

Reinicio de la ventana ante un tiempo idle (1 RTO sin transmitir):

$$RW = \min(IW, cwnd)$$

Estimación del RTT:

$$RTT[i + 1] = (1 - \alpha) * RTT[i] + \alpha * SRTT \text{ siendo } SRTT \text{ el } i - \text{esimo } RTT \text{ medido}$$

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 Informational, 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. Típicamente ubicada en la **frontera** de la red interna.

Mensaje: M

Criptograma: C

Digesto: D

Clave simétrica: K

Clave pública de Alice: K_A^+

Clave privada de Alice: K_A^-

Encriptar M utilizando la clave Q: $E_Q(M) = C$ con $Q \in \{K, K_A^+, K_A^-\}$

Desencriptar el C utilizando la clave Q: $D_Q(C) = M$ 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.

