Solución Examen – 26 de julio de 2025
(ref: sol_erc202507.odt)

Instrucciones

- **Indique su nombre completo y número de cédula en cada hoja.**
- **Numere todas las hojas e indique la cantidad total de hojas que entrega en la primera.**
- **Escriba las hojas de un solo lado y utilice una caligrafía claramente legible.**
- **Comience cada pregunta teórica y cada ejercicio en una hoja nueva.**
- **Solo se responderán dudas de letra. No se responderán dudas de ningún tipo los últimos 30 minutos del examen.**
- **El examen es individual y sin material. Apague su teléfono celular mientras esté en el salón del examen.**
- **Es obligatorio responder correctamente al menos 15 puntos en las preguntas teóricas y 20 de los problemas prácticos. Los puntos ganados en el curso se suman a los puntos de teórico.**
- **El puntaje mínimo de aprobación es de 60 puntos.**
- **Para todos los ejercicios, si es necesario, puede suponer que dispone de los tipos de datos básicos (p.ej. lista, cola, archivo, string, etc.) y sus funciones asociadas (ej: tail(lista), crear(archivo), concatenar(string, string).**
- **Justifique todas sus respuestas.**
- **Duración: 3 horas. Culminadas las 3 horas el alumno no podrá modificar las hojas a entregar de ninguna forma.**

Preguntas Teóricas

Pregunta 1 (10 puntos)

a) Indique los participantes involucrados en el envío y recepción de correo electrónico y qué protocolos utilizan para comunicarse.

b) Describa brevemente los protocolos de acceso a correo vistos en el curso y sus principales características.

c) Suponga que le han dicho que el nombre de host del (único) servidor de correos de `fing.edu.uy` es `correo-e.fing.edu.uy`.

   i. ¿Cómo podría verificarlo sin comunicarse con `correo-e.fing.edu.uy`?

   ii. ¿Cómo podría obtener la dirección IP del servidor de correos de `fing.edu.uy` una vez obtenido el nombre de host?

Solución

a) Los participantes involucrados son: agente de usuario remitente, servidor de correos remitente, servidor de correos destino, agente de usuario destino. Los protocolos usados son: SMTP o HTTP (en el caso de webmail) para el envío de correo del agente de usuario remitente al servidor de correos remitente, SMTP para envío de correo desde el servidor de correos remitente al servidor de correos destino, y POP, IMAP o HTTP para la recepción del correo del servidor de correos destino al agente de usuario destino.

b) Los protocolos de acceso a correo vistos en el curso son POP, IMAP y HTTP.

POP (Post Office Protocol) permite listar, leer y eliminar correos pero no mantiene estado entre sesiones. Puede operar como *download and delete*, borrando los mensajes después de descargados del servidor o *download and keep*, donde los mensajes se mantienen en el servidor después de descargados. No almacena estado, entonces por ejemplo no se pueden marcar correos como leídos.

IMAP (Internet Message Access Protocol) al igual que POP permite listar, leer y eliminar correos pero mantiene estados al introducir la noción de carpetas. Los mensajes pueden asociarse a carpetas como Recibidos, Favoritos, Papelera, Spam y demás, así manteniendo estado entre sesiones.

HTTP se utiliza como protocolo de acceso a correo en el caso del webmail. Los agentes de usuario, en este caso navegadores web, se comunican con el servidor de correos vía HTTP para obtener los correos e interactuar con ellos.

c) i) Haciendo una consulta DNS para obtener el valor del registro MX de fing.edu.uy se obtiene el nombre de host del servidor de correos de fing.edu.uy. Si es correo-e.fing.edu.uy, lo que le han dicho

es cierto.
ii) Haciendo una consulta DNS para obtener el valor del registro A asociado al nombre de host hallado en la parte anterior se obtiene la dirección IP del servidor de correos de fing.edu.uy.

Pregunta 2 (10 puntos)

a) Explique la estrategia de generación de segmentos ACK de TCP vista en el curso, considerando qué eventos en el receptor generan qué acciones por parte de éste.
b) Considere 2 situaciones de conexiones TCP utilizando Ethernet en Capa de Enlace de Datos:
unas sobre un enlace con una tasa de pérdidas de un segmento cada 100 transmitidos, y otras sobre un enlace con una tasa de pérdidas de un segmento cada 1.000.000 transmitidos. Comente y justifique respecto a si al comparar las 2 situaciones planteadas, la generación de ACKs se podría ver afectada y de qué forma.

Solución

a) En el curso se vieron 4 situaciones:
1. Evento: llegada de un segmento en orden con el número de secuencia esperado. Todos los datos hasta el número de secuencia esperado ya han sido reconocidos.
Acción: ACK retardado. Esperar hasta durante 500 milisegundos la llegada de otro segmento en orden. Si el siguiente segmento en orden no llega en este intervalo, enviar un ACK.
2. Evento: llegada de un segmento en orden con el número de secuencia esperado. Hay otro segmento en orden esperando la transmisión de un ACK.
Acción: enviar inmediatamente un único ACK acumulativo, reconociendo ambos segmentos ordenados.
3. Evento: llegada de un segmento desordenado con un número de secuencia más alto que el esperado. Se detecta un hueco.
Acción: enviar inmediatamente un ACK duplicado, indicando el número de secuencia del siguiente byte esperado (que es el límite inferior del hueco).
4. Evento: llegada de un segmento que completa parcial o completamente el hueco existente en los datos recibidos.
Acción: enviar inmediatamente un ACK, suponiendo que el segmento comienza en el límite inferior del hueco.

b)
La lógica que el receptor TCP aplica para generar ACK no cambia con la tasa de error del enlace: siempre responde a los cuatro eventos listados en la parte a).
Lo que sí varía es la frecuencia con la que cada evento ocurre, y por tanto la cantidad y el tipo de ACK que realmente se envían.

En un enlace con pérdidas relativamente altas (un segmento perdido por cada cien transmitidos, 1%) aparecen huecos en la secuencia de mensajes con mayor frecuencia. Cada vez que un segmento se pierde, los que llegan después lo hacen “por delante” del esperado, de modo que el receptor detecta la brecha y envía de inmediato ACK duplicados (evento 3) para indicar el byte que falta. Cuando el emisor retransmite y completa ese hueco, el receptor reacciona con un ACK inmediato (evento 4). Además, el receptor apenas puede aprovechar la técnica del ACK retardado debido a las pérdidas. El resultado global es una mayor generación de ACKs debido a los duplicados y ACKs inmediatos, subutilización del canal y retrasos en el envío de la información contenida en los segmentos a las aplicaciones que está haciendo uso de las conexiones TCP afectadas.

En cambio, cuando la tasa de errores es muy baja (un segmento perdido cada millón, 0,0001 %) los segmentos casi siempre llegan en orden y sin huecos. Predominan los eventos 1 y 2: la mayoría de los ACK pueden agrupar datos porque otro segmento consecutivo suele llegar antes de que expire el retardo de 500 ms. Los eventos 3 y 4 solo se producen excepcionalmente, así que los ACK duplicados casi desaparecen. El flujo de ACK se vuelve estable, con menos ACKs individuales y mayor proporción de ACKs acumulativos por lo que el canal se utiliza mas eficientemente para transportar la información

útil de las aplicaciones.

Pregunta 3 (10 puntos)

Respecto a IPv6:

a) Enumere y explique dos diferencias con IPv4.
b) Indique los tipos de direcciones existentes. ¿Para qué se utiliza cada uno?
c) Dos subredes que utilizan IPv6 deben comunicarse entre sí a través de una red que utiliza IPv4. Explique una técnica para poder lograr la comunicación.

Solución

a) Dos diferencias son:

1. Mayor tamaño de dirección. Con 32 bits en IPv4 y 128 bits en IPv6, IPv6 permite tener un número de direcciones mucho mayor que IPv4, solucionando el problema de agotamiento de direcciones. El total de direcciones IPv6 es 2^128, suficientes como para que cada grano de arena del planeta tenga su propia dirección IPv6.
2. Desaparición de la fragmentación y reensamblado en routers intermedios. En IPv6, la fragmentación y el reensamblado debe realizarse en los emisores y receptores, no en los routers intermedios. Si un router intermedio recibe un datagrama IPv6 cuyo tamaño supera el MTU del enlace de salida, se descarta y se envía un mensaje ICMP de notificación al emisor, quien puede reenviar los datos en datagramas más pequeños.

b) Los tipos de direcciones existentes son:

i) Unicast – Identifican una única interfaz en la red.
ii) Multicast – Identifican un grupo de interfaces. Un datagrama enviado a una dirección multicast se entrega a todos los miembros del grupo.
iii) Anycast – También identifica un grupo de interfaces, pero un datagrama enviado a una dirección anycast se entrega a un solo miembro del grupo, el más próximo.
iv) Direcciones reservadas – No identifican interfaces, cumplen propósitos específicos. Por ejemplo, la dirección sin especificar (::/128), la dirección de loopback (::1/128) y la dirección de ruta por defecto (::/0).

c) Para comunicar dos subredes IPv6 a través de una red IPv4, una posibilidad es aplicar la técnica de *tunneling*: en el router de origen que une la red IPv6 con la red IPv4, se encapsula el datagrama IPv6 como carga útil de un datagrama IPv4. El datagrama IPv4 con el datagrama IPv6 encapsulado se enruta y transmite a través de la red IPv4 hasta que llega al router que une la red IPv4 con la red IPv6 de destino, quien desencapsula el datagrama IPv6 y lo envía dentro de la red IPv6.

Pregunta 4 (10 puntos)

La empresa “ACME Networking” fabrica placas de red Ethernet y accidentalmente les ha asignado la misma dirección MAC a todas. Usted compra tres equipos (A, B y C) con una tarjeta de red marca ACME cada uno, y los instala en una subred privada, donde A, B y C tienen direcciones IP distintas.
Se envía un ping de A hacia B. Explique y justifique si la operación funcionaría correctamente, mencionando el tráfico observado en los tres hosts, si todos los dispositivos están conectados a través de:

a) Un hub.
b) Un switch.

Nota: En cada parte, todas las tablas inicialmente están vacías.

Solución

Como todas las tablas están vacías y A y B están en la misma subred, realizar el ping implica un ARP Request de A solicitando la MAC asociada a la IP de B, un ARP Reply de B a A, un Echo Request de A a B

y un Echo Reply de B a A.

a) Un hub es un dispositivo de capa física que repite los datos recibidos por todas sus interfaces (excepto la interfaz por la que llegó). El ARP Request llegará a todos los dispositivos de la red, debido al comportamiento del hub. La dirección IP contenida en el ARP Request coincide con la dirección IP de B, por lo que B responde con un ARP Reply. El ARP Reply tendrá la misma dirección MAC en origen y destino, que además coincide con las MAC de A, B y C. Al estar los hosts conectados mediante un hub, el ARP Reply llega a todos los dispositivos (excepto B). La dirección MAC de destino del paquete coincide con las direcciones MAC de A y C, por lo que ambos procesan el paquete. Sin embargo, C recibe un ARP Reply sin un ARP Request previo, y además la IP de destino contenida en el ARP Reply no coincide con la IP de C; por lo tanto, C descarta el paquete. A recibe el ARP Reply, lo acepta y ya puede enviar el Echo Request.

Por el hub el Echo Request es recibido por todos los dispositivos de la subred (excepto A); como la MAC de destino coincide con la MAC de B y C, B y C aceptan el paquete en su capa de enlace y lo pasan a la capa de red. Sin embargo, en C la dirección IP de destino no coincide con la IP de la interfaz por lo que se descarta. En B el paquete coincide en dirección MAC de destino y dirección IP de destino, por lo que se procesa y envía el Echo Reply.

Siguiendo la misma lógica, por el hub el Echo Reply es recibido por todos los dispositivos de la subred (excepto B); como la MAC de destino coincide con la MAC de A y C, A y C aceptan el paquete en su capa de enlace y lo pasan a la capa de red. Sin embargo, en C la dirección IP de destino no coincide con la IP de la interfaz por lo que se descarta. En A el paquete coincide en dirección MAC de destino y dirección IP de destino por lo que se recibe correctamente el Echo Reply.

La operación funciona, con procesamiento adicional.

b) Llamemos MAC_ACME a la MAC de A, B y C. Inicialmente el switch tiene su tabla vacía por lo que el ARP Request de A es enviado por flooding a todos los dispositivos de la red excepto A. El switch asocia el puerto conectado a A con la MAC MAC_ACME, ya que es la MAC de origen del paquete. La dirección IP en la solicitud coincide con la dirección IP de B, por lo que B responde con un ARP Reply. El switch recibe el ARP Reply, y ahora asocia el puerto conectado a B con la MAC MAC_ACME, ya que es la MAC de origen del paquete. La interfaz de origen y la interfaz por la que se enviaría según lo recién aprendido son iguales, por lo que el switch descarta la trama (filtrado). El ARP Request de A no tuvo éxito, por lo que no puede enviar el Echo Request.

La operación no funciona.

Problemas Prácticos

Problema 1 (30 puntos)

La empresa “Monte Videos” le ha encargado la implementación de su nuevo servicio de transmisión en vivo de eventos deportivos por Internet. El servicio consiste en que los clientes se conectan al sistema e inmediatamente comienzan a recibir la transmisión. Para la gestión del sistema (iniciar o pausar la transmisión en vivo) también se cuenta con el rol de administrador, y solo puede conectarse a lo sumo un administrador por vez.

El servidor de video estará accesible en la dirección `envivo.montevideos.uy`, al que se conectará un administrador en el puerto TCP 11611 y clientes en el puerto TCP 22322. El servidor obtiene los datos de video mediante la función `get_video():bytes`, que devuelve un conjunto de bytes de video que luego deben ser enviados a todos los clientes conectados.

Los comandos enviados por el administrador son “PLAY\n” (inicia o retoma el envío del stream a todos clientes), “STOP\n” (detiene el envío del stream para todos los clientes) y “DISCONNECT\n” (indica desconexión del administrador). El servidor devuelve “RCVD\n” luego de cada comando recibido, incluyendo el de desconexión (en ese caso luego de enviarlo cierra la conexión). Si se recibe un comando que no tiene efecto (ej: “PLAY\n” cuando ya se está enviando video) el servidor igualmente envía “RCVD\n”.

Inicialmente, cuando el primer cliente se conecta, el servidor debe transmitir el video al cliente, no es necesario un comando de PLAY inicial.

Se pide: Implemente el servidor del servicio de transmisión en vivo en un lenguaje de alto nivel usando las primitivas de Sockets de la cartilla del curso. Dispone de funciones auxiliares para estructuras de datos, manipulación de strings, etc.

Solución

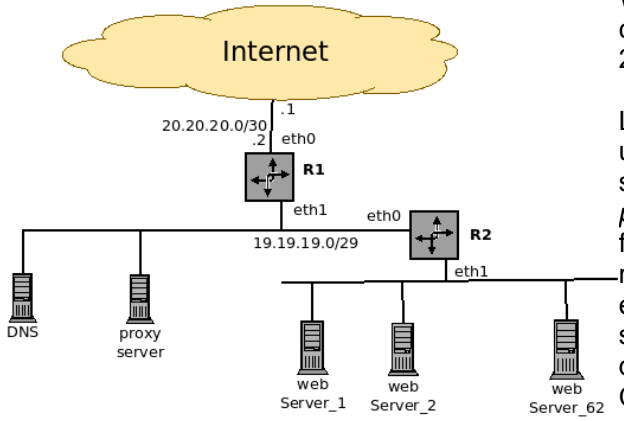
```
program ej1;

clientes : set of socket;
sem_video : semaphore(1); // semáforo inicializado en 1
enviar_video : boolean;

procedure servidor();
begin
   thread.new(hilo_admin);

   master = socket.tcp();
   master.bind(envivo.montevideos.uy, 22322);
   server = master.listen();
   server.settimeout(-1);
   enviar_video = true;

   thread.new(enviar_datos_video);

   while true do begin
      client, err = server.accept();
      if (not err) then  // si hay error con un cliente no cierro los demás
         clientes.add(client);
   end;

   server.close(); // inalcanzable
end;

procedure hilo_admin();
```

```
begin
   master = socket.tcp();
   master.bind(envivo.montevideos.uy, 11611);
   server = master.listen();
   server.settimeout(-1);

   while true do begin
      admin, err = server.accept();

      while (true) do // se acepta solo una conexión por vez
         buff = "";
         err = false;
         while (“\n” not in buff and not err) do begin
            data, err = admin.receive();
            buff = buff + data;
         end;

         if (err) then begin
              admin.close();
              break;
         end;

         if (buff == "PLAY\n" and not enviar_video) then begin
            enviar_video = true;
            sem_video.release(); // libero hilo transmisión de video
         end;
         else if (buff == "STOP\n" and enviar_video) then begin
            enviar_video = false;
            sem_video.acquire(); // tranco hilo transmisión de video
         end;

         resp = “RCVD\n”;
         err = false;
         while (resp <> "" and not err) do
            resp, err = admin.send(resp);

         if (err or buff == "DISCONNECT\n") then begin
            admin.close();
            break;
         end;
      end;
   end;
end;

procedure enviar_datos_video();
begin
   while (true) do begin
      sem_video.acquire(); // queda trancado si se recibió STOP
      sem_video.release();

      data = get_video();
      for (client in clientes) do begin
         video = data;
         err = false;
         while (video <> "" and not err) do
            video, err = client.send(video);
         if (err) then begin
            client.close();
```

```
            clientes.remove(client);
          end;
        end;
      end;
    end;
```

Problema 2 (30 puntos)

La empresa “WebService” brinda servicios de alojamiento de páginas web de diferentes clientes, las que se deben poder acceder desde Internet mediante sitios con nombre *clienteX.webservice.uy*, donde *clienteX* refiere a la página web del cliente X.
La empresa tiene contratada su conexión a Internet a través de un ISP, conectado al router R1. El ISP asignó a WebService la red pública 19.19.19.0/29 . La conectividad con Internet es a través de la IP 20.20.20.1 en el ISP y 20.20.20.2 en router R1, como muestra la figura.



La empresa cuenta con un conjunto de 62 servidores web en una red privada que serán utilizados para atender las solicitudes de los usuarios. Para esto, se cuenta con un *proxy inverso,* ubicado en la red pública (*proxy server* en la figura), que atiende las solicitudes web recibidas y las reenvía al servidor que corresponda. Más específicamente, este equipo acepta una solicitud de un usuario, la reenvía al servidor que corresponda y devuelve al usuario la respuesta dada por éste.
Como se muestra en la figura, los 62 servidores web de los clientes se encuentran conectados a través del router R2 (el cual no implementa NAT).
El DNS de la figura es el autoritativo de la zona *webservice.uy*.

Se pide:

a) Asigne direcciones IP a cada interfaz de red de la empresa, e indique las tablas de ruteo de los routers R1 y R2, del *proxy_server* y de un *web_Server_X*.
b) Indique cómo se debería configurar el servidor de DNS de WebService para un sitio *clienteX.webservice.uy*, indicando IP y tipo de registro. Explique cómo un navegador de un usuario obtendrá esa información para acceder al sitio web del cliente X.
c) Muestre en una tabla el camino seguido por una solicitud HTTP desde una computadora con IP 55.55.5.5 hacia un servidor web de un cliente, y su respuesta. Indique IPs y puertos origen y destino de cada paso. Justifique brevemente cada paso.
d) Suponga que se desea agregar más servidores *proxy in0versos* para distribuir la carga de las peticiones de los usuarios*;* explique qué configuración anterior debe modificar y cómo. Para ello no se pueden agregar ni equipamientos ni funcionalidades. ¿Tiene límite la cantidad de servidores a agregar? Justifique.

Solución

a)
Asignación de IPs:

En red 20.20.20.0/30

R1_eth0	20.20.20.2

En red 19.19.19.0/29

R1_eth1	19.19.19.1
R2_eth0	19.19.19.2
DNS	19.19.19.3
proxy_server	19.19.19.4

Para la red privada se utiliza el prefijo 10.0.0.0/25

R2_eth1	10.0.0.1

web_server_1	10.0.0.2
web_server_2	10.0.0.3
web_server_3	10.0.0.4
….	
web_server_62	10.0.0.63

Tablas

R1

Prefijo	Next Hop	Interfaz
20.20.20.0/30	DC	eth0
19.19.19.0/29	DC	eth1
0/0	20.20.20.1	eth0

R2

Prefijo	Next Hop	Interfaz
19.19.19.0/29	DC	eth0
10.0.0.0/25	DC	eth1

proxy_server

Prefijo	Next Hop	Interfaz
19.19.19.0/29	DC	eth0
10.0.0.0/25	19.19.19.2	eth0
0/0	19.19.19.1	eth0

web_server

Prefijo	Next Hop	Interfaz
10.0.0.0/25	DC	eth0
19.19.19.0/29	10.0.0.1	eth0

a)

Para configurar el dominio nombre.webservice.uy, se debe agregar en la zona webservice.uy un registro A (Asocia el nombre de dominio con una dirección IP). La IP asignar es la del proxy server.

Dominio	TTL	Tipo	registro
nombre.webservice.uy	14400	A	19.19.19.4

Cuando se desea acceder a la página web, el cliente consultará al DNS por el dominio nombre.webservice.uy, donde el servidor root de DNS lo redirccionará al servidor que atiende uy. Este servidor rediccionará al DNS de la empresa, quién contestara la IP del proxy server.

b) Se considera un flujo con origen 55.55.5.5 hacia el dominio nombre.webservice.uy. Se agregan los pasos intermedios de los routers mostrados en la figura (R1 y R2).

IP origen	IP destino	puerto origen	puerto destino	observaciones
55.55.5.5	19.19.19.4	8888	443	Recibido en R1_eth0
55.55.5.5	19.19.19.4	8888	443	Transmitido por R1_eth1 y recibido por proxy_server
19.19.19.4	10.10.10.2	9999	443	Transmitido por proxy_server y recibido por R2_eth0

19.19.19.4	10.10.10.2	9999	443	Transmitido por R2_eth1 y recibido por web_server
10.0.0.2	19.19.19.4	443	9999	Transmitido por web server y recibido por R2_eth1
10.0.0.2	19.19.19.5	443	9999	Transmitido por R2_eth0 y recibido por proxy_server
19.19.19.4	55.55.5.5	443	8888	Transmitido por proxy_server y recibido por R1_eth1
19.19.19.4	55.55.5.5	443	8888	Transmitido por R1_eth0

d)

Para agregar un servidor proxy, puede realizarse agregando una nueva IP al dominio presentado en la parte b.

Dominio	**TTL**	**Tipo**	**registro**
nombre.webservice.uy	14400	A	19.19.19.4
nombre.webservice.uy	14400	A	19.19.19.5
nombre.webservice.uy	14400	A	19.19.19.6

El DNS devuelve los dos valores cambiando el orden cada vez que responde.

La cantidad máxima de servidores, está dado por las IPs públicas disponibles, dado que para ser accedido desde Internet debe tener una red pública. La red 19.19.19.0/29 permite tener 6 hosts (mas la dirección de red y broadcast), y tiene las interfaces de R1, R2 y el DNS, por lo que quedan 3 IP libres.