Introducción a las Redes de Computador{ae}s y Comunicación de Datos

Solución Examen – 3 de febrero de 2011

(ref: sirc1102.odt)

Preguntas Teóricas

Pregunta 1 (10 puntos)

a) Clase 1 de Seguridad (Clase 25), diapositiva 2 de la hoja 2.
   Confidencialidad: sólo el emisor y el receptor deberían "entender" el contenido del mensaje. El emisor cifra el mensaje . El receptor descifra el mensaje .
   Integridad del mensaje: el emisor y el receptor buscan asegurar que el mensaje no ha sido alterado (en tránsito o después) sin ser detectado
   No repudio: no poder negar la autoría de un mensaje

b) Clase 1 de Seguridad (Clase 25), diapositiva 2 de la hoja 15. Al diagrama presentado en dicha diapositiva falta agregarle,previo a ingresarlo al buzón, el cifrado de todo con la clave pública del destinatario. En el destino, lo primero que se hacer luego de retirado del buzón es descifrar todo con la clave privada del destinatario.

Pregunta 2 (10 puntos)

Explique el funcionamiento del protocolo DHCP detallando el intercambio de mensajes entre cliente y servidor.

http://www.fing.edu.uy/inco/cursos/redescomp/teorico/cap04_2_1xhoja_2009.pdf slides 44-46
http://www.fing.edu.uy/inco/cursos/redescomp/teorico/cap03_1_2009_2xhoja.pdf slide 19

Pregunta 3 (10 puntos)

Mencione y explique los campos más importantes de los segmentos TCP y UDP.

http://www.fing.edu.uy/inco/cursos/redescomp/teorico/cap03_3_2009_2xcarilla.pdf slide 5

Pregunta 4 (10 puntos)

a) Describa la técnica denominada NAT, explicando las modificaciones que un router NAT debe realizar sobre los paquetes salientes y entrantes.

   http://www.fing.edu.uy/inco/cursos/redescomp/teorico/cap04_2_1xhoja_2009.pdf pág 17 (4-53)

b) De una justificación para la siguiente frase: NAT no respeta el principio de aislación de capas

   http://www.fing.edu.uy/inco/cursos/redescomp/teorico/cap04_2_1xhoja_2009.pdf pág 19 (4-55)

c) Describa brevemente las tres soluciones planteadas en el teórico para atravesar un router NAT por parte de un cliente que se encuentra en una red con direcciones públicas y quiere contactar a un servidor que está en una red con direcciones privadas.

   http://www.fing.edu.uy/inco/cursos/redescomp/teorico/cap04_2_1xhoja_2009.pdf pág 20,21,y 22 (4-56,57 y 58)

Problemas Prácticos

Problema 1 (30 puntos)

a) Considerando un overhead de 16 bytes en la transmisión de una muestra de sonido, ¿que tamaño tiene el campo de datos de cada paquete UDP transmitido por el origen?

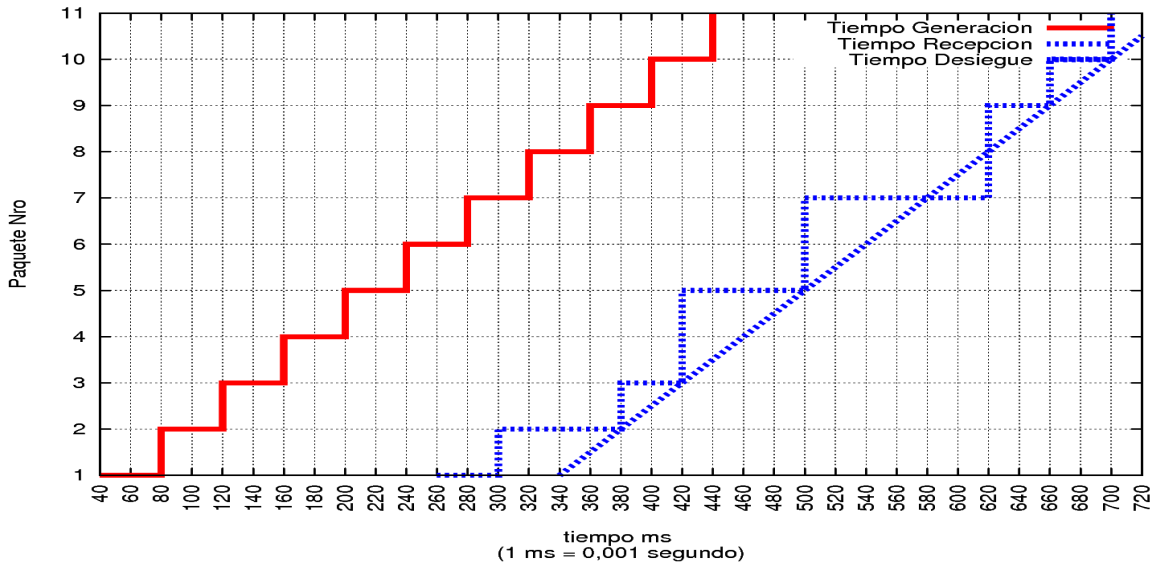
Se envía una muestra cada 40 ms.
Entonces por segundo se enviarán 1000/40 = 25 muestras por segundo
El flujo total es de 64 kbps = 64000 bps
Entonces 64000 bps / 25 muestras/s = 2560 bits/muestra = 320 bytes/muestra
Por lo tanto el campo de datos del paquete UDP contiene 16 bytes + 320 bytes = 336 bytes.

b) Sean t_i y r_i los tiempos de generación y recepción del datagrama *i*. El receptor reproduce los datagramas en el tiempo $t_i + p$, siendo *p* lo suficientemente grande para que la reproducción sea continua. Para los primeros 9 datagramas presentes en la gráfica, determinar el mínimo tiempo *p.* En este caso suponer que no ocurren pérdidas de datagramas en la red.

Se debe determinar el mayor de los tiempos entre generación t_i y recepción r_i que será el tiempo *p*. El tiempo deberá ser mayor o igual que el máximo de éstos tiempos.

Paquete	ri	ti	ri-ti
1	260	40	220
2	300	80	220
3	380	120	260
4	420	160	260
5	420	200	220
6	500	240	260
7	500	280	220
8	620	320	300
9	620	360	260

El mayor ri-ti se encuentra en el paquete 8, con un valor de 300 ms. Si se considera un retardo en el despliegue de 300 ms se tendrán todas las muestras al tiempo de ser presentadas.



c) Implemente dos procedimientos del lado del receptor, uno que almacene las muestras recibidas en una estructura auxiliar, y otro que las reproduzca.
Para el cálculo de la latencia p_i de cada datagrama aplicar el mecanismo de promedio ponderado que se define en la nota al final del ejercicio.
Se suponen conocidos los parámetros t_i y r_i para cada datagrama llegado (medidos en ms). La solución enviará una señal para cancelar la reproducción cuando, durante *N* períodos de 40ms consecutivos, p_i supere los 400ms y/o la pérdida de datagramas supere el 10% (que se verificará por medio del estudio de los números de secuencia recibidos).
Se cuenta con las siguientes primitivas:

Para la recepción y reproducción de muestras:

- `getMuestra(r,t,nro_sec,muestra)`, si existe en el buffer un paquete con muestra de sonido devuelve 0, en caso contrario devuelve -1. En t devuelve el tiempo de generación (en ms), en r el tiempo de recepción (en ms), en nro_sec el número de secuencia de la muestra y en muestra la muestra recibida.
- `reproduceMuestra(muestra)`, reproduce la muestra pasada como parámetro (debe invocarse en el tiempo que corresponde su reproducción).
- `now()` procedimiento que devuelve el tiempo actual.

Para el almacenamiento temporal de muestras en el equipo destino:

- `insertMuestra(u,nroSec,muestra)`, inserta en una estructura auxiliar la muestra a ser reproducida en el tiempo *u*, con número de secuencia *nroSec* y con la muestra de sonido pasada en *muestra*. La inserción se realiza ordenada por tiempo *u*.
- `getTimeNext()`, devuelve el tiempo de reproducción *u* de la próxima muestra disponible en la estructura auxiliar.
- `getNroSecNext()`, devuelve el número de secuencia *nroSec* de la próxima muestra disponible en la estructura auxiliar.
- `getMuestraNext()`,devuelve y elimina de la estructura auxiliar lal próxima muestra a ser reproducida.

Los procedimientos utilizan variables comunes.

Se supone que la numeración de los números de secuencia siempre comienza en 0.

Considero muestras perdidas, a las que al momento de ser reproducidas no están presentes.

Variables globales a los dos procedimientos:

```
diExcedidos = 0;
di = 400;


Procedure get()

while (true) {
      if (getMuestra(r,t,nroSec,muestra) == 0){
            di = 0.9 * di + 0.1 * (r – t);
            if ( t+di > now() ){
                  // inserto solamente si se reproduce en
                  // tiempo futuro
                  insertMuestra(t+di,nroSec,muestra);
            }
            // determina cuantos di excedidos continuos hubo
            if ( di > 400 ){
                  diExcedidos++;
            }else{
                  diExcedidos=0;
            }
      }
}
```

```
Procedure reproduce()
nroRep = -1;
perdidos[0..N-1] = false;  // para determinar perdidas en ultimos N muestras
while (true) {
      // verifico si hay muestra para reproducir
      if ( getTimeNext() <= now() ){
            auxNroSec = getNroSecNext();
            reproduceMuestra(getMuestraNext());
            // marco nros de secuencia perdidos
            if ( ((nroRep + 1)%N) != (auxNroSec%N) ){
                  for i=(nroRep+1) to (auxNroSec-1)
                        perdidos[i%N] = true;
            }
            perdidos[(auxNroSec%N)] = false;
            nroRep=auxNroSec;
            // verifico si se excede límites aceptados
            cantPerdidos=0;
            for i=0 to (N-1){
                  if (perdidos[i]) cantPerdidos++;
            }
            if ( ((cantPerdidos/N) > 0.1) or (diExcedidos>N)){
                  print “Valores permitidos excedidos”;
                  kill(get);
                  exit();
            }
      }
      sleep(5ms);
}
```

Problema 2 (30 puntos)

a)
Transita por los segmentos WLAN1, LAN1 y LAN3 y en ese orden.
WLAN1 - SA: MAC1, RA: MAC4, DA: MAC2, IPorigen: 172.172.0.17, IPdestino: 203.203.203.3
LAN1 - SA: MAC1, DA: MAC2, IPorigen: 172.172.0.17, IPdestino: 203.203.203.3
LAN3 - SA: MAC8, DA: MAC9, IPorigen: 172.172.0.17, IPdestino: 203.203.203.3

b)
i)
Transita por los segmentos WLAN2, LAN2 y LAN3 y en ese orden.
WLAN2 - SA: MAC1, RA: MAC7, DA: MAC5, IPorigen: 172.172.0.17, IPdestino: 203.203.203.3
LAN2 - SA: MAC1, DA: MAC5, IPorigen: 172.172.0.17, IPdestino: 203.203.203.3
LAN3 - SA: MAC8, DA: MAC9, IPorigen: 172.172.0.17, IPdestino: 203.203.203.3

ii)
Se debería implementar un túnel (mecanismo de tunneling o encapsulation) entre el router HA y el router FA (gracias al vínculo existente entre las empresas y por tratarse de una solución ampliamente utilizada y los administradores respectivos y, es posible y escalable pues sólo requiere la configuración de dos routers) , de forma de “forzar” (agregando un encabezado IP al paquete original cuya dirección destino sea el otro el extremo del túnel) el forwarding de los paquetes destinados a MN, que ahora está en la Foreign Network; en caso contrario, si el HA realiza el forwarding hacia la FN de los paquetes destinados al MN, el next hop lo devolverá (creando un loop y finalmente descartando los paquetes por TTL) debido a que para que la solución sea posible y realizable, no debe implicar modificar los routers intermedios (por ejemplo, agregando rutas estáticas en cada una). Dicho túnel se utilizaría en esta configuración sólo en el sentido HA → FA y los paquetes enviados a través de él se traducen en paquetes a los que se les agrega un encabezado IP con IPorigen: 111.1.1.1 e IPdestino: 222.1.1.1 (solución simplificada)

c)
caso a)
desde MN hacia CN - IPorigen: 172.172.0.17, IPdestino: 203.203.203.3
desde CN hacia MN - IPorigen: 203.203.203.3, IPdestino: 172.172.0.17

caso b)
desde MN - IPorigen: 172.172.0.17, IPdestino: 203.203.203.3
desde CN - IPorigen: 203.203.203.3, IPdestino: 172.172.0.17 (para llegar al HA)
IPorigen: 111.1.1.1, IPdestino: 222.1.1.1 (para llegar al FA) y que encapsula un paquete con IPorigen: 203.203.203.3, IPdestino: 172.172.0.17