# Linux Networking-concepts HOWTO

Rusty Russell
Ricardo Javier Cárdenes Medina *a1402@dis.ulpgc.es*
v1.0.1 Lunes 1 de Mayo 16:19:12 CST 2000, traducción del 27 de Junio de 2000

Este documento describe qué es una red (tal como la Internet), y los fundamentos de su funcionamiento.

## Índice



## 1. Introducción

Bienvenido, gentil lector.

He escrito varios documentos COMO sobre redes en el pasado, y se me ocurrió que hay montón de jerga en cada uno. Tenía tres opciones: las otras dos eran ignorar el problema y explicar los términos en cada uno. Ninguna era atractiva.

El **detalle** del software Libre es que usted debería tener libertad para explorar y juguetear con los sistemas de software que usa. Creo que permitir a la gente experimentar esta libertad es una noble meta; no sólo la gente se siente atraída por el reto (como reconstruir el motor de un coche), sino que la naturaleza de la moderna Internet y del software Libre le permiten compartir la experiencia con millones de personas.

Pero tiene que empezar en algún lugar, así que aquí estamos.

## 2. ¿Qué es una «red de ordenadores»?

Una red de ordenadores es un conjunto de material preparado para que los nodos puedan comunicarse uno con otro (con «nodos» me estoy refiriendo a ordenadores, impresoras, máquinas de Coca-Cola y cualquier otra cosa que quiera). No importa realmente **cómo** están conectados: pueden usar cables de fibra óptica o palomas mensajeras. Obviamente, algunas elecciones son mejores que otras (especialmente si tiene gato).

Normalmente, si se va a limitar a conectar dos ordenadores, no se le llama red; realmente, necesitará tres o más para tener una red. Pasa como con la palabra «grupo»: dos personas son sólo una pareja, pero tres ya pueden ser «grupo». Además, las redes suelen estar conectadas unas con otras, para hacer redes más grandes. Cada pequeña red (normalmente llamadas «subredes») puede ser parte de una red más grande.

La verdadera conexión entre dos ordenadores se llama a menudo «enlace de red» (network link). Si hay un cable que va de la parte de atrás de su ordenador hasta las otras máquinas, ese es su enlace de red.

Hay cuatro cosas que solemos tener en cuenta cuando hablamos de redes de ordenadores:

**Tamaño**

Si va a conectar los cuatro ordenadores de casa, tiene lo que llamamos LAN (Local Area Network - Red de Area Local). Si todo está a una distancia razonable que se pueda cubrir caminando, se le suele llamar LAN, da igual cuántas máquinas estén conectadas, y de qué manera esté hecha la red.

El otro extremo del espectro es una WAN (Wide Area Network - Red de Area Amplia). Si tiene un ordenador en Lahore, Pakistán, otro en Birmingham, Reino Unido y otro en Santiago, Chile, e intenta conectarlos, es una WAM.

**Topología: La Forma**

Dibuje un mapa de la red: las líneas son los 2 (enlaces de red), y cada nodo es un punto. Quizá cada línea lleve a un nodo central, como una gran estrella, lo que quiere decir que todo el mundo se comunica a través de un punto (una «topología en estrella»):

```
    o   o   o
     \_ | _/
       \|/
 o-----o-----o
      _/|\_
     /  |  \
    o   o   o
```

Quizá todo el mundo habla en una línea, como aquí:

```
    o------o------o-------o--------o
    |                              |
    |                              |
```

```
|                             o
|                             |
o                             |
                              o
```

O puede ser que tenga tres subredes conectadas a través de un nodo:

```
            o
o           |  o--o--o
|           |  |
o--o--o--o--o  o
       \       |
        o------o
       /       |
o--o--o--o--o  o
|           |  |
o           |  o--o
            o
```

Verá muchas topologías como estas en la vida real, y mucho más complejas.

**Aspecto físico: De qué está hecha**

La segunda cosa a tener en cuenta es con qué ha construido la red. La más barata es la «sneakernet» (red a zapato), donde gente mal vestida lleva disquetes de un ordenador a otro. La sneakernet es casi siempre una 2 (LAN). Los disquetes cuestan menos de $1, y se puede comprar un sólido par de sneakers («sneaker» es una manera de llamar a determinado tipo de calzado, como el deportivo) por unos $20.

El dispositivo más común usado en casa para conectar a redes mayores se llama «módem» (MODulador/DEModulador), que convierte una línea de teléfono normal en un enlace de red. Transforma la información del ordenador en sonidos, y escucha los sonidos que vienen del otro lado para convertirlos de nuevo en información para el ordenador. Como puede imaginar, esto no es muy eficiente, y las líneas de teléfono no fueron diseñadas para este uso, pero es popular porque las líneas de teléfono son comunes y baratas: se vende módems por menos de $50 y una línea de teléfono suele costar un par de cientos de dólares al año.

La manera más común de conectar máquinas en una LAN es usar Ethernet. Ethernet vienen en las siguientes modalidades principales (listadas de más vieja a más nueva): Thinwire/Coax/10base2, UTP (Unshielded Twisted Pair/10baseT y UTP/100baseT. También se está empezando a difundir Gigabit ethernet (el nombre 1000baseT comenzaba a ser tonto). El cable 10base2 suele ser coaxial negro, con enlaces en forma de T para conectarlos a las cosas: todo el mundo está conectado en una gran fila, con «terminadores» especiales en ambos extremos. UTP suele ser cable azul[1] con conectores transparentes al estilo de los teléfonos que se enchufan: cada cable conecta un nodo a un «hub» (un concentrador) central. El cable costará un par de dólares el metro, y las tarjetas 10baseT/10base2 (muchas tienen ambos conectores) están sobre los $30. Las tarjetas 100baseT, que también pueden trabajar con 10baseT, son diez veces más rápidas, y andan por los $100.

En el otro lado tenemos la Fibra; un delgado filamento de cristal, encerrado en una capa protectora que se puede tender entre continentes. La fibra cuesta millares (de dólares).

Solemos llamar a cada conexión a un nodo «interfaz de red», o «interfaz» para abreviar. Linux les da nombres como «eth0» para la primera interfaz ethernet, y «fddi0» para la primera interfaz de fibra. La orden `/sbin/ifconfig` las enumera.

[1](N. del T.: en España lo suelo ver blanco o gris)

**Protocolo: Qué se habla**

El último detalle a tener en cuenta es el lenguaje que van a hablar los ordenadores. Cuando dos 2 (módems) están comunicándose por una línea de teléfono, se tienen que poner de acuerdo en el significado de cada sonido, porque si no, no funcionará. Esta convención se denomina «protocolo». Según la gente descubre nuevas formas de codificiar lo que dicen las computadores en sonidos más pequeños, se inventan nuevos protocolos, y la mayoría de los módems probarán con varios hasta que encuentren unos que el otro extremo entienda.

Otro ejemplo es la red 2 (100baseT) que mencionamos antes: usa los mismos 2 (enlaces de red) físicos (2 (UTP)) que 2 (10baseT), pero habla diez veces más rápido.

Estos dos protocolos son lo que llamamos protocolos de «nivel de enlace»; la manera en que se controla la información entre dos enlaces individuales de red, o «un salto». La palabra «protocolo» también se refiere a otras convenciones, como veremos más adelante.

# 3. ¿Qué es la «Internet»?

Internet es una 2 (WAN) que abarca todo el globo: es una de las más grandes redes de ordenadores existentes. La expresión «internetiworking» se refiere a conectar redes separadas para construir una más grande, de manera que «La Internet» es la conexión de un gran montón de subredes.

De manera que ahora miraremos a la lista anterior y nos preguntaremos: ¿cuál es el tamaño de Internet, sus detalles físicos y protocolos?

El tamaño ya lo hemos establecido: es global.

Los detalles físicos, sin embargo, son variados: cada pequeña subred se conecta de forma diferente, con un aspecto y naturaleza física diferente. Los intentos de hacer un mapa útil de Internet han acabado de forma general en un abyecto fracaso.

Los protocolos que se hablan entre cada enlace también son diferentes a menudo: todos los 2 (protocolos de nivel de enlace) que nombramos antes, y muchos más.

## 3.1. ¿Cómo funciona La Internet?

Entonces se nos presenta la pregunta: ¿cómo puede hablar cada nodo de Internet con otros, si todos utilizan diferentes protocolos de nivel de enlace?

La respuesta es muy sencilla: necesitamos otro protocolo que controla cómo fluyen las cosas a través de la red. El protocolo de nivel de enlace describe cómo llegar de un nodo a otro si están conectados de forma directa: el «protocolo de red» nos dice cómo llegar de un punto de la red a otro, yendo a través de otros enlaces si fuera necesario.

Para la Internet, el protocolo de red es el *Internet Protocol* (versión 4), o «IP». No es el único que hay (tenemos otros como el Appletalk de Apple, IPX de Novell, DECNet de Digital y el NetBEUI de Microsoft) pero es el más ampliamente adoptado. Hay una nueva versión de IP denominada IPv6, pero aún no es tan común.

Para enviar un mensaje de un lado del planeta a otro, su ordenador escribe un poco de *Internet Protocol*, lo envía por el módem, que usa algún protocolo de nivel de enlace de módems para enviarlo al otro módem al que está llamando, que posiblemente esté enchufado a un servidor terminal (básicamente una gran caja de módems), que lo envía a otro nodo dentro de la red del ISP (Internet Service Provider - Proveedor de Servicios de Internet), que lo envía normalmente a otro nodo mayor, que lo manda al siguiente... y así en adelante. Un nodo que conecta dos o más redes se llama «router»[2]: tendrá una 2 (interfaz) para cada red.

Llamamos a este conjunto de protocolos una «pila de protocolos», que se suele dibujar de esta manera:

```
  [ Aplicación: Controla Porno ]        [ Capa de aplicación: Sirve Porno ]
                |                                       ^
                v                                       |
[ TCP: Controla la Retransmisión ]      [ TCP: Controla la Retransmisión ]
                |                                       ^
                v                                       |
[ IP: Controla el Encaminamiento ]      [ IP: Controla el Encaminamiento ]
                |                                       ^
                v                                       |
[ Enlace: Controla un solo Salto ]      [ Enlace: Controla un solo Salto ]
                |                                       |
                +---------------------------------------+
```

De manera que en el diagrama vemos un Netscape (la Aplicación de la izquiereda) obteniendo una página web de un servidor web (la Aplicación de la derecha). Para hacerlo utiliza el «Transmission Control Protocol» o «TCP»: alrededor del 90 % del tráfico de la Internet hoy día es TCP, y se emplea para Web y correo electrónico.

De manera que el Netscape hace una consulta mediante una conexión TCP al servidor web remoto: esto lo controla la capa TCP, que se la pasa a la capa IP, que se hace cargo de la dirección que tiene que seguir, y la pasa a la capa de enlace apropiada, que la transmite al otro extremo del enlace.

En el otro extremo, la capa de enlace la pasa a la capa IP, que comprueba que vaya destinado a esa máquina (si no, puede enviarla a otra capa de enlace diferente para que pase al siguiente nodo), se la entrega a la capa TCP que, por último, se la manda al servidor.

De manera que tenemos lo siguiente:

1. La aplicación (Netscape, o el servidor web en el otro extremo) decide con quién quiere hablar, (y qué le quiere enviar).

2. La capa TCP envía paquetes especiales para iniciar la conversación con el otro extremo, y entonces empaqueta los datos en «paquetes» TCP: un paquete es sólo un término para describir un grupo de datos que pasan a través de la red. La capa TCP delega este paquete en la capa IP: estará mandándoselo a la capa IP hasta que la capa TCP del otro extremo responda diciendo que lo ha recibido. Esto se llama «retransmisión», y conlleva un montón de reglas complejas que deciden cuándo retransmitir, cuánto esperar, etc. También le da a cada paquete un número, lo que significa que el otro extremo podrá ponerlos en el orden correcto.

3. La capa IP comprueba el destino del paquete, y averigua el siguiente nodo al que mandárselo. Este sencillo acto se llama «encaminamiento» (*routing*), y va desde lo realmente sencillo (si sólo tiene un módem, y no hay otra interfaz de red, todos los paquetes saldrán por ahí) a lo extremadamente complejo (si tiene 15 grandes redes conectadas directamente con usted).

[2] N. del T.: mantengo el nombre router, ya que es el más común entre los propios hispanohablantes. También he escuchado «enrutador» o «encaminador»

# 4. Esa cosa llamada IP

De manera que el papel de la capa IP es averiguar cómo «encaminar» paquetes a su destino final. Para hacerlo posible, cada interfaz en la red necesita una «dirección IP». Una dirección IP consiste en cuatro números separados por puntos, como «167.216.245.249». Cada número estará entre cero y 255.

Las interfaces de la misma red tienden a tener direcciones IP vecinas. Por ejemplo «167.216.245.250» estará cerca de la máquina con la dirección IP «167.216.245.249». Recuerde también que un *router* es un nodo con interfaces en una o más redes, de manera que el *router* tendrá una dirección IP por cada interfaz.

Por tanto la capa IP del Núcleo de Linux tiene una tabla con diferentes «rutas», que describe cómo llegar a varios grupos de direcciones IP. La más sencilla de ellas se llama «ruta por defecto»: si la capa IP no sabe qué hacer, es ahí a donde envía los paquetes. Puede ver una lista de las rutas usando `/sbin/route`.

Las rutas pueden indicar tanto un enlace, como un nodo particular que está conectado a otra red. Por ejemplo, cuando llamamos a un ISP, la ruta por defecto indicará el enlace del módem, porque por ahí se llega al mundo entero.

```
Módem de             Módem  ~~~~~~
 Rusty             del ISP {      }
     o------------------o { La Red }
                           {      }
                            ~~~~~~
```

Pero si tenemos una máquina en nuestra red que conecta con el mundo exterior, es un poco más complejo. En el siguiente diagrama, mi máquina puede comunicarse directamente con las de Tridge y Paul, y con el cortafuegos («firewall»), pero necesita saber que los paquetes dirigidos al resto del mundo han de pasar por el cortafuegos, que los reenviará. Esto significa que hay dos rutas: una dice «si está en mi red, sencillamente suéltalo ahí», y luego la ruta por defecto que dice «en cualquier otro caso, envía lo al cortafuegos».

```
                       o  La estación de trabajo
                       |    de Tridge         ~~~~~~
La estación de trabajo |                     {      }
 de Rusty     o--------+-----------------o--{ La Red }
                       |          ortafuegos {      }
                       |                      ~~~~~~
                       o  La estación de trabajo
                            de Paul
```

## 4.1. Grupos de direcciones IP: Máscaras de Red

Hay un último detalle: hay una notación estándar para grupos de direcciones IP, a veces llamada «dirección de red». Igual que un número de teléfono puede ser separado en prefijo de área y el resto, podemos separar una dirección IP en el prefijo de red y el resto.

La gente solía hablar sobre «la red 1.2.3», refiriéndose a todas las 256 direcciones de la 1.2.3.0 a la 1.2.3.255. O si no les bastaba con esa red, se referían a «la red 1.2», que implica todas las direcciones desde la 1.2.0.0 a la 1.2.255.255.

Normalmente no escribimos «1.2.0.0 - 1.2.255.255». En su lugar, lo abreviamos como «1.2.0.0/16». Esta extraña notación «/16» (se llama «netmask» - máscara de red), necesita algo de explicación.

Cada número entre los puntos en una dirección IP se compone de 8 dígitos binarios (00000000 a11111111): los escribimos en la forma decimal para hacerlos más legibles a los humanos. El «/16» significa que los primeros 16 dígitos binarios constituyen la dirección d red, o en otras palabras, «1.2.» es la parte de la red (recuerde: cada dígito representa 8 binarios). Esto significa que cualquier dirección IP que comience por «1.2» es parte de la red: «1.2.3.4» y «1.2.3.50» lo son, y «1.3.1.1» no.

Para hacer la vida más fácil, solemos usar redes que acaban en «/8», «/16» y «/24». Por ejemplo, «10.0.0.0/8» es una gran red que contiene las direcciones desde la 10.0.0.0 a la 10.255.255.255 (¡alrededor de 24 millones de direcciones!). 10.0.0.0/16 es más pequeña, y sólo contiene las direcciones IP de la 10.0.0.0 a la 10.0.255.255. 10.0.0.0/24 es aún más pequeña, y sólo contiene las direcciones 10.0.0.0 a 10.0.0.255.

Para hacer las cosas más confusas, hay otras maneras de escribir máscaras de red. Podemos escribirlas como direcciones IP:

```
10.0.0.0/255.0.0.0
```

Para terminar, merece la pena señalar que la IP más grande de cualquier red está reservada para la «dirección de difusión», que se puede usar para

Here is a table of network masks:

```
Forma   Forma                   Máximo número   Comentarios
  Corta   Completa                Máquinas

/8      /255.0.0.0              16,777,215      Se suele llamar «clase A»
/16     /255.255.0.0            65,535          Se suele llamar «clase B»
/17     /255.255.128.0          32,767
/18     /255.255.192.0          16,383
/19     /255.255.224.0          8,191
/20     /255.255.240.0          4,095
/21     /255.255.248.0          2,047
/22     /255.255.252.0          1,023
/23     /255.255.254.0          511
/24     /255.255.255.0          255             Se suele llamar «clase C»
/25     /255.255.255.128        127
/26     /255.255.255.192        63
/27     /255.255.255.224        31
/28     /255.255.255.240        15
/29     /255.255.255.248        7
/30     /255.255.255.252        3
```

# 5. Nombres de máquinas y direcciones IP

De manera que cada interfaz en cada nodo tiene una dirección IP. Rápidamente los humanos se dieron cuenta que era bastante difícil tener que recordar números, de manera que decidieron (igual que con los números de teléfono) tener un directorio de nombres. Pero como de todas maneras estamos utilizando ordenadores, es mejor que él mismo haga las consultas por nosotros de forma automática.

De manera que tenemos el Domain Name System (DNS - Sistema de Nombres de Dominio). Hay nodos que tienen direcciones IP bien conocidas a las que los programas pueden preguntar nombres, para obtener direcciones IP a cambio. Casi todos los programas que use serán capaces de hacer esto, y es la razón por la que usted puede poner «www.linuxcare.com» en el Netscape, en lugar de «167.216.245.249».

Por supuesto, necesita al menos la dirección IP de uno de estos «servidores de nombre»: normalmente están almacenados en el fichero `/etc/resolv.conf`

Como las consultas y respuestas DNS son bastante pequeñas (un paquete cada una), no se suele usar el protocolo TCP: proporciona retransmisión automática, ordenación, y fiabilidad en general, pero al coste de enviar paquetes adicionales por la red. En su lugar usaremos el más sencillo «User Datagram Protocol», que no ofrece ninguna de las maravillosas características de TCP que no necesitamos.

# 6. Diferentes servicios: Correo electrónico, Web, FTP, Servicio de Nombres

En el ejemplo anterior, mostramos a Netscape enviando una consulta TCP a un servidor web ejecutándose en otro nodo. Pero imagine que el nodo del servidor web también está ejecutando un servidor de correo electrónico, otro de FTP y un servidor de nombres: ¿cómo sabe a qué servidor va dirigido cada conexión TCP?

Es por esto que TCP y UDP tienen un concepto de «puertos». Cada paquete tiene espacio para un «puerto de destino», que indica para qué servicio es el paquete. Por ejemplo, el puerto 25 de TCP es el servidor de corre, y el puerto 80 TCP es el servidor web (aunque a veces encuentre servidores web en puertos diferentes). Puede encontrar una lista de puertos en `/etc/services`.

Además, si dos ventanas de netscape acceden a la vez a diferentes partes del servidor web, ¿cómo sabe la máquina con el Linux ejecutando Netscape repartir correctamente los paquetes TCP con las respuestas del servidor web?

Aquí es donde entra el «puerto de origen»: cada nueva conexión TCP toma un puerto diferente, de manera que todo el mundo pueden diferenciarlas, incluso si van dirigidas a los mismos IP y puerto de destino. Normalmente, el primer puerto disponible será el 1024, e irá incrementándose con el tiempo y el uso.

# 7. Interfaces de llamada: PPP

Cuando llama con su módem a un ISP (Proveedor de Servicios de Internet), y conecta con el de ellos, el núcleo no sabe cómo enviar paquetes IP mediante él. Hay un protocolo llamado «Point-to-Point Protocol» (Protocolo Punto a Punto) o «PPP», que se usa para negociar con el otro extremo antes de permitir que pase ningún paquete. El ISP lo utiliza para identificar quén llama: en su máquina Linux, hay un programa llamado «demonio PPP» que controla su extremo de la negociación.

Como hay tantos usuarios «de llamada» en el mundo, normalmente no tienen su propia dirección IP: la mayoría de los ISP le asignarán una de las de ellos de forma temporal mientras está usted conectado (el demonio PPP la negociará). A menudo se le llama a esto «dirección IP dinámica», en contraposición a «dirección IP estática», que sería el caso normal cuando que usted tiene una conexión permanente. Normalmente van asignadas a los módem (de ellos): la siguiente vez que marque, posiblemente acceda por un módem diferente de la reserva de módems, y por lo tanto obtendrá una IP diferente.

# 8. Qué aspecto tienen los paquetes

Para el excepcionalmente curioso (y el curiosamente excepcional), aquí tenemos una descripción del aspecto real de un paquete. Hay varias herramientas que miran qué paquetes están entrando y saliendo de su máquina Linux: el más común es «tcpdump» (que comprende más que TCP actualmente). Estos programas se llaman «esnifadores de paquetes» (packet sniffers).

El principio de cada paquete dice a dónde va, de dónde viene, el tipo de paquete, y otros detalles administrativos. Esta parte se denomina «cabecera del paquete». El resto del paquete, contiene los datos a transmitir en sí, y normalmente sel es llama «cuerpo del paquete».

Por lo tanto, cualquier paquete IP comienza con la «cabecera IP»: de al menos 20 bytes de largo. Parece algo como esto: (este diagrama ha sido robado sin ningún tipo de remordimiento de conciencia del RFC 790):

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Versión|  IHL  |Tipo de Servic.|          Tamaño Total         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Identificación        |Flags|  Desplaz. del Fragmento |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Tiempo de Vida |   Protocolo   |    Checksum de la cabecera    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     Dirección de Origen                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     Dirección de Destino                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Los campos importantes son el Protocolo, que indica si es un paquete TCP (número 6), UDP (número 17) u otra cosa, la Dirección IP de Origen y la Dirección IP de Destino.

Ahora, si el campo de protocolo dice que es un paquete TCP, entonces a esta cabecera IP le sigue inmediatamente una cabecera TCP: la cabecera TCP también tiene al menos 20 bytes de longitud:

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        Puerto de Origen       |       Puerto de Destino       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      Número de Secuencia                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Número de Confirmación                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Deplz. |           |U|A|P|R|S|F|                               |
|de los | Reservado |R|C|S|S|Y|I|            Ventana            |
| Datos |           |G|K|H|T|N|N|                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           Checksum            |      Puntero de Urgencia      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Los campos más importantes son el puerto de origen y el de destino, que dicen a qué servicio está destinado el paquete (o de cual viene, en el caso de que sea un paquete de respuesta). Los números de secuencia y confirmación (acknowledgement) se utilizan para mantener el orden de los paquetes, y decirle al otro extremos cuántos paquetes se han recibido. Los indicadores (flags) ACK, SYN, RST y FIN (escritos de mayor a menor) son simples bits que se utilizan en la negociación de apertura (SYN) y cierra (RST o FIN) de las conexiones.

Siguiendo a esta cabecera viene el verdadero mensaje que la aplicación envió (el cuerpo del paquete). Un paquete normal puede tener hasta 1500 bytes: esto significa que el mayor espacio que pueden ocupar los datos es de 1460 bytes (20 bytes para la cabecera IP y 20 para la cabecera TCP): alrededor del 97 %.

# 9. Sumario

De manera que la Internet moderna utiliza paquetes IP para comunicarse, y la mayoría de estos paquetes usan internamente TCP. Hay nodos especiales llamados «routers» que conectan todas las pequeñas redes juntas en redes mayores, y dejan pasar estos paquetes hacia su destino. La mayoría de las máquinas normales están conectadas a una red (esto es, sólo tienen una interfaz), y por lo tanto no son *routers*.

Cada interfaz tiene una única dirección IP, como «1.2.3.4»: las interfaces de la misma red tendrán direcciones IP relacionades, con los mismos primeros números, de la misma manera que las conexiones telefónicas de la misma zona tienen el mismo prefijo. Estas direcciones de red se parecen a las direcciones IP, con una «/» para decir cuánto de ellas es el prefijo, por ejemplo «1.2.0.0/16» indica que los primeros dos dígitos son la dirección de red: cada dígito representa 8 bits.

A las máquinas se les da nombres usando el Servicio de Nombres de Dominio: los programas le piden a los servidores de nombre que les den direcciones IP, dado un nombre como «www.linuxcare.com». Entonces se puede usar esa dirección IP para comunicarse con ese nodo.

Rusty es realmente malo escribiendo documentación, especialmente para novatos.

¡Disfrute!

Rusty.

# 10. Agradecimientos

Gracias a Alison, por empaparse el terrible borrador original, y decirme lo malo que era, de la manera más bonita posible.

# 11. Indice