Características del protocolo TCP

TCP (que significa Protocolo de Control de Transmisión) es uno de los principales protocolos de la capa de transporte del modelo TCP/IP. En el nivel de aplicación, posibilita la administración de datos que vienen del nivel más bajo del modelo, o van hacia él, (es decir, el protocolo IP). Cuando se proporcionan los datos al protocolo IP, los agrupa en datagramas IP, fijando el campo del protocolo en 6 (para que sepa con anticipación que el protocolo es TCP). TCP es un protocolo orientado a conexión, es decir, que permite que dos máquinas que están comunicadas controlen el estado de la transmisión.

El fin de TCP es proveer un flujo de bytes confiable de extremo a extremo sobre una internet no confiable. TCP puede adaptarse dinámicamente a las propiedades de la internet y manejar fallas de muchas clases.

Las principales características del protocolo TCP son las siguientes:

- TCP permite colocar los datagramas nuevamente en orden cuando vienen del protocolo IP.
- TCP permite que el monitoreo del flujo de los datos y así evita la saturación de la red.
- TCP permite que los datos se formen en segmentos de longitud variada para "entregarlos" al protocolo IP.
- TCP permite multiplexar los datos, es decir, que la información que viene de diferentes fuentes (por ejemplo, aplicaciones) en la misma línea pueda circular simultáneamente.
- Por último, TCP permite comenzar y finalizar la comunicación amablemente.

El objetivo de TCP

Con el uso del protocolo TCP, las aplicaciones pueden comunicarse en forma segura (gracias al sistema de acuse de recibo del protocolo TCP) independientemente de las capas inferiores. Esto significa que los routers (que funcionan en la capa de Internet) sólo tienen que enviar los datos en forma de datagramas, sin preocuparse con el monitoreo de datos porque esta función la cumple la capa de transporte (o más específicamente el protocolo TCP).

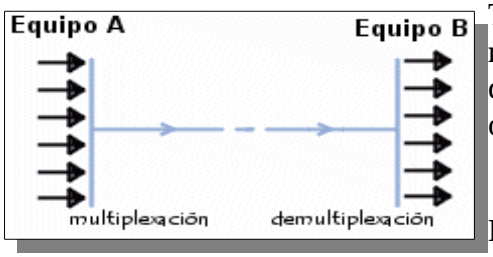
Durante una comunicación usando el protocolo TCP, las dos máquinas deben establecer una conexión. La máquina emisora (la que solicita la conexión) se llama cliente, y la máquina receptora se llama servidor. Por eso es que decimos que estamos en un entorno Cliente-Servidor.

Las máquinas de dicho entorno se comunican en modo en línea, es decir, que la comunicación se realiza en ambas direcciones.

Para posibilitar la comunicación y que funcionen bien todos los controles que la acompañan, los datos se agrupan; es decir, que se agrega un encabezado a los paquetes de datos que permitirán sincronizar las transmisiones y garantizar su recepción.

Otra función del TCP es la capacidad de controlar la velocidad de los datos usando su capacidad para emitir mensajes de tamaño variable. Estos mensajes se llaman segmentos.

La función multiplexión



TCP posibilita la realización de una tarea importante: multiplexar/demultiplexar; es decir transmitir datos desde diversas aplicaciones en la misma línea o, en otras palabras, ordenar la información que llega en paralelo.

Estas operaciones se realizan empleando el concepto de puertos (o conexiones), es decir, un número vinculado a un tipo de aplicación que, cuando se combina con una dirección de IP, permite determinar en forma exclusiva una aplicación que se ejecuta en una máquina determinada.

El formato de los datos en TCP

Un segmento TCP está formado de la siguiente manera:

<table>
<tr><td colspan="32">0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31</td></tr>
<tr><td colspan="16">Puerto de origen</td><td colspan="16">Puerto de destino</td></tr>
<tr><td colspan="32">Número de secuencia</td></tr>
<tr><td colspan="32">Número de acuse de recibo</td></tr>
<tr><td colspan="4">Margen de datos</td><td colspan="6">Reservado</td><td colspan="16">Ventana</td><td colspan="6"></td></tr>
<tr><td colspan="16">Suma de control</td><td colspan="16">Puntero urgente</td></tr>
<tr><td colspan="22">Opciones</td><td colspan="10">Relleno</td></tr>
<tr><td colspan="32">Datos</td></tr>
</table>

Significado de los diferentes campos:

- **Puerto de origen (16 bits)** : Puerto relacionado con la aplicación en curso en la máquina origen
- **Puerto de destino (16 bits)** : Puerto relacionado con la aplicación en curso en la máquina destino
- **Número de secuencia (32 bits)** : Cuando el indicador SYN está fijado en 0, el número de secuencia es el de la primera palabra del segmento actual. Cuando SYN está fijado en 1, el número de secuencia es igual al número de secuencia inicial utilizado para sincronizar los números de secuencia (ISN - Número de Secuencia Inicial).
- **Número de acuse de recibo (32 bits)** : El número de acuse de recibo, también llamado número de descargo se relaciona con el número (secuencia) del último segmento esperado y no el número del último segmento recibido.
- **Margen de datos (4 bits)** : Esto permite ubicar el inicio de los datos en el paquete. Aquí, el margen es fundamental porque el campo opción es de tamaño variable.
- **Reservado (6 bits)** : Un campo que actualmente no está en uso pero se proporciona para el uso futuro.
- **Indicadores (6x1 bit)** : Los indicadores representan información

adicional:

- **URG** : Si este indicador está fijado en 1, el paquete se debe procesar en forma urgente.
- **ACK** : Si este indicador está fijado en 1, el paquete es un acuse de recibo.
- **PSH (PUSH)** : Se utiliza para forzar el enviado inmediato de los datos tan pronto como sea posible. Si el TCP emisor envía un paquete con este flag activado, el TCP receptor sabe que tiene que entregar los datos inmediatamente a la aplicación receptora sin ponerlo en un buffer y esperar a más datos.
- **RST** : Si este indicador está fijado en 1, se restablece la conexión.
- **SYN** : El indicador SYN de TCP indica un pedido para establecer una conexión.
- **FIN** : Si este indicador está fijado en 1, se interrumpe la conexión.

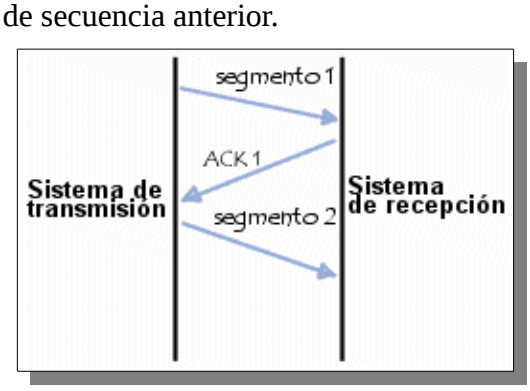
- **Ventana (16 bits)** : Campo que permite saber la cantidad de bytes que el receptor desea recibir sin acuse de recibo.
- **Suma de control (CRC)** : La suma de control se realiza tomando la suma del campo de datos del encabezado para poder verificar la integridad del encabezado.
- P**untero urgente (16 bits)** : Indica el número de secuencia después del cual la información se torna urgente.
- **Opciones (tamaño variable)**: Diversas opciones
- **Relleno** : Espacio restante después de que las opciones se rellenan con ceros para tener una longitud que sea múltiplo de 32 bits.

Confiabilidad de las transferencias

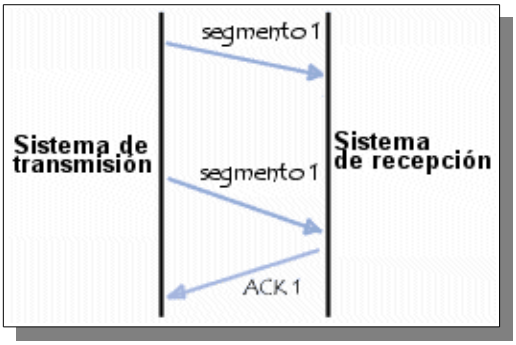
El protocolo TCP permite garantizar la transferencia de datos confiable, a pesar de que usa el protocolo IP, que no incluye ningún monitoreo de la entrega de datagramas.

De hecho, el protocolo TCP tiene un sistema de acuse de recibo que permite al cliente y al servidor garantizar la recepción mutua de datos.

Cuando se emite un segmento, se lo vincula a un número de secuencia. Con la recepción de un segmento de datos, la máquina receptora devolverá un segmento de datos donde el indicador ACK esté fijado en 1 (para poder indicar que es un acuse de recibo) acompañado por un número de acuse de recibo que equivale al número de secuencia anterior.



Además, usando un temporizador que comienza con la recepción del segmento en el nivel de la máquina originadora, el segmento se reenvía cuando ha transcurrido el tiempo permitido, ya que en este caso la máquina originadora considera que el segmento está perdido.



Sin embargo, si el segmento no está perdido y llega a destino, la máquina receptora lo sabrá, gracias al número de secuencia, que es un duplicado, y sólo retendrá el último segmento que llegó a destino.

Cómo establecer una conexión

Considerando que este proceso de comunicación, que se produce con la transmisión y el acuse de recibo de datos, se basa en un número de secuencia, las máquinas originadora y receptora (cliente y servidor) deben conocer el número de secuencia inicial de la otra máquina.

La conexión establecida entre las dos aplicaciones a menudo se realiza siguiendo el siguiente esquema:

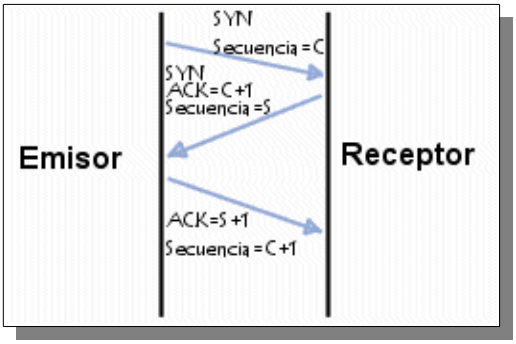
- Los puertos TCP deben estar abiertos.
- La aplicación en el servidor es pasiva, es decir, que la aplicación escucha y espera una conexión.
- La aplicación del cliente realiza un pedido de conexión al servidor en el lugar donde la aplicación es abierta pasiva. La aplicación del cliente se considera "abierta activa".

Las dos máquinas deben sincronizar sus secuencias usando un mecanismo comúnmente llamado negociación en tres pasos que también se encuentra durante el cierre de la sesión.

Este diálogo posibilita el inicio de la comunicación porque se realiza en tres etapas, como su nombre lo indica:

- En la primera etapa, la máquina originadora (el cliente) transmite un segmento donde el indicador SYN está fijado en 1 (para indicar que es un segmento de sincronización), con número de secuencia N llamado número de secuencia inicial del cliente.
- En la segunda etapa, la máquina receptora (el servidor) recibe el segmento inicial que viene del cliente y luego le envía un acuse de recibo, que es un segmento en el que el indicador ACK está fijado en 1 y el indicador SYN está fijado en 1 (porque es nuevamente una sincronización). Este segmento incluye el número de secuencia de esta máquina (el servidor), que es el número de secuencia inicial para el cliente. El campo más importante en este segmento es el de acuse de recibo que contiene el número de secuencia inicial del cliente incrementado en 1.
- Por último, el cliente transmite un acuse de recibo, que es un segmento en el que el indicador ACK está fijado en 1 y el indicador SYN está fijado en 0 (ya no es un segmento de sincronización). Su número de secuencia está incrementado y el acuse de recibo representa el

número de secuencia inicial del servidor incrementado en 1.



Después de esta secuencia con tres intercambios, las dos máquinas están sincronizadas y la comunicación puede comenzar.

Existe una técnica de piratería llamada falsificación de IP, que permite corromper este enlace de aprobación con fines maliciosos.

Método de ventana corrediza o deslizante

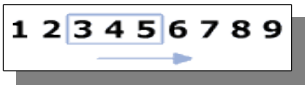
La ventana corrediza ó deslizante es un dispositivo de control de flujo de tipo software, es decir, el control del flujo se lleva a cabo mediante el intercambio específico de caracteres o tramas de control, con los que el receptor indica al emisor cuál es su estado de disponibilidad para recibir datos.

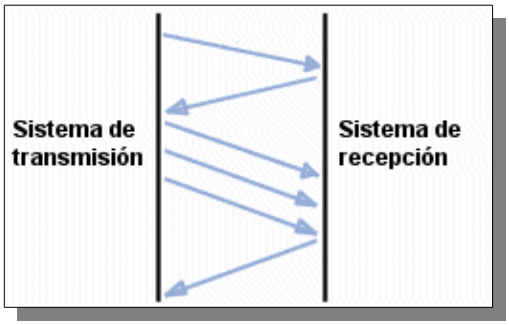
Este dispositivo es necesario para no inundar al receptor con envíos de tramas de datos. El receptor al recibir datos debe procesarlo, si no lo realiza a la misma velocidad que el transmisor los envía se verá saturado de datos, y parte de ellos se pueden perder. Para evitar tal situación la ventana deslizante controla este ritmo de envíos del emisor al receptor.

Con este dispositivo se resuelven dos grandes problemas: el control de flujo de datos y la eficiencia en la transmisión.

En muchos casos, es posible limitar la cantidad de acuses de recibo con el fin de aliviar el tráfico en la red. Esto se logra fijando un número de secuencia después del cual se requiera un acuse de recibo. Este número en realidad se guarda en el campo ventana del encabezado TCP/IP.

Este método se llama efectivamente el "el método de la ventana corrediza" porque, en cierta medida, se define una serie de secuencias que no necesitan acuses de recibo y que se desplaza a medida que se reciben los acuses de recibo.





Además, el tamaño de esta ventana no es fijo. De hecho, el servidor puede incluir el tamaño de la ventana que considera más apropiado en sus acuses de recibo guardándolo en el campo ventana. De este modo, cuando el acuse de recibo indica un pedido para aumentar la ventana, el cliente se desplazará al borde derecho de la ventana.

Por el contrario, en el caso de una reducción, el cliente no desplazará el borde derecho de la ventana hacia la izquierda sino que esperará que avance el borde izquierdo (al llegar los acuses de recibo).

Cómo terminar una conexión

El cliente puede pedir que se termine una conexión del mismo modo que el servidor. Para terminar una conexión se procede de la siguiente manera:

- Una de las máquinas envía un segmento con el indicador FIN fijado en 1, y la aplicación se autocoloca en estado de espera, es decir que deja de recibir el segmento actual e ignora los siguientes.
- Después de recibir este segmento, la otra máquina envía un acuse de recibo con el indicador FIN fijado en 1 y sigue enviando los segmentos en curso. Después de esto, la máquina informa a la aplicación que se ha recibido un segmento FIN y luego envía un segmento FIN a la otra máquina, que cierra la conexión.

Protocolo UDP

El protocolo UDP "User Datagram Protocol" de la capa de transporte es un servicio no orientado a conexión y la unidad de datos que envía o recibe este protocolo es conocido con el nombre de datagrama UDP. El protocolo UDP goza del mismo mecanismo de multiplexamiento utilizado por el protocolo TCP.

Las aplicaciones que requieran de una entrega fiable y ordenada de secuencias de datos deberían utilizar el Protocolo TCP o que la aplicación cumpla con los principios de un protocolo orientado a conexión.

UDP es un protocolo estándar con número 6 de STD. Este protocolo se describe en el RFC 768 - Protocolo de Datagrama de Usuario. Es simple, eficiente e ideal para aplicaciones como el TFTP (Trivial file transfer Protocol - Protocolo de transferencia de archivos trivial) y el DNS. Una dirección IP sirve para dirigir el datagrama hacia una máquina en particular, y el número de puerto de destino en la cabecera UDP se utiliza para dirigir el datagrama UDP a un proceso específico en dicha máquina. La cabecera UDP también contiene un número de puerto origen que permite al proceso recibido conocer como responder al datagrama.

Este protocolo se usa cuando una entrega rápida es más importante que una entrega garantizada, o en los casos en que se desea enviar tan poca información que cabe en un único datagrama. Así, una de sus utilidades más comunes es el envío de mensajes entre aplicaciones de dos host.

UDP no admite numeración de los datagramas, factor que, sumado a que tampoco utiliza señales de confirmación de entrega, hace que la garantía de que un paquete llegue a su destino sea mucho menor que si se usa TCP. Esto también origina que los datagramas pueden llegar duplicados y/o desordenados a su destino. Por estos motivos el control de envío de datagramas, si existe, debe ser implementado por las aplicaciones que usan UDP como medio de transporte de datos, al igual que el reensamble de los mensajes entrantes.

Es por ello es un protocolo del tipo best-effort (máximo esfuerzo), porque hace lo que puede para transmitir los datagramas hacia la aplicación, pero no puede garantizar que la aplicación los reciba.
Cuando se detecta un error en un datagrama, en lugar de entregarlo a la aplicación destino, se descarta.
Cuando una aplicación envía datos a través de UDP, éstos llegan al otro extremo como una unidad.

Al igual que TCP, UDP usa al protocolo IP para transportar sus segmentos.

Características del UDP:

1. No orientado a conexión
2. Utiliza puertos para la comunicación con aplicaciones
3. No usa acknowledge o control de flujo
4. Los mensajes UDP pueden:
    1. Perderse
    2. Duplicarse
    3. Recibidos de forma desordenada
5. RFC 768

Campos

Segmento UDP

0										10										20										30	
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
Puerto UDP origen																Puerto UDP destino															
Longitud del datagrama																Checksum UDP															
Datos																															
...																															

Puerto de Origen : Es opcional; cuando tiene sentido, indica el puerto del proceso emisor, y puede que se asuma que ése sea el puerto al cual la respuesta debería ser dirigida en ausencia de otra información. Si no se utiliza, se inserta un valor cero.
Puerto de Destino : Tiene significado dentro del contexto de una dirección de destino en un entorno Internet particular.
Longitud : Representa la longitud en octetos de este datagrama de usuario, incluyendo la cabecera y los datos. (Esto implica que el valor mínimo del campo Longitud es ocho.)
Checksum : Suma de Control, es el complemento a uno de 16 bits de la suma de los complementos a uno de las palabras de la combinación de una pseudo-cabecera construida con información de la cabecera IP, la cabecera UDP y los datos, y rellenada con octetos de valor cero en la parte final (si es necesario) hasta tener un Múltiplo de dos octetos.

Si la suma de control calculada es cero, se transmite como un campo de unos (el equivalente en la aritmética del complemento a uno). Un valor de la suma de control trasmitido como un campo de ceros significa que el emisor no generó la suma de control (para depuración o para protocolos de más alto nivel a los que este campo les sea indiferente).

Pseudo-cabecera : Que imaginariamente antecede a la cabecera UDP contiene la dirección de origen, la dirección de destino, el protocolo y la longitud UDP. Esta información proporciona protección frente a datagramas mal encaminados. Este procedimiento de comprobación es el mismo que el utilizado en TCP.

Aplicación del Protocolo
Los usos principales de este protocolo son el Servidor de Nombres de Internet y la Transferencia Trivial de Ficheros (Trivial FileTransfer).

- El protocolo UDP a pesar de su sencillez y de haber sido opacado por TCP, poderosas y muy utilizadas aplicaciones se basan en UDP. Entre ellas están:
    - NFS (Network File System): permite utilizar discos de estaciones remotas como si fueran propios.
    - DNS (Domain Name Server): servicio de nombres.
    - SNMP (Simple Network Management Protocol)

Los estándares internacionales son generados y publicados por Organismos Internacionales que discuten y acuerdan definiciones relevantes.

Algunas de las Organizaciones internacionales más conocidas son las siguientes:

- Organización Internacional de Estándares (ISO, International Organization for Standarization). Responsable del modelo de referencia OSI y su conjunto de protocolos.
- Instituto nacional de estándares americanos (ANSI, American National Stadards Institute). Miembro de la ISO al interior de los estados unidos. Su estándar más reconocido es FDDI
- Asociación de industrias electrónicas (EIA, Electronic Industries Association). Especifican estándares de transmisión eléctrica. Su estándar más reconocido es EIA/TIA 232. Comúnmente RS232.
- Instituto de ingenieros electricistas y electrónicos (IEEE, Institute of electrical and electronic engineers). Organización de profesionales que definen estándares de redes. Sus estándares mas conocidos son los IEEE de redes locales.
- Comité consultivo internacional para la telefonía y la telegrafía. (CCITT, Committed for International Telegraph and Telephone). Anterior comité de telecomunicaciones de las naciones unidas. Ahora ITU-T.
- Unión Internacional de Telecomunicaciones (ITU, International Telecommunication Union).
- Sector de estandarización internacional para telecomunicaciones. (ITU-T, International Telecommunication Union Telecommunication Standardization Sector). Es el organismo internacional que desarrolla los estándares de comunicaciones. Su estándar mas reconocido es X.25.
- Consejo de actividades de Internet (IAB, Internet Activities Board). Grupo de investigadores que discuten lo concerniente a Internet, proporciona la investigación y desarrollo de los protocolos TCP/IP. Definen los estándares de Internet en forma de RFC’s (Request for comments) a partir de fuerzas de tarea (IETF, Internet Engineer Task Forces).
- Centro integrado de información de red (INTERNIC, Integrated Network Information Center). Concepto registrado por el departamento de comercio de US para integrar la información de Internet.

Algunos puertos UDP/TCP

echo (7/tcp,udp) .- Se utiliza únicamente para depuración. Sin embargo, un atacante puede realizar "labores de depuración" creando bucles en la red a partir de este puerto (véase udp chargen/19). BLOQUEAR.

systat (11/tcp/udp) .- Muestra información acerca del host como usuarios conectados, carga del sistema, procesos en funcionamiento, etc.. BLOQUEAR.

chargen (19/tcp,udp).- Se utiliza únicamente para depuración. Basta con enviar un paquete a este puerto aparentemente originado en el puerto de echo (7/udp) para provocar un bucle en la red. BLOQUEAR.

telnet (23/tcp,udp).- Vulnerable a "toma de sesiones". Es preferible utilizar en su lugar otras soluciones como SSH.

smtp (25/tcp,udp) .- Históricamente la mayoría de las entradas en hosts han venido a través de este puerto. Se debe FILTRAR este puerto y mantener SIEMPRE la última versión estable conocida de cualquier programa de correo, especialmente si trabajamos con sendmail.

time (37/tcp,udp) .- Devuelve la hora del sistema en un formato legible por la máquina (4 bytes mas o

menos). Puede ser accedido tras un ataque vía ntp(123/tcp,udp).

nameserver (42/tcp,udp).- Si dispone de una red privada, debe instalar un servidor de nombres para ella. Bloquee el acceso a dicho servidor desde el exterior, y utilice siempre la última versión de BIND para resolver nombres. En este caso, puede cortar sin excesivos problemas el acceso al DNS sobre UDP.

tftp (69/tcp,udp) .- Falta de autentificación. Bloquear si no se dispone de máquina alguna con arranque remoto.

private dialout (75/tcp,udp) - - - [RFC1700] .- Si encontramos una traza de este puerto en los diarios del sistema (logs), en el mejor de los casos estaremos siendo analizados por un scanner de puertos. BLOQUEAR.

finger (79/tcp,udp) .- Puede obtenerse información acerca de usuarios concretos, información que puede utilizarse para adivinar claves de acceso. BLOQUEAR

http (80/tcp,udp) .- ¡¡¡Cuidado!!! los servidores web son cada vez más complejos y permiten demasiadas cosas. Conviene redirigir el acceso a un puerto no privilegiado en maquinas unix.

npp (92/tcp,udp) - [Network Printing Protocol] .- Nadie quiere imprimir documentos ajenos ¿ verdad ?.

objcall (94/tcp,udp) - [Tivoli Object Dispatcher] .-
Utilizado por la herramienta de Gestión de redes Tivoli. Si utilizamos tivoli, aplicar las mismas precauciones que con SNMP.

sunrpc (111/tcp,udp) .- Especialmente peligroso sobre UDP. No autentifica fuentes, y es la base para otros servicios como NFS.

auth (113/tcp,udp) .- No debería permitirse obtener información acerca de puertos privilegiados (puede utilizarse para realizar un portscan). No se utiliza mas que en Unix.

ntp (123/tcp,udp) [Network Time Protocol] .- Se utiliza para sincronizar los relojes de las máquinas de una subred. Un ejemplo de ataque clásico consiste en enviar paquetes a este puerto para distorsionar los logs de la máquina.

netbios (137,138,139/tcp,udp) .- No dispone de suficiente autenticación. Afortunadamente según los RFC2001 y 2002 NetBIOS es capaz de funcionar correctamente a pesar de que se estén enviando bloques de datos con información errónea o corrompida.

irc (194/tcp,udp) – No es peligroso en sí; sin embargo sus usuarios suelen divertirse atacando los hosts de otras personas con el fin de echarlos cuando no pueden hacer uso de la orden 'kick'. Generalmente conviene bloquear los puertos 6666, 6667 y 6668 ya que son a los que se enganchan los servidores de IRC.

biff (512/udp) .- Notifica de la llegada de correo. Buen candidato para posibles desbordamientos de buffer, o simplemente para obligar a abandonar la sesión a un usuario debido a la llegada masiva de mensajes de correo. (biff suele funcionar incluso con mesg n)

BLOQUEAR.

who (513/udp) .- Muestra quien está utilizando el host remoto. Se puede obtener información bastante detallada acerca de quién utiliza una máquina y desde que terminal, uptime (tiempo que lleva en funcionamiento), carga de la máquina, etc...
BLOQUEAR.