

Redes: Diseño, Configuración, Topología y Seguridad

Por Paco Aldarias Raya

Impreso: 4 de julio de 2004

Email: pacolinux@inicia.es

Web: <http://pagina.de/pacodebian>

Con Linux Debian. En Valencia (España)

Este documento es de libre reproducción siempre que se cite su fuente.

Realizado con: **L^AT_EX**

Índice

| | |
|---|----------|
| Índice | 1 |
| 1. Introducción | 1 |
| 2. Redes Privadas y Públicas | 1 |
| 2.1. Clases de redes Privadas | 1 |
| 3. Valores de las máscaras de subred: subneting | 2 |
| 4. Máscaras válidas para una red. | 2 |
| 4.1. Máscaras válidas para una red de clase A | 2 |
| 4.2. Máscaras válidas para una red de clase B | 3 |
| 4.3. Máscaras válidas para una red de clase C | 4 |
| 5. Router | 4 |
| 6. Bastions Hosts | 5 |

| | |
|---|-----------|
| 7. Firewalls (Cortafuegos - FW) | 6 |
| 7.1. ¿Por qué es necesaria la seguridad en las redes? | 6 |
| 7.2. Seguridad | 9 |
| 8. Diseño de redes | 9 |
| 8.1. Diseño de red básico. Sin Cortafuegos | 9 |
| 8.2. Diseño básico de un red C/B | 10 |
| 8.3. Diseño de red clase B con DMZ y firewall: Red Segura | 11 |
| 9. Dirección de Broadcast | 12 |
| 9.1. Ejemplo | 12 |
| 9.2. Ejemplo | 13 |
| 10. Saber en que red se encuentra un ip | 13 |
| 10.1. Ejemplo | 13 |
| 10.2. Ejemplo | 14 |
| 11. Segmentar una clase C en subredes | 14 |
| 11.1. Dirección de Red: 192.168.0.0/24 | 14 |
| 11.2. Dirección de Red: 192.168.0.0/25 | 14 |
| 11.3. Dirección de Red: 192.168.0.0/26 | 15 |
| 11.4. Dirección de Red: 192.168.0.0/27 | 15 |
| 12. Bibliografía | 15 |
| Índice alfabético | 20 |

1. Introducción

Vamos a ver que significa una dirección ip, una máscara, una subred. Veremos ejemplos de redes con sus topologías , e ips.

2. Redes Privadas y Públicas

Si tenemos que diseñar una red, lo normal es coger una ip pública, y el resto de la red deberá usar ips privadas.

2.1. Clases de redes Privadas

Existen direcciones IP reservadas para redes privadas, para usos internos, que se establecieron por convenio. Estas direcciones no son vistas desde el exterior, no son públicas, y sus rangos son:

- Clase A: 10.0.0.0
- Clase B: 172.16.0.0 a 172.31.0.0
- Clase C: 192.168.X.0 (con X variando).

3. Valores de las máscaras de subred: subnetting

Dado que los bits en la máscara de subred han de ser contiguos, esto reduce la cantidad de máscaras de subred que se pueden crear.

Tabla Binario - Octeto

| BITS DEL OCTETO | DECIMAL |
|-----------------|---------|
| 00000000 | 0 |
| 10000000 | 128 |
| 11000000 | 192 |
| 11100000 | 224 |
| 11110000 | 240 |
| 11111000 | 248 |
| 11111100 | 252 |
| 11111110 | 254 |
| 11111111 | 255 |

La mascara por defecto de la clase A es 255.0.0.0

La mascara por defecto de la clase B es 255.255.0.0

La mascara por defecto de la clase C es 255.255.255.0

Una máscara de subred por si sola no nos dice nada. Tiene que ir siempre relacionada con una dirección IP, ya que por ejemplo la máscara 255.255.255.0 puede ser relacionada con una clase A o B, porque estamos haciendo Subnetting o con la clase C, sin hacer Subnetting.

4. Máscaras válidas para una red.

4.1. Máscaras válidas para una red de clase A

Aparecen los siguiente valores:

- MÁSCARA: MÁSCARA DE SUBRED
- BITS: NUMERO DE BITS DE RED
- REDES: NUMERO DE REDES
- MÁQUINAS: NUMERO DE MÁQUINAS.

Subnet Mask Networking Bits Number of Networks Number of Hosts. Class A

| MÁSCARA | BITS | REDES | MAQUINAS |
|-----------------|------|-----------|------------|
| 255.255.255.252 | /30 | 4,194,304 | 2 |
| 255.255.255.248 | /29 | 2,097,152 | 6 |
| 255.255.255.240 | /28 | 1,048,576 | 14 |
| 255.255.255.224 | /27 | 524,288 | 30 |
| 255.255.255.192 | /26 | 262,144 | 62 |
| 255.255.255.128 | /25 | 131,072 | 126 |
| 255.255.255.0 | /24 | 65,536 | 254 |
| 255.255.254.0 | /23 | 32,768 | 510 |
| 255.255.252.0 | /22 | 16,384 | 1,022 |
| 255.255.248.0 | /21 | 8,192 | 2,046 |
| 255.255.240.0 | /20 | 4,096 | 4,094 |
| 255.255.224.0 | /19 | 2,048 | 8,190 |
| 255.255.192.0 | /18 | 1,024 | 16,382 |
| 255.255.128.0 | /17 | 512 | 32,766 |
| 255.255.0.0 | /16 | 256 | 65,534 |
| 255.254.0.0 | /15 | 128 | 131,070 |
| 255.252.0.0 | /14 | 64 | 262,142 |
| 255.248.0.0 | /13 | 32 | 524,286 |
| 255.240.0.0 | /12 | 16 | 1,048,574 |
| 255.224.0.0 | /11 | 8 | 2,097,150 |
| 255.192.0.0 | /10 | 4 | 4,194,302 |
| 255.128.0.0 | /9 | 2 | 8,388,606 |
| 255.0.0.0 | /8 | 1 | 16,777,216 |

4.2. Máscaras válidas para una red de clase B

Subnet Mask Networking Bits Number of Networks Number of Hosts.
Class B

| MÁSCARA | BITS | REDES | MAQUINAS |
|-----------------|------|--------|----------|
| 255.255.255.252 | /30 | 32,768 | 2 |
| 255.255.255.248 | /29 | 8,192 | 6 |
| 255.255.255.240 | /28 | 4,096 | 14 |
| 255.255.255.224 | /27 | 2,048 | 30 |
| 255.255.255.192 | /26 | 1,024 | 62 |
| 255.255.255.128 | /25 | 512 | 126 |
| 255.255.255.0 | /24 | 256 | 254 |
| 255.255.254.0 | /23 | 128 | 510 |
| 255.255.252.0 | /22 | 64 | 1,022 |
| 255.255.248.0 | /21 | 32 | 2,046 |
| 255.255.240.0 | /20 | 16 | 4,094 |
| 255.255.224.0 | /19 | 8 | 8,190 |
| 255.255.192.0 | /18 | 4 | 16,382 |
| 255.255.128.0 | /17 | 2 | 32,764 |
| 255.255.0.0 | /16 | 1 | 65,534 |

4.3. Máscaras válidas para una red de clase C

Subnet Mask Networking Bits Number of Networks Number of Hosts.
Class C

| MÁSCARA | BITS | REDES | MAQUINAS |
|-----------------|------|-------|----------|
| 255.255.255.252 | /30 | 64 | 2 |
| 255.255.255.248 | /29 | 32 | 6 |
| 255.255.255.240 | /28 | 16 | 14 |
| 255.255.255.224 | /27 | 8 | 30 |
| 255.255.255.192 | /26 | 4 | 62 |
| 255.255.255.128 | /25 | 2 | 126 |
| 255.255.255.0 | /24 | 1 | 254 |

5. Router

Un router es un elemento de red, que permite cambiar de red. Debemos de darle siempre la puerta de enlaces. Y tiene por tanto una tabla de rutas.

Tipos:

1. Router Adsl: Es el router que nos proporciona el proveedor de internet (ISP).
2. Router Software. Es un pc que permite pasar los paquetes de una red a otra. Linux da soporte para este tipo de software, llamado reenvio (forwarding).
3. Router Hardware. Es un router que permite pasar de una subred a otra. Hace de enmascaramiento. Es un dispositivo, q está sobre 42 euros. Es una opción interesante si la red es nueva, y no se disponen de ordenadores antiguos para hacerlos por software.

6. Bastions Hosts

Denominaremos como Bastion Host a un sistema informático catalogado como punto peligroso en la seguridad de nuestra red informática. En base, dispone de una serie de medidas que le diferencia del resto, tales como mejores auditorías, monitorización del sistema, control de accesos al mismo (conexiones de la red interna, conexiones de la red externa ...). Este sistema debe haber sufrido un proceso de testing para catalogar posibles fallos no solo en seguridad, sino también en el propio software que utiliza.

Normalmente se suele permitir el paso del tráfico de red autorizado a través del BH debido a que este nos detallara todo en todo momento, y además conociendo correctamente su funcionamiento, podremos asegurar en un gran margen que el sistema está preparado para evitar posibles ataques o accesos no deseados a nuestra red interna.

Un Bh deberá incluir, entre otros, una serie de normas de seguridad. En principio, el sistema no deberá contener cuentas de acceso a usuarios. En el caso de GNU/LiNEX, solo deberá mantenerse aquellas derivadas a daemons y la del administrador. Se recomienda eliminar el demonio SysKLogd, e instalar otro de los muchos disponibles en web sites como <http://www.freshmeat.net>, que nos den un mayor rango de seguridad inherente, de forma que ante posibles ataques a nuestro sistema, los ficheros, de registro, etc corran menor peligro. Un buen ejemplo de ello, sería la codificación y encriptación de los mismos. De cualquier modo, es recomendado leer previamente toda documentación y, como no, la parte relativa a registros de este documento.

Como ya bien se especifica en la parte correspondiente en este documento, el envío de los logs a otra máquina de nuestra red nos puede ser de gran utilidad. Con Syslogd, es bastante sencillo, simplemente indicando en la configuración del demonio que registros y políticas se han de enviar a la máquina

mediante el parametro "z a continuacion la IP de la Maquina en cuestion. Un ejemplo seria:

Deberemos controlar todo lo relativo a enrutado desde el BH. Evitaremos situaciones como encaminamientos no autorizados. También deberemos desechar todos aquellos servicios de red como HTTPd, NNTPd, etc. excepto aquellos que nos permitan a nosotros, administradores, el control remoto de la maquina. Estos podrian ser el telnetd y el ftpd. Deberemos cambiar los puertos de acceso a los mismos, o buscar formas de acceso a la maquina mediante una sola IP de acceso (Revisar Hosts.deny y Hosts.allow). Los métodos personales míos de administracion prefiero mantenerlos offside ;-). Simplemente es pensar en como actuaría una persona ajena al encontrarse con un sistema de este tipo. SSH nos ayudará mucho en esta tarea.

7. Firewalls (Cortafuegos - FW)

7.1. ¿Por qué es necesaria la seguridad en las redes?

Actualmente, Internet se compone de decenas de miles de redes conectadas entre sí. La seguridad en las redes resulta esencial en este entorno, ya que toda red organizada es accesible desde cualquier computadora de la red y potencialmente es vulnerable a las amenazas de personas que no necesitan acceso físico a ella. En un sondeo reciente dirigido por el Computer Security Institute (CSI), el 70 % de las organizaciones encuestadas declararon que las defensas de sus redes habían sido atacadas y el 60 % afirmaba que los incidentes procedían desde dentro de las propias empresas.

Aunque sea difícil calcular el número de empresas que tiene problemas de seguridad relacionados con Internet y las pérdidas financieras debidas a tales problemas, queda claro que los problemas existen. Definición del diseño de redes seguras Una internetwork se compone de muchas redes que están conectadas entre sí. Cuando se accede a información en un entorno de internetwork, hay que crear áreas seguras. El dispositivo que separa cada una de estas áreas se denomina firewall. Aunque un firewall suele separar una red privada de una red pública, esto no siempre es así. Lo normal es usar un firewall para separar los segmentos de una red privada.

NOTA: Un firewall, tal y como lo define el Dictionary of Internetworking Terms and Acronyms (Diccionario para términos y acrónimos de Internetworking), es un router o servidor de acceso, o varios routers o servidores de acceso, que actúan como búfer entre las redes públicas y una red privada.

Un router firewall utiliza listas de acceso y otros métodos para garantizar la seguridad de la red privada . Un firewall suele tener un mínimo de tres

interfaces, aunque las primeras implementaciones sólo incluían dos.

Todavía resulta habitual instalar firewalls de dos interfaces.

Cuando se usa un firewall con tres interfaces, se crea un mínimo de tres redes. Las tres redes que crea el firewall se describen de este modo:

Interior El interior es el área de confianza de la internetwork. Los dispositivos que están en el interior forman la red privada de la organización. Estos dispositivos comparten unas directivas de seguridad comunes con respecto a la red exterior (Internet). Sin embargo, resulta muy habitual que un firewall segmente el entorno de confianza. Si un departamento, como Recursos Humanos, tiene que ser protegido del resto de usuarios de confianza, se puede utilizar un firewall.

Exterior El exterior es el área de no confianza de la internetwork. El firewall protege los dispositivos del interior y de la DMZ (Zona desmilitarizada) de los dispositivos del exterior. Para ofrecer servicios, ya sean Web, FTP público u otros, las empresas suelen permitir el acceso a la DMZ desde el exterior. En ocasiones, es necesario configurar un firewall para el acceso selectivo desde el exterior hasta los hosts y servicios de la DMZ. Si es inevitable, es posible configurar un firewall para permitir el acceso desde un dispositivo del exterior hasta un dispositivo de confianza del interior, siendo la razón principal para esto, el que no todas las empresas quieren invertir en tener varios servidores. Esto es mucho más arriesgado que permitir el acceso, desde el exterior hasta la DMZ aislada.

DMZ (Zona desmilitarizada) La DMZ es una red aislada, a la que pueden acceder los usuarios del exterior. Es necesario configurar el firewall para permitir el acceso desde el exterior o el interior hasta la DMZ. La creación de una DMZ posibilita que una empresa ponga la información y los servicios a disposición de los usuarios del exterior dentro de un entorno seguro y controlado. Esto permite el acceso a los usuarios del exterior, sin permitir el acceso al interior. Los hosts o servidores que residen en la DMZ suelen denominarse hosts bastión. En este caso, un host bastión es un host que está actualizado con respecto a su sistema operativo y las modificaciones experimentadas por este último. El hecho de que esté actualizado generalmente lo hará menos vulnerable a los ataques, ya que el fabricante habrá establecido o "parcheado" todos los defectos conocidos. El host bastión es un host que sólo ejecuta los servicios necesarios para realizar sus tareas de aplicación. Los servicios innecesarios (y a veces más vulnerables) son desactivados o eliminados.

En la figura 1 de la página 8, muestra una red general.

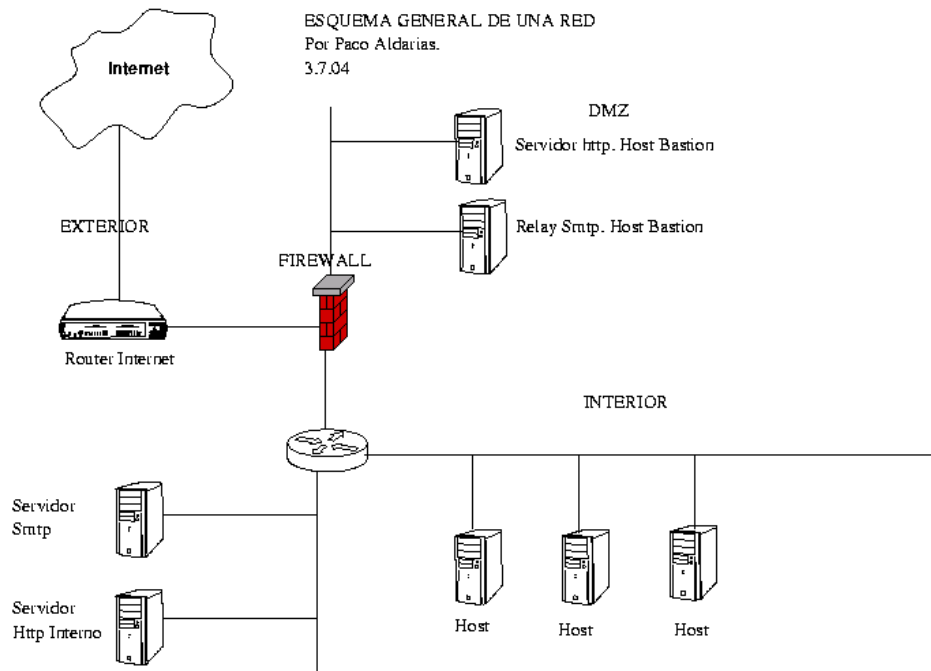


Figura 1: Red General

El cometido básico de un firewall consiste en llevar a cabo las siguientes funciones:

- No permitir acceso desde el exterior hasta el interior
- Permitir un acceso limitado desde el exterior hasta la DMZ
- Permitir todo el acceso desde el interior hasta el exterior
- Permitir un acceso limitado desde el interior hasta la DMZ

En muchos diseños de red existen excepciones a algunas de estas reglas (o a todas ellas). Por ejemplo, podría ser necesario permitir los mensajes SMTP desde el exterior hasta el interior. Si un entorno no tiene un servidor SMTP en la DMZ o carece de un host de relay de correo SMTP en la DMZ, sería necesario permitir acceder al servidor SMTP que reside físicamente en el interior. El hecho de permitir este tráfico incrementa considerablemente el riesgo en la red interna. Otra excepción podría ser que no se permitiera a la totalidad del tráfico pasar del interior al exterior. Potencialmente, una dirección IP, una subred, o la totalidad de la red del interior, podrían estar limitadas a la hora de usar una determinada aplicación (puerto). Otra restricción podría ser el filtrado de los URL.

7.2. Seguridad

En principio, el propósito genérico de un firewall es controlar y auditar los accesos a un servicio determinado. Su función es la de multiplexar los accesos a una red interna desde Internet; es una puerta entre una IntraNET y la InterNET. La vigilancia que otorga el firewall requiere unas normativas de seguridad impuestas por el propio administrador.

Una política bastante correcta y fiable, es la de hacer pasar siempre por el firewall el tráfico que se necesite originar entre Internet y viceversa, de forma que se audite y controle todo lo que accede a la red y/o sale de la misma. Esto nos permitiría sistemas de autenticación segura, detección de posibles intentos de acceso no autorizados, etc etc.

Una falacia es la idea que establece que un Firewall es inatacable. Esto es totalmente falso, existen métodos, con mayor o menor riesgo para el sistema, pero existen. Un ejemplo sería dar la oportunidad al atacante de reestablecer las políticas de filtrado y selección. Esto crearía un gran agujero de seguridad que posiblemente le permita acceder a cualquier host de la red interna que desee.

El firewall debe ser capaz de evaluar los posibles daños ofertados por un ataque e informar al administrador de ello. Tengamos en cuenta el bug propuesto antes. Una eliminación de políticas de auditoría podría darnos muchos dolores de cabeza.

Bajo GNU/LINUX, tenemos a nuestra disposición numerosos programas capaces de convertir nuestro sistema en un potente firewall. El ejemplo más conocido quizás sea iptables.

8. Diseño de redes

8.1. Diseño de red básico. Sin Cortafuegos

Suponemos que estamos en el caso básico que están los centros de enseñanza secundaria cuando llevan Internet al centro.

Un router ADSL en multipuesto:

- la IP externa la tiene el router
- tiene la IP local 192.168.0.1 (será la puerta de enlace de los PCs de la red)
- DHCP dinámico 192.168.0.1 - 192.168.0.254
- máscara 255.255.255.0

- Tiene todos los puertos cerrados.

Con lo que se crea una red local de tipo C privada, con una única subred 192.168.0.0 El número máximo de máquinas es: $2^8 - 2 = 254$ pcs.
En el figura 2 de la página 17, muestra la topología.

Ventajas:

1. Fácil de instalar y matener. Sólo hay q activar el dhcp en los pcs.
2. Limite de 254 pcs.

Inconvenientes:

1. Se podria instalar un proxy, pero abria que añadirlo en el navegador su ip.
2. Red poco segura, todas las máquinas tienen acceso a toda la red.
3. No se pueden poner servidores web al exterior, por tener el acceso al router bloqueado.
4. Tiene un gran tráfico de paquetes de broadcast.

8.2. Diseño básico de un red C/B

Una solución intermedia, sería montar un router linux, que cambie las ips, anulando la red 192.168.0.0/255.255.255.0, y crear nosotros subredes de clase B, 172.16.0.0/255.255.255.0 a a partir del firewall.

Es decir, tendremos una clase C (192.168.0.0), solo hasta el firewall, y el resto de la red privada, será un clase B (172.16.0.0). La clase B, permitirá aislar y crear subredes.

Ventajas:

1. Fácil de instalar y matener. Sólo hay q activar el dhcp en los pcs.
2. Se bloquea el acceso de las aulas a otros pcs
3. Se podria instalar un proxy transparente.
4. Red segura, ya que todas las máquinas no tienen acceso a toda la red.
5. Tiene un gran tráfico de paquetes de broadcast más bajo.

Inconvenientes:

1. No se pueden poner servidores web al exterior, por tener el acceso al router bloqueado.
2. Hay que añadir un firewall.

En el figura 3 de la página 18, muestra la topología.

8.3. Diseño de red clase B con DMZ y firewall: Red Segura

Suponemos que queremos varias subredes por aulas y departamentos. Queremos que los pcs de las aulas de vean entre ellos (esto deberá contemplarse en la cuadro de encaminamientos).

Usaremos la red de tipo B privada:

172.16.0.0 / 255.255.255.0 o lo que es lo mismo 172.16.0.0 /24

Esto significa que tenemos, esta máscara:

11111111. 11111111.11111111.00000000

Es decir, podemos tener:

- Subredes : 2 elevado a 8 (11111111 del tercer número de la máscara) =256
- Hosts: 2 elevado a 8 - 2 : (00000000 del cuarto número de la máscara) =256-2=254

Subredes para 172.16.0.0/255.255.255.0

| Subred | De | A | Mascara |
|--------|--------------|----------------|---------------|
| 1 | 172.16.1.0 | 172.16.1.254 | 255.255.255.0 |
| 2 | 172.16.2.0 | 172.16.2.254 | 255.255.255.0 |
| 3 | 172.16.3.0 | 172.16.3.254 | 255.255.255.0 |
| ... | ... | ... | ... |
| 254 | 172.16.254.0 | 172.16.254.254 | 255.255.255.0 |

No se toman en cuenta la red 172.16.0.0 por representar la red, ni la 172.16.255.0, por representar el broadcasting.

En el figura 4 de la página 19, muestra la topología.

- Las ips 172.17.16.1, 172.17.16.100 son ips locales

- La red 172.17.2.0/24, se encuentra accesible por la ip del router del aula 2, 172.17.16.2.100
- Para el resto de redes, ir a la 172.17.16.100.100

Tabla de rutas (encaminamientos) del router del aula 1:

| Destination | Gateway | Genmask | Flags | Metric | Ref | Use | Iface |
|---------------|-------------------|---------------|-------|--------|-----|-----|-------|
| 172.17.16.1 | 0.0.0.0 | 255.255.255.0 | U | 0 | 0 | 0 | eth1 |
| 172.17.16.100 | 0.0.0.0 | 255.255.255.0 | U | 0 | 0 | 0 | eth0 |
| 172.17.2.0 | 172.17.16.2.100 | 255.255.255.0 | U | 0 | 1 | 0 | eth0 |
| 0.0.0.0 | 172.17.16.100.100 | 255.255.255.0 | U | 0 | 1 | 0 | eth0 |

9. Dirección de Broadcast

Se utiliza para emitir paquetes que deben recibir todas las máquinas de la subred.

Así pues, si el número de host de la subred se obtiene mediante el último octeto de la dirección IP (o sea, la máscara es 255.255.255.0), su dirección de broadcast será su dirección de red y haciendo un OR con 0.0.0.255. Pero esto sólo es cierto cuando no hay subnetting.

Tablas de broadcast:

| Dirección de Red | Mascara | Dirección Broadcast |
|------------------|-----------------|-------------------------------|
| 192.168.0.0/24 | 255.255.255.0 | 192.168.0.255 |
| 192.168.0.0/25 | 255.255.255.128 | 192.168.0.128 y 192.168.0.255 |
| 172.16.0.0/16 | 255.255.0.0 | 172.16.0.255 |
| 172.16.0.0/24 | 255.255.255.0 | 172.16.255.255 |

9.1. Ejemplo

La dirección de broadcast siempre es la última IP de la red que tengas definida. Por eso en el caso de una red de 4 ip's (mascara 255.255.255.252) solo tenemos 2 ip's para equipos.

- Red: 192.168.0.0/30
- Mascara: 255.255.255.252 (11111111.11111111.11111111.11111100)
- Subredes: 1

- Máquinas: 2 elevado a 2 (2 elevado al numero de ceros) - 2 = 4-2=2
- Ips Validas: 192.168.0.1, 192.168.0.2
- Broadcast: 192.168.0.3

9.2. Ejemplo

Este es un caso de red segmentada.

- Red: 192.168.0.0/25
- Mascara: 255.255.255.128 (11111111.11111111.11111111.10000000)
- Subredes: 2 elevado a 1 (2 elevado al número de unos del último octeto) = 2
- Máquinas: 2 elevado a 7 (2 elevado al numero de ceros) - 2 = 128-2=126
- Ips Validas:
Red 1: 192.168.0.1 a 192.168.0.127 Broadcast: 192.168.0.128
Red 2: 192.168.0.129 a 192.168.0.254 Broadcast: 192.168.0.255

10. Saber en que red se encuentra un ip

Para saber si dos máquinas son visibles entre ellas, estas debe estar en la misma red.

La forma de comprobar q están en la misma red, es haciendo un and BIT A BIT entre la ip y su máscara, y comprobar q da la misma red.

10.1. Ejemplo

Red: 192.168.0.0

Máscara: 255.255.255.0

Subredes= 2 elevado a 0 = 1

Ip1: 192.168.0.1 AND 255.255.255.0 = Red 192.168.0.0

Ip2: 192.168.0.2 AND 255.255.255.0 = Red 192.168.0.0

10.2. Ejemplo

Red: 192.168.0.0

Máscara: 255.255.255.128 (11111111.11111111.11111111.10000000)

Subredes = 2 elevado a 1 = 2

Ip1: 192.168.0.1 AND 255.255.255.128 = Red 192.168.0.0

Ip2: 192.168.0.2 AND 255.255.255.128 = Red 192.168.0.0

Ip3: 192.168.0.129 (x.x.x.10000001) AND 255.255.255.128 = Red 192.168.0.128

Ip4: 192.168.0.130(x.x.x.10000010) AND 255.255.255.128 = Red 192.168.0.128

11. Segmentar una clase C en subredes

Podemos tener una red de tipo C, 192.168.0.0, y podemos crear varias subredes a través de la máscara.

Podemos ver las subredes 192.168.0.0 según su máscara:

| Subredes | Rango | Subredes |
|----------------|-----------------|----------|
| 192.168.0.0/24 | 255.255.255.0 | 1 |
| 192.168.0.0/25 | 255.255.255.128 | 2 |
| 192.168.0.0/26 | 255.255.255.192 | 4 |
| 192.168.0.0/27 | 255.255.255.224 | 8 |

Veamos detalladamente las subredes.

11.1. Dirección de Red: 192.168.0.0/24

Subredes: 1

Hosts por subred: 2 elevado a 8 -2 = 253

Mascara: 255.255.255.0

| Subred | Rango | Broadcast |
|--------|-----------------|---------------|
| 1 | 192.168.0.1-254 | 192.168.0.255 |

11.2. Dirección de Red: 192.168.0.0/25

Subredes: 2

Hosts por subred: 2 elevado a 7 -2 = 126

Máscara: 255.255.255.128

| Subred | Rango | Broadcast |
|--------|-------------------|---------------|
| 1 | 192.168.0.1-126 | 192.168.0.127 |
| 2 | 192.168.0.128-254 | 192.168.0.254 |

11.3. Dirección de Red: 192.168.0.0/26

Subredes: 4

Hosts por subred: 2 elevado a 6 -2 = 62

Máscara: 255.255.255.192

| Subred | Rango | Broadcast |
|--------|-------------------|---------------|
| 1 | 192.168.0.1-62 | 192.168.0.63 |
| 2 | 192.168.0.64-126 | 192.168.0.127 |
| 3 | 192.168.0.128-190 | 192.168.0.191 |
| 4 | 192.168.0.192-254 | 192.168.0.255 |

11.4. Dirección de Red: 192.168.0.0/27

Subredes: 8

Hosts por subred: 2 elevado a 5 -2 = 30

Máscara: 255.255.255.224

| Subred | Rango | Broadcast |
|--------|-------------------|---------------|
| 1 | 192.168.0.1-30 | 192.168.0.31 |
| 2 | 192.168.0.32-62 | 192.168.0.63 |
| 3 | 192.168.0.64-94 | 192.168.0.95 |
| 4 | 192.168.0.96-126 | 192.168.0.127 |
| 5 | 192.168.0.128-158 | 192.168.0.159 |
| 6 | 192.168.0.160-190 | 192.168.0.191 |
| 7 | 192.168.0.192-222 | 192.168.0.223 |
| 8 | 192.168.0.224-254 | 192.168.0.255 |

12. Bibliografía

1. Subredes. http://www.htmlweb.net/redes/subredes/subredes_1.html
2. Valores de las máscaras de subred: subneting <http://www.consultascna.com/informacion/tcpip/subneti/valores.php>
3. Guia de Administración de redes linux. <http://es.tldp.org/Manuales-LuCAS/GARL2/garl-2.0.pdf>
4. Seguridad en Redes http://members.fortunecity.es/mardedudascom/Informatica/_inf_redes/seguridadredes.htm
5. Seguridad en redes unix. <http://es.tldp.org/Manuales-LuCAS/doc-unixsec/unixsec-html/>

6. Firewall. <http://www.redes.upv.es/~mperez/rc2/trabajos/FireWallstxt.pdf>

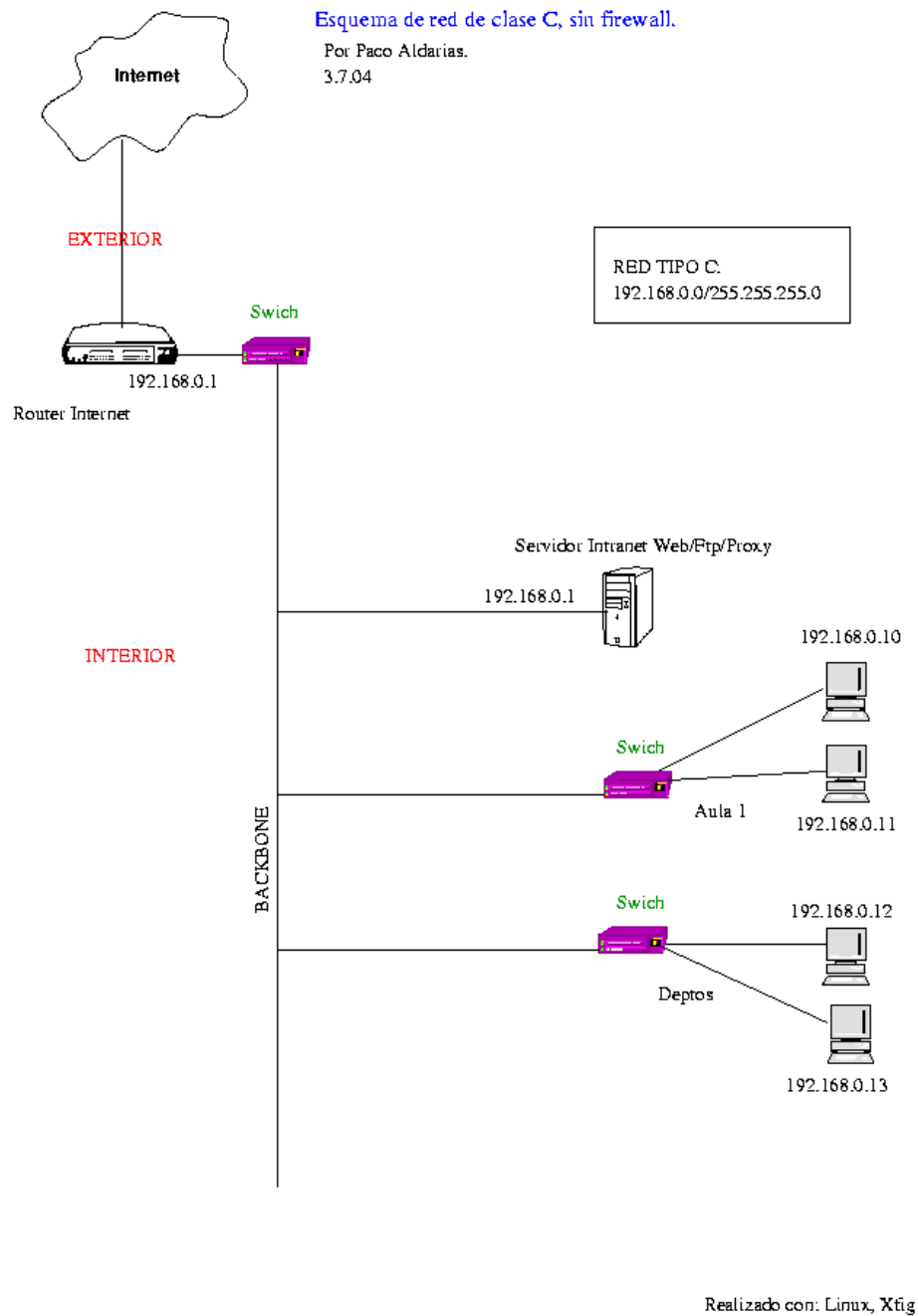


Figura 2: Ejemplo red de clase C

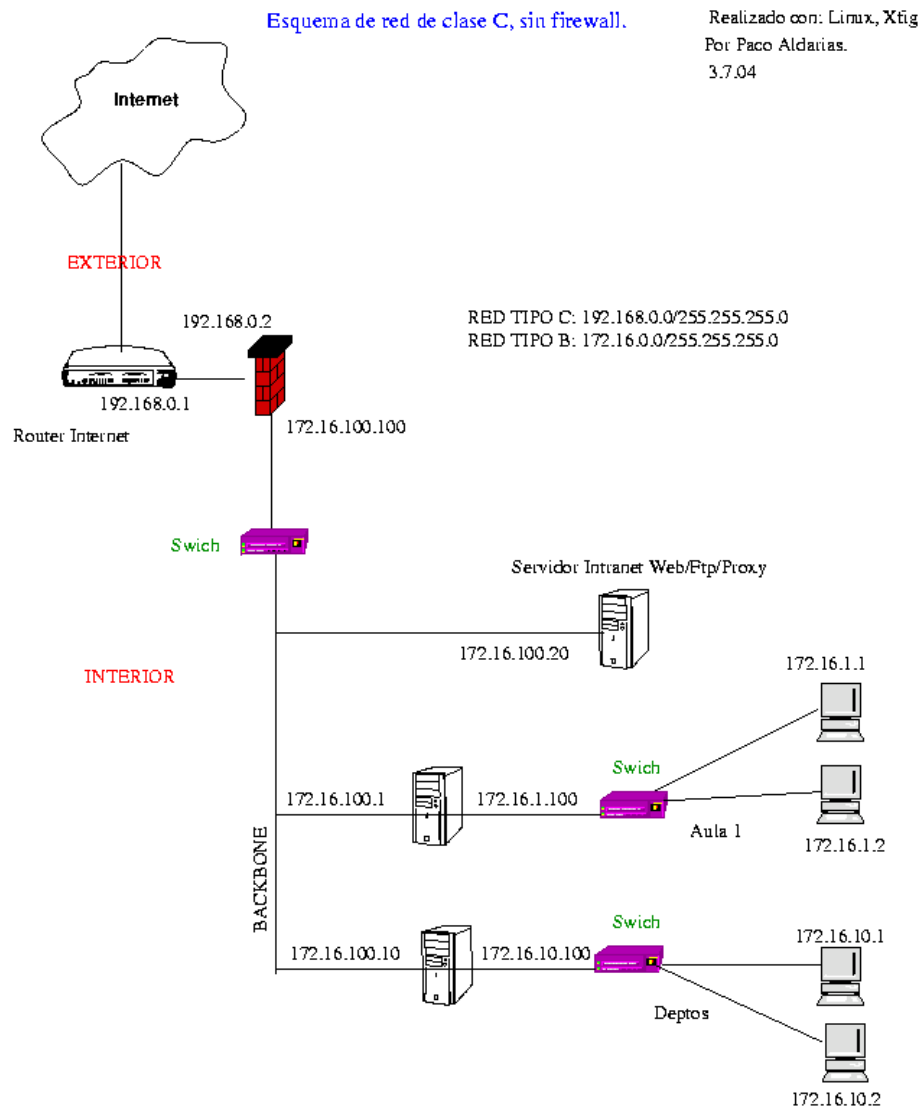
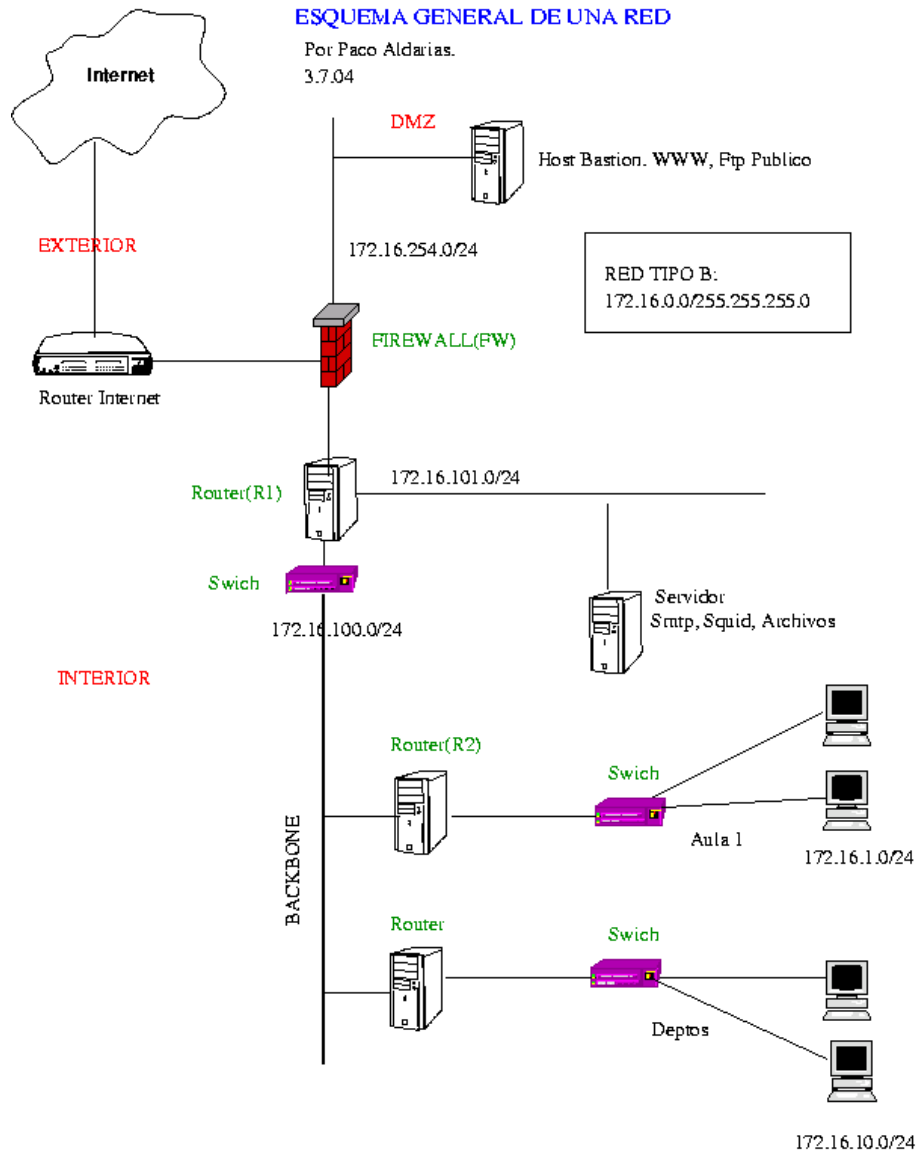


Figura 3: Ejemplo red de clase C/B



Realizado con: Linux, Xfig

Figura 4: Ejemplo red con DMZ

Índice alfabético

bastion host, 6

broadcast, 13

cortafuegos, 7

firewall, 7

red privada, 3

redes, 2

router, 5

seguridad redes, 10

subneting, 3