores DNS se realizan mediante lo que se llama una **transferencia de zona**. Una **zona** (por ejemplo, **mec.es**) tiene **registros DNS** (por ejemplo, **www.mec.es**) que son los encargados de asociar un nombre a una dirección IP. En la tabla se muestran los diferentes tipos de registros DNS de un servidor de nombres entre los que se destacan:

- ✓ **Registro tipo A**. Es el más utilizado y permite asociar un **nombre** (por ejemplo, **www.mec.es**) con una **dirección IP** (por ejemplo: **193.147.0.29**).
- ✓ **Registro tipo CNAME**. Permite establecer un **alias entre dos registros**. Por ejemplo, **www.mec.es** es igual que **ftp.mec.es**.
- ✓ **Registro MX**. Este registro es muy importante ya que permite indicar dónde se encuentra el **servidor de correo electrónico (Mail eXchanger)**. Este tipo de registro se asocia siempre a otro nombre y permite asignar prioridades en los servidores. Así la entrada **MX10** indica el **primer servidor de nombres**, **MX20** el segundo, etcétera.

Tipos de registro	
Registro	Función
SOA	Inicio de autoridad. Fija los parámetros de la zona.
NS	Servidor de nombre. Nombre de un servidor autorizado para el dominio.
A	Dirección de anfitrión. Asigna a un nombre una dirección.
CNAME	Nombre canónico. Establece un alias para un nombre verdadero.
MX	Intercambio de correo. Especifica qué máquinas intercambian correo.
TXT	Texto arbitrario. Forma de añadir comentarios.
PTR	Puntero. Permite la conversión de una dirección a nombre.
HINFO	Descripción de la computadora. CPU y S.O.
WKS	Servicios públicos disponibles en la computadora.



Administrador del servidor DNS con bind

Si quieres obtener más información, puedes ver más información sobre el servicio DNS.

http://es.wikipedia.org/wiki/Domain_Name_System

4.3.- Servicio FTP.

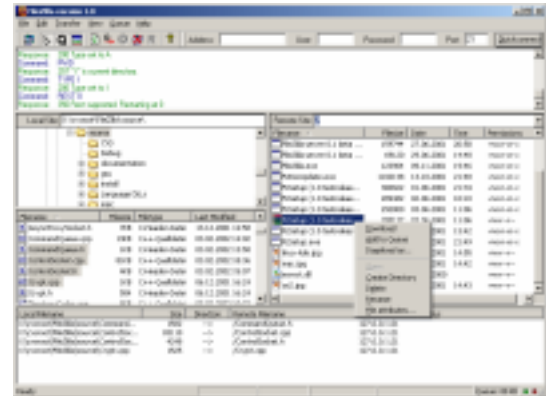
FTP es el protocolo más antiguo de la capa de aplicación TCP/IP que permite la transferencia de ficheros. FTP define un protocolo cliente/servidor que describe la manera en que se establece la comunicación entre los servidores y clientes FTP. Concretamente, permite el envío y la recepción de archivos del servidor.

Aunque pueden contemplarse otras posibilidades, hay dos tipos fundamentales de acceso a través de FTP:

- ✓ **Anónimo**. La comunicación se realiza sin ningún tipo de identificación y, por lo tanto el usuario tendrá muy pocos privilegios en el servidor. En este caso, el usuario estará confinado en un directorio público donde puede descargar los archivos allí ubicados pero sin posibilidad de escribir o modificar ningún fichero.
- ✓ **Acceso autorizado**. El usuario establece la comunicación con una cuenta de usuario. Tras identificarse, se confina al usuario a su directorio predeterminado desde donde puede descargar

ficheros y, si la política del sistema lo permite, también escribir. Esta opción es ampliamente utilizada para que los usuarios puedan acceder a sus ficheros o para poder actualizar de forma remota su portal web.

Existen programas que permiten conectarse cómodamente a un servidor FTP (por ejemplo: filezilla, cufteft, vsftp, Internet Explorer). Sin embargo, la forma más simple de utilizar un servidor FTP es estableciendo una conexión por línea de comandos. Para poder conectarte a un servidor puedes ejecutar "ftp servidor" en el intérprete de comandos de tu sistema, y utilizando los comandos FTP que aparecen en la tabla de comandos de FTP, sin importar el sistema operativo que utilices, puedes trabajar en el servidor FTP.



Filezilla

A continuación mostramos la tabla de comandos de FTP, que citamos anteriormente, y que te servirá para poder utilizar el protocolo FTP.

Tabla Comandos FTP	
Comando	Descripción
ascii	Establece el tipo de transferencia de archivos a la modalidad ASCII.
bell	Emite una señal acústica cuando se completa un comando.
binary	Establece el tipo de transferencia de archivos a modalidad Binario.
bye	Finaliza la sesión ftp y cierra.
cd	Cambia el directorio de trabajo del ordenador remoto.
cdup	Cambia el directorio de trabajo del ordenador remoto al raíz.
close	Finaliza la sesión ftp.
delete	Borra archivos remotos.
dir	Lista el contenido del directorio remoto.
get	Obtiene un archivo del ordenador remoto.
help	Muestra la ayuda.
lcd	Cambia el directorio local de trabajo.
ls	Lista el contenido del directorio remoto.
mkdir	Crea un directorio.
open	Establece una conexión con el servidor ftp remoto.
put	Envía un archivo al ordenador remoto.
pwd	Muestra el directorio de trabajo en la máquina remota.
quit	Finaliza la sesión ftp y sale.
rename	Renombra un archivo.
rmdir	Elimina un directorio de la máquina remota.
status	Muestra el estado actual.
system	Muestra información sobre el sistema remoto.
user	Envía nueva información de usuario.

4.4.- Servicio Web.

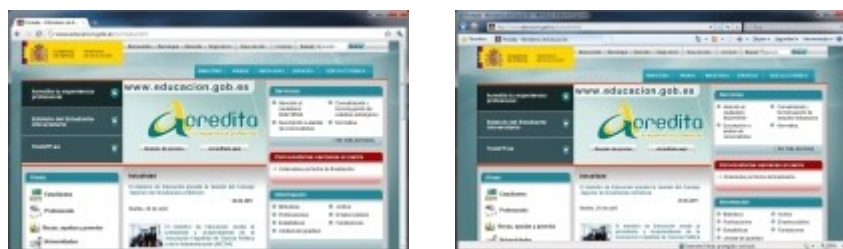
Conocido con el nombre de World Wide Web, o más concretamente, por sus siglas WWW que, además, aparecen en el nombre de prácticamente todos los servidores web, el servicio web es, posiblemente, el servicio más extendido y utilizado de los que se ofrecen en Internet, con el permiso del sistema de correo electrónico.

El servidor web se encarga del almacenaje y la difusión de información mediante la distribución de páginas HTML. Su arquitectura se basa en la archiconocida cliente-servidor, típica de los servicios basados en TCP/IP, en la que se distinguen: el proceso servidor, como por ejemplo, Apache, Internet Information Server e Iplanet y el proceso cliente (también llamado navegador), como Mozilla Firefox, Google Chrome, Internet Explorer, etcétera.

El servidor es el que almacena y sirve las páginas HTML. Los navegadores se encargan, además de realizar la petición de la página deseada, de interpretarla y mostrar el resultado al usuario. Para que el cliente y el servicio se entiendan, se comunican mediante el protocolo HTTP. Este es un protocolo orientado a conexión y del tipo de solicitud-respuesta, es decir, no se guarda información de estado sino que toda interacción entre el cliente y el servidor se fundamenta en pedir y servir.

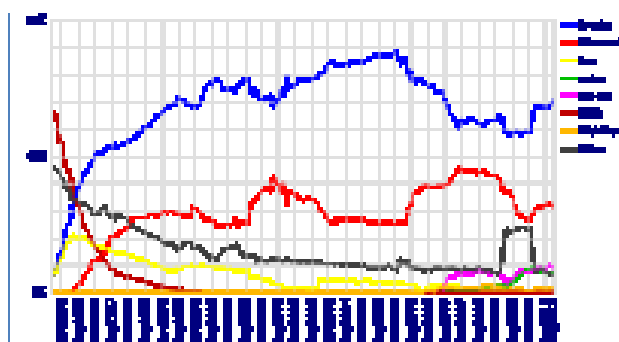
Para identificar qué página desea un cliente, éste realiza una petición con la que especifica toda la información necesaria para que tanto el navegador como el servidor web interpreten correctamente qué recurso desea el cliente y dónde se encuentra. La petición se realiza mediante el llamado localizador universal de recursos (URL).

Para solicitar páginas y visualizarlas, los **clientes web (navegadores)** presentan un **entorno gráfico** y amigable que facilita la **navegación por la WWW**. Existen multitud de navegadores con la misma funcionalidad y, prácticamente, con las mismas características. Las principales diferencias entre los clientes web residen en el número e importancia de vulnerabilidades que presentan así como en diferentes matizaciones que existen en cuanto a la interpretación del código HTML y que puede impedir la correcta visualización de algunas páginas en determinados clientes. En las siguientes figuras puede ver dos navegadores diferentes: a la izquierda Google Chrome y a la derecha Internet Explorer.



Ejemplos de clientes Web

En la actualidad existen varios **servidores Web** tanto para sistemas GNU/Linux como para sistemas Windows. Como se observa en la siguiente gráfica, **Apache es el servidor Web más utilizado** en Internet muy por encima del resto de competidores.



Cuota de mercado de servidores web (Fuente: www.netcraft.com)

4.5.- Servicio de correo electrónico.

El sistema de correo electrónico es, junto al WWW, el servicio proporcionado en Internet que más importancia y auge ha presentado, al menos en cuanto al número de usuarios se refiere. De hecho, se considera como uno de los principales factores que ha popularizado el uso de Internet.

Este servicio es un sistema para la transferencia de mensajes, rápido y eficiente, ideado bajo la arquitectura cliente-servidor típica de Internet. No es simplemente un programa cliente que se

comunica con un servidor mediante un protocolo de aplicación, sino que está compuesto por varios subsistemas, cada uno con una funcionalidad determinada que interaccionan entre sí mediante distintos protocolos de aplicación. La funcionalidad que todo usuario espera de este sistema es:

- ✓ Composición del mensaje.
- ✓ Transferencia desde el origen al destino sin intervención del usuario.
- ✓ Generación de un informe de la transmisión del mensaje.
- ✓ Visualización de los correos recibidos.
- ✓ Gestión de los correos: lectura, borrado, almacenaje...

Otras características que puede aportar un sistema de correo electrónico a un usuario son, por ejemplo, la redirección de correos de unas cuentas a otras, listas de correo, correo de alta prioridad o cifrado... El sistema de correo electrónico lo constituyen cuatro componentes:

- ✓ Cliente de correo electrónico (MUA). Ofrece los mecanismos necesarios para la lectura y composición de los mensajes de correo.
- ✓ Servidor de correo saliente (MTA). Recibe el correo electrónico y lo envía al servidor de entrada del dominio del receptor. Normalmente utiliza los protocolos SMTP o IMAP.
- ✓ Servidor de correo entrante (MTA). Almacena los correos electrónicos enviados a los buzones que gestiona y cuando un cliente consulta su cuenta le envía los correos electrónicos que ha recibido. Normalmente utiliza los protocolos POP o IMAP.

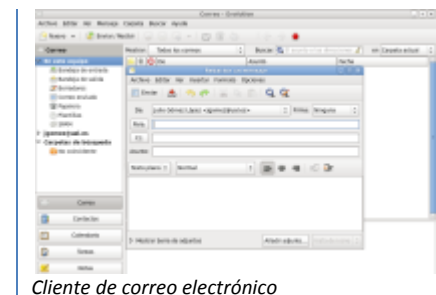


Para comunicar los distintos subsistemas que componen la arquitectura del servicio de correo, se dispone de los protocolos:

- ✓ Simple Mail Transport Protocol (SMTP) encargado del transporte de los mensajes de correo.
- ✓ Postal Office Protocol (POP) e Internet Message Access Protocol (IMAP) encargados, ambos, de comunicar a los agentes de usuario (MUA) con los agentes de entrega de correo (MDA). Además, permiten la gestión, por parte de los usuarios, de sus buzones de correo.

El cliente de correo electrónico es una aplicación que proporciona al usuario una interfaz -más o menos amigable- con los mecanismos necesarios para escribir, recibir y contestar a mensajes. A continuación se muestra el cliente de correo Evolution.

Existen clientes de correo electrónico basados en diferentes interfaces, de texto o gráfica, que introducen más o menos familiaridad y coste de aprendizaje para el usuario, pero todos presentan las mismas funciones: recepción, composición y ordenación mediante carpetas y subcarpetas del correo electrónico.

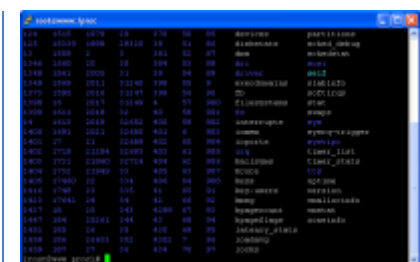


Si desea gestionar el correo electrónico en un terminal GNU/Linux puede ejecutar el comando mail.

4.6.- Servicio de acceso remoto.

Los servicios que permiten acceder de forma remota a un equipo a través de la red. Los servicios de acceso remoto se clasifican en dos categorías:

- ✓ Acceso remoto en modo terminal. Para acceder a un servidor GNU/Linux en modo terminal es posible utilizar los servicios Telnet (Telecommunication NETwork) y SSH (Secure SHell). Actualmente el servicio SSH es el más utilizado ya que garantiza la seguridad de las



comunicaciones mientras que el servicio Telnet no se utiliza por ser inseguro.

- ✓ **Acceso remoto en modo gráfico.** Para acceder en modo gráfico a un servidor puede utilizar el servicio VNC (Windows y GNU/Linux) o el servicio de Escritorio remoto (o Terminal Server) en sistemas Windows.



Conexión a Escritorio Remoto



Acceso al servidor por VNC con Vinagre (Linux)

¿Qué servicio permite conectarse a un servidor de forma remota por terminal?

- ☒ **Telnet.**
- ☐ VNC.
- ☐ Terminal server.
- ☒ **SSH.**