http://blog.smaldone.com.ar/2006/11/21/tutorial-sobre-tcpip/

La dirección IP es un valor de 4 bytes (32 bits) que se interpreta de la siguiente forma: W.X.Y.Z <Dirección de red, dirección de ordenador > Hay cinco clases de direcciones IP:

```
Red A -> W -> 0XXXXXXX -> 00000000 – 01111111 -> 0-126 (ojo es de 0 a 126 ya que la 127 está reservada)
```

En la suite TCP/IP existen varios tipos de protocolos, vamos a ver algunos de ellos y sus particularidades

TCP

El protocolo TCP tiene las siguientes características:

- Negociación de conexión
- Acuse de recibo de cada paquete
- Control de no duplicidad de paquetes
- Inmune a la llegada desordenada de paquetes
- Inmune a la perdida de paquetes (se solicitan otra vez)

SYN:

El bit se syn indica un intento de iniciar una comunicación

RST:

Se devuelve un paquete rst cuando se intenta conectar a un puerto sin servicio. (esto normalmente indica un escaneo de puertos)

UDP

UDP es un protocolo simple para transferir datos sin toda la sobrecarga del TCP y sin ninguna de sus virtudes. En las conexiones UDP no hay negociación, ni acuse de recibo, ni control de perdida o desorden o duplicación de paquetes, todo esto debe ser gestionado por el servicio que emplea la conexión.

ICMP

El protocolo ICMP es un protocolo de control, los paquetes ICMP no tienen puerto de origen o de destino, en vez de ello tienen un tipo y un subtipo ó código.

Tabla 9-2. Tipos de datagramas de ICMP			
Número de tipo	**Código**	**Nombre**	**Descripción del tipo**
0		echo-reply	Respuesta a eco

Tabla 9-2. Tipos de datagramas de ICMP			
Número de tipo	**Código**	**Nombre**	**Descripción del tipo**
3		destination-unreachable	Destino inalcanzable
	0	Net unreachable	
	1	Host unreachable	
	3	Port unreachable	
	4	Fragmentation needed	
4		Source-quench	Congestión en el tráfico
5		Redirect	Redirección
8		echo-request	Solicitud de eco
11		time-exceeded	Tiempo superado
	0	TTL Exceeded	
	1	Fragment reassembly timeout	
12		parameter-problem	Problema de parámetros
13		timestamp-request	Solicitud de marca de tiempo
14		timestamp-reply	Respuesta de marca de tiempo
15		None	Solicitud de información
16		None	Respuesta de información
17		Address-mask-request	Petición de máscara de dirección
18		Address-mask-reply	Respuesta de máscara de dirección

Paquetes ICMP para verificar las comunicaciones

Fragmentation Needed Ü(3/4):

Se utiliza para descubrir la unidad máxima de transferencia (MTU). En conexiones WAN debería de permitirse.

Ping =>(8/-) <=(0/-)

Si queremos permitir el ping tenemos que permitir los siguiente:

- echo-request 8 (salida del ping)
- echo-reply 0 (respuesta del ping)

Traceroute <=(3/3) <=(11/0)

Para permitir el traceroute:

- port unreachable: Tipo 3 / Código 3
- TTL excedeed : 11 / 0
- Paquetes UDP en el rango 33434:33600

Paquetes ICMP sospechosos o peligrosos:

Redirect <=(5/-)

Alguien intenta redirigir nuestro router.

Source-Quench <=(4/-)

Puede ser un intento de ataque DoS, ya que estos paquetes enlentecen la comunicación.

Parameter Problems => (12/-)

Indica que se nos está aplicando algún tipo de detección de sistema operativo o algún tipo de hackeo.

Port unreachable => (3/3)

Las salidas de paquetes ICMP 3/3 delatan la existencia de un escaneo de puerto de nuestra red.

Fragmentos

Los fragmentos pueden ser de cualquier protocolo (TCP, UDP, ICMP, etc). Como los fragmentos posteriores al primero no llevan la cabecera del protocolo (TCP, UDP, ICMP, etc) solo contienen información de IP (IP origen, IP destino, TOS, etc...) y no los puertos que van en la cabecera TCP/UDP. Por lo tanto en las reglas de filtrado, en las que se acostumbra a filtrar por puertos, no sabremos que hacer con los fragmentos. Por lo tanto hay que crear una regla específica para evitar ataques con paquetes fragmentados.