PROTOCOLO TCP/IP

Protocolo	Nivel OSI	Temas	Métodos
IP (Internet Protocol)es enrutable responsable del direccionamiento IP y de la fragmentación y unión de los paquetes.	Red	Direccionamiento	Red Lógica
		Conmutación	Paquete
		Selección de Ruta	Dinámico
		Servicios de Conexión	Control de Errores (Sólo de la cabecera IP no de los datos)
ICMP (Internet Control Message Protocol)	Red	Servicios de Conexión	Control de Errores Control de flujo de nivel de red
RIP Protocolo de Informacion del router	Red	Descubrimiento de ruta	Vector de Distancia
OSPF Abrir ruta más corta primero	Red	Descubrimiento de ruta	Estado de Enlace
TCP (Transmisión Control Protocol)	Red	Direccionamiento	Servicio
	Transporte	Direccionamiento	Identificador de Conexión
		Desarrollo de segmento	División y combinación
		Servicios de conexión	Secuencia de Segmento Control de Errores Control de flujo de extremo a extremo
UDP (Protocolo de Datagrama de usuario)	Transporte	Direccionamiento	Identificador de Conexión
		Desarrollo de segmento	Combinación
		Servicios de conexión	Sin Conexión
ARP Protocolo de Resolución de Direcciones	Red	Resolución de direcciones	
DNS Sistema de Nombres de Dominio	Transporte	Resolución de nombres/dirección	
FTP Protocolo de transferencia de Ficheros	Sesión Presentación Aplicación		
SMTP Protocolo Simple de Transferencia de Correo	Aplicación	Servicios de Red	Servicio de Mensajes
TELNET Emulación de Terminal Remoto	Sesión Presentación Aplicación		
RPC Llamada de procedimiento remoto	Sesión	Administración de Sesión	
XDR Representación de datos externos	Presentación	Traducción	
NFS Sistema de Archivos de Red	Aplicación	Aplicación	

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
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

Tabla 9-2. Tipos de datagramas de ICMP			
Número de tipo	**Código**	**Nombre**	**Descripción del tipo**
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.

DIRECCIONAMIENTO

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:

Clase A → W →0 # # # # # # # → 00000000 – 01111111 → 0-126 (ojo es de 0 a 126 ya que la 127 está reservada)

Nº de Redes: 27=128-2=126 (Se quitan 2 ya que las direcciones 0000000 y 1111111 están reservadas). Nº de Host por red =224=16.777.216-2=16.777.214

Clase B → W.X → 1 0 # # # # # # → 10000000 – 10111111 □ 128-191

Nº de redes:2^14=16384 (no se quita nada porque no hay dentro de este rango ninguna dirección con todo 0 ó todo 1)

Nº de Host por red = 216=65.536-2=65.534 (se le quitan 2 por la dirección todo 0 y todo 1)

Clase C → W.X.Y → 110 # # # # # → 11000000 – 11011111 □ 192-223

Nº de redes=221=20.097.152 Nº de Host por red=28-2=254

Clase D los primeros cuatro bits a 1110 → 224.xxx.xxx.xxx-239.xxx.xxx.xxx Reservada para direcciones IP multicast

Clase E los primeros cinco bits a 11110 → 240.xxx.xxx.xxx-247.xxx.xxx.xxx Reservada

Clase	Valor de W	Identificador de Red	Identificador de Host	Nº de redes	Nº de Host por Red
A	1-126	W	x.y.z	126	16.777.214
B	128-191	w.x	y.z	16.384	65.534
C	192-223	w.x.y	z	2.097.152	254

Dentro de las clases hay direcciones con un significado especial como las siguientes:

- Todo a 0 (0.0.0.0) La utiliza el sistema sólo durante el arranque antes de saber su propia dirección.
- Todo a 1 (255.255.255.255) Broadcast o Multidifusión
- Dirección de la red a 0 + dirección del nodo (0.0.0.62) identifica al propio host en la red a la que pertenece. En este ejemplo identifica al host 62 de esa red.
- Dirección de red y resto a 0 (192.168.12.0) Identifica a la dirección de la red, con lo cual se pueden enviar paquetes a todos los nodos de la red.
- La dirección Clase A 127.xxx.xxx.xxxse usa para comunicación dentro del mismo ordenador. Convencionalmente se utiliza 127.0.0.1 como la dirección de bucle cerrado los procesos que necesitan comunicarse con otros a través de TCP/IP en el mismo ordenador, usan esta dirección para evitar tener que enviar paquetes a la red.
- Poniendo todos los bits a uno en toda la dirección del nodo significa un mensaje para todos los ordenadores. Por ejemplo la dirección 128.18.255.255 significa todos los ordenadores de la red clase B 128.18

Existen además unas direcciones reservadas para redes privadas:

- 1.xxx.xxx.xxx (1 Clase A)
- 172.16.xxx.xxx a 172.31.xxx.xxx
- 192.168.0.xxx a 193.168.255.xxx

Referencias

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