ANÁLISIS DEL PROTOCOLO TCP

Morales Aguilar Miguel Angel.
Instituto Tecnológico de Cancún

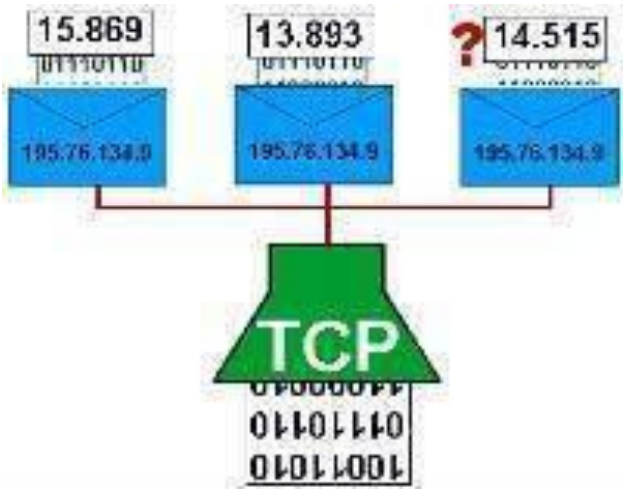
Ismael Jiménez Sánchez.

¿QUÉ ES PROTOCOLO TCP?

Diseñado para ofrecer un transporte fiable sobre el servicio no fiable.

Servicio orientado a conexión.

Los paquetes TCP se llaman segmentos.



FUNCIONES DEL PROTOLO TCP

- Mutiplexar el nivel de aplicación.
- Establecer y terminar conexiones.
- Controlar errores, retransmitir segmentos perdidos o erróneos. Eliminar duplicados.

FILTROS TRAFICO TCP

1. tcp.srcport == 21
2. tcp.dstport == 80
3. tcp.hdr_len> 20
4. (tcp.window_size <1460) && (tcp.flags.fin == 0) && (tcp.flags.reset == 0)
5. ! (tcp.flags.cwr == 0) || ! (tcp.flags.ecn == 0)
6. tcp.options.mss_val <1460
7. tcp.options.wscale_val
8. tcp.analysis.flags
9. tcp.analysis.lost_segment

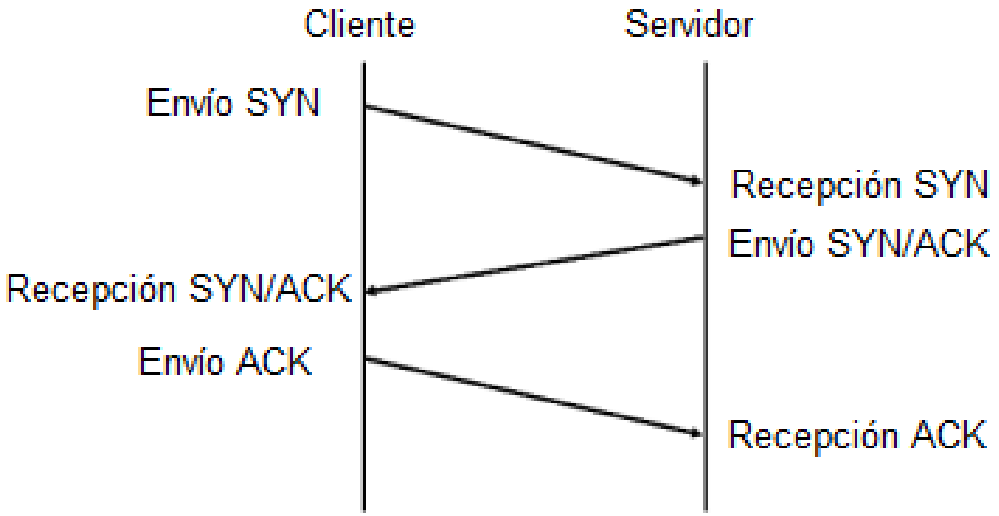
FLAGS TCP

- CWR
- ECE
- URG
- ACK
- PSH
- RST
- SYN
- FIN

ESTABLECIMIENTO DE CONEXIÓN TCP

Las conexiones TCP se establece mediante un protocolo de enlace de tres vías.

- [SYN]
- [SYN, ACK]
- [ACK]

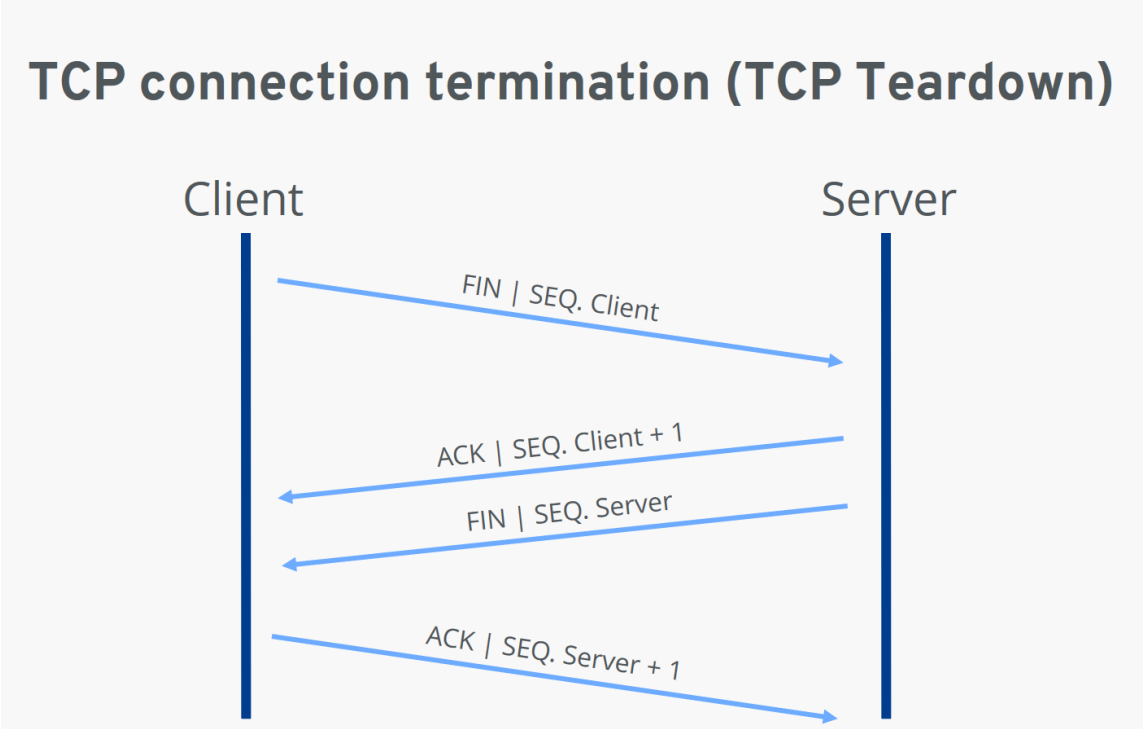


TERMINACIÓN DE LAS CONEXIONES TCP

[FIN]

[FIN, ACK]

[ACK]



PREGUNTAS

CONCLUSIÓN.