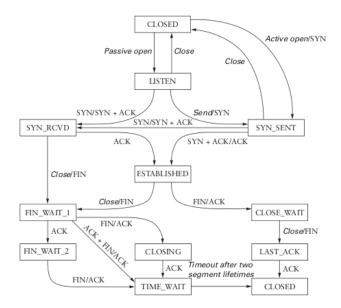
End to End

Máquina de estados TCP:



Congestión

Ventana máxima:

MaxWindow = Min(RWND, CWND)

Ventana efectiva:

EffectiveWindow = MaxWindow - (LastByteSent - LastByteAcked)

Ventana de congestión inicial:

CWND = IW = 2 * SMSS

Tamaño de segmento inicial:

SMSS = 2KB

Tamaño de SSTHRESH inicial:

ISSTHRESH = 64kb

Incremento de la ventana de congestión en Slow Start (CWND < SSTHRESH):

CWND+=min(N,SMSS) por cada ACK con N la cantidad de bytes reconocidos por el ACK.

Incremento de la ventana de congestión en Congestion Avoidance (CWND > SSTHRESH):

CWND+=SMSS*SMSS/CWND por cada ACK o hasta un 1 SMSS por RTT.

Decremento de la ventana y el umbral ante un time-out:

 $SSTHRESH = max(FlightSize/2, 2*SMSS) \\ CWND = LW = 1 \ SMSS$

Decremento de la ventana y el umbral ante 3 ACKs duplicados (FR/FR):

 $SSTHRESH = max(FlightSize/2, 2*SMSS) \\ CWND = SSTHRESH + 3$

Incremento de la ventana de congestión en FR/FR:

CWND+=SMSS por cada ACK Duplicado.

Salida de FR/FR:

CWND = SSTHRESH ante un ACK que reconoce datos nuevos.

```
Reinicio de la ventana ante un tiempo idle ( 1 RTO sin transmitir ):
   RW = min(IW, cwnd)
   Estimación del RTT:
   RTT[i+1] = (1 - alpha) * RTT[i] + alpha * SRTT siendo SRTT el i - esimo RTT medido
   Ajuste del RTO:
   RTO[i] = 2 * RTT[i]
Dominios y Servicios
Web (HTTP):
    Infraestructura: Servidor Web, Proxy, Browser
    Mensajes del cliente (Requests): GET, HEAD, POST
        Formato de request:
(Tipo de request) (Recurso) (Versión HTTP) Host:(Nombre del host)
        Ejemplo:
GET /casa.jpg HTTP 1.1 Host: www.dc.uba.ar
Pide el recurso casa.jpg usando HTTP/1.1 al host www.dc.uba.ar
    Mensajes del servidor (Responses):
    1xx Informatinal, 2xx Success, 3xx Redirection, 4xx Client Error, 5xx Server Error
   Sistema de nombres de dominio (DNS):
    Infraestructura: Servidor autoritativo (primario o secundario), Resolver
    Mensajes del cliente: Consulta Recursiva, Consulta Iterativa
    Mensajes del servidor: Respuesta autoritativa, Respuesta no autoritativa
   E-Mail (SMTP):
    Infraestructura: Servidor saliente (SMTP), Servidor entrante (POP3/IMAP), Relay, User agent
    Mensajes Cliente:.
     SMTP: HELO, MAIL, RCPT, DATA, QUIT.
     POP3: USER, PASS, STAT, RETR, DELE, QUIT.
     IMAP: LOGIN, SELECT, FETCH, DELETE, SEARCH, CLOSE.
    Mensajes Servidor:.
     SMTP: 2xx Ok, 3xx Waiting, 4xx Not available, 5xx Error.
     POP3: +OK, -ERR, #xxx.
     IMAP: OK, NO, BAD.
Seguridad
Criptografía simétrica y asimétrica, Firma Digital, Certificados, Conexiones Seguras, Firewalls
   DMZ: Zona demilitarizada de la red. Tipicamente ubicada en la frontera de la red interna.
   Mensaje: M
   Criptograma: C
   Digesto: D
   Clave simétrica: K
   Clave pública de Alice: K_{4}^{+}
   Clave privada de Alice: K_A^-
   Encriptar M utilizando la clave Q: E_Q(M) = C \text{ con } Q \in \{K, K_A^+, K_A^-\}
```

Desencriptar el C utilizando la clave Q: $D_Q(C) = M \text{ con } Q \in \{K, K_A^+, K_A^-\}$

Aplicar Función de Hash Criptográfico: FHC(M) = D

Aclaración: La notación permite combinar cada algoritmo con cada tipo de clave para obtener distintos resultados. No todo algoritmo permite toda clave. Deberá aclararse qué algoritmo es el utilizado.

Integración

Arquitectura de capas. Modelo OSI. Modelo TCP/IP.

