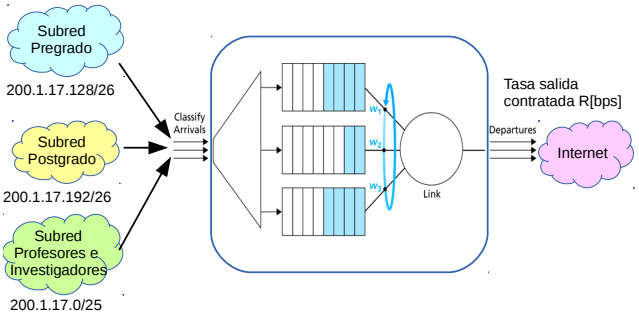
ELO323: Redes de Computadores II /IPD438: Seminario de Redes de Computadores 10.01.14

2° Certamen Tiempo 90 min.

1. (30 puntos) Consideremos la red de un departamento de alguna universidad, en particular consideraremos su acceso a Internet como se muestra en la figura. En particular analizaremos opciones para distribuir la tasa de salida de datos hacia Internet. Suponga que los laboratorios de pregrado, los de postgrado, y las oficinas de profesores e investigadores está organizados en subredes independientes.



a) Suponga que en lugar de varias colas, como en la figura, se usa sólo una cola con política FIFO. Si hay sólo un alumno de pregrado trabajando en su subred, ¿Cuál es la tasa de salida mínima que podría recibir? ¿Cuál es la tasa de salida máxima que podría recibir? Explique cuándo ocurre cada escenario.

La peor situación se produce cuando todos los usuarios están generando tráfico de salida en forma permanente desde las otras subredes. El alumno recibirá en promedio una fracción del tráfico de salida R/n, siendo n el número de usuarios enviando tráfico.
La mejor situación se produce cuando nadie más está trabajando en cualquiera de las redes. La tasa máxima recibida es R [bps].

Nota: Alguien puede notar que el protocolo puede hacer una diferencia. La respuesta previa asume todos usan el mismo protocolo de transporte. Si el alumno envía tráfico UDP y los demás TCP. El alumno obtendrá mayor tasa que todo el resto pues cuando el TCP de los demás reduzca su tasa por congestión, el tráfico UDP del alumno podrá ocupar la capacidad liberada.

b) Suponga varias colas, como en la figura, pero con política Round-Robin y con tráfico clasificado según subred de origen. Si hay sólo un alumno de pregrado trabajando en su subred, ¿Cuál es la tasa de salida mínima que podría recibir? ¿Cuál es la tasa de salida máxima que podría recibir? Explique cuándo ocurre cada escenario.

El peor caso se produce cuando en todo momento hay tráfico de las otras dos subredes. Las tres colas siempre tendrán tráfico que enviar y la política Round-Robin enviará una misma cantidad desde cada cola (o subred), luego al alumno obtendrá como mínimo R/3.
El mejor caso nuevamente se produce cuando nadie más está trabajando. En este caso la política Round-Robin notar´a las otras colas vacías y asignará toda la tasa R al tráfico del alumno como único en la cola.

c) Con R=7 Mbps, se desea garantizar que cada subred disponga de una fracción mínima de la tasa de salida, de tal manera que la subred de pregrado obtenga al menos 2 Mbps, la de postgrado al menos 2 Mbps y la de profesores al menos 3 Mbps. Obtenga los valores w1, w2 y w3. Si hay sólo un alumno de pregrado en su subred, ¿Cuál es la tasa de salida mínima que podría recibir? ¿Cuál es la tasa de salida máxima que podría recibir? Explique cuándo ocurre cada escenario.

Los pesos deben corresponder a la tasa deseada para cada cola. En este caso sería:
w1=w2= $\frac{2}{7}$ *, y* $w3=\frac{3}{7}$.
El peor caso para el alumno es que haya tráfico permanente en las otras dos redes. Siendo él el único en su red obtendrá una tasa de 2R/7, es decir 2 [Mbps].
La tasa máxima sigue siendo R=7Mbps cuando nadie más está usando ese enlace de salida.

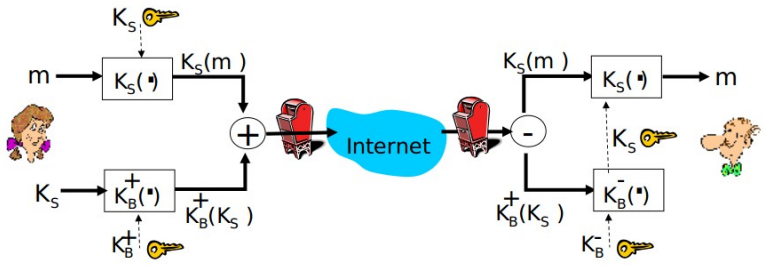
Nota: Para garantizar esas asignaciones mínimas de tasa para cada subred, debemos usar Weighted Fair Queueing. En este caso al recorrer las colas se envía una cantidad de bytes (paquetes) no constante entre todas ellas, así se logra diferenciar la tasa asignada a cada una.

2. (12 puntos) Mencione 4 características nuevas o mejoras de la TV Digital respecto de la TV Analógica.
** La TVD mejora la calidad de la imagen. Esto se refleja en su resolución y la nitidez lograda para cada pixel el cual está libre de ruido y efectos "fantasmas".*
** La TVD hace un mejor uso del ancho de banda. Esto permite, entre otros, el envío de varios programas de televisión en el mismo ancho de banda usado por la TV análoga para el envío de sólo un programa.*
** La TVD permite el envío de datos digitales. Esto permite enviar los subtítulos (close caption) en más de un idioma, cuyo despliegue es seleccionado por el usuario. También permite el envío de la Guía Electrónica de la Programación.*
** La TVD envía una señal especialmente adaptada para dispositivos móviles. Ésta es más robusta ante usuarios en movimiento.*
** La TVD permite el envío de aplicaciones interactivas.*
** La TVD contempla el envío de alertas de emergencias en caso de catástrofes.*

3. (12 puntos) El lenguaje NCL para programar aplicaciones interactivas se basa en responder preguntas como ¿qué mostrar?, ¿cuándo mostrar?, etc. Indique qué relación existe entre éstas preguntas (y otras) con los siguientes rótulos del lenguaje NCL:
a) <region> b) <media> c) <descriptor> d) <link>

a) <region> Permite definir dónde se mostrará un contenido multimedia.
b) <media> Permite definir qué medio será considerad (video, imagen, audio, texto, otra aplicación anidada, etc)
c) <descriptor> Permite definir cómo el contenido multimedio debe ser mostrado (duración, semi-transparente, etc.)
d) <link> Ppermite definir cuándo un contenido debe ser mostrado (junto con el inicio de otro, al término de otro, etc.)

4. (24 puntos) Indique si el esquema de comunicación mostrado ofrece cada uno de los siguientes servicios.



Explique en cada caso.
a) Autenticación de fuente
b) Autenticación del destino
c) Confidencialidad
d) Integridad

a) Autenticación de fuente: Servicio no es ofrecido. La información enviada no incluye datos que permitan garantizar que el mensaje fue enviado por Alicia.
b) Autenticación de destino: Sí es ofrecida. El mensaje podrá ser descifrado sólo por Bob. Esto por el uso de su clave pública para encriptar la clave simétrica usada para cifrar/descifrar el mensaje.
c) Confidencialidad: Sí es ofrecida. Nadie más que Alicia y Bob pueden acceder al contenido del mensaje. En el caso que el mensaje sea capturado o eliminado, igual no se viola la confidencialidad. La confidencialidad no obliga a que Bob deba acceder al mensaje original.
d) Integridad: No es ofrecida. Si alguien tiene acceso al mensaje lo puede descartar y enviar uno completamente nuevo. Bob usará su clave privada para extraer la nueva clase simétrica y no podrá saber si el mensaje fue alterado.

5. (22 puntos) Mi amigo Pedro desarrolló un sistema para abrir una puerta a distancia. Creó con un control remoto en el cual grabar una clave simétrica presionando una secuencia en sus botones. Lo mismo puede hacer con el dispositivo receptor para grabar la misma clave simétrica.
Luego de programar la clave, al presionar un botón el control remoto ~~éste~~ envía un código cifrado para abrir y otro para cerrar la puerta. Usando la clave simétrica el receptor descifra el código enviado y actúa según éste indica.

Al poco tiempo Pedro se enteró que venden duplicadores, los cuales capturan y pueden reproducir las transmisiones enviadas por un control remoto. Pedro toma contacto con usted y le pide ayuda para mejorar su sistema.
¿Cuál sería su recomendación? Explique su recomendación de hardware y método (pasos) para apertura y cerrado. Usted puede agregar pares transmisor-receptor y/o hacer cambios al método usado por Pedro.

Esta pregunta es un ejemplo de cómo las ideas usadas en un contexto pueden ser portada a uno similar.
El sistema ideado por Pedro ocupa siempre las mismas secuencias cifrada para apertura y para cerrado. Eso da espacio a que sistemas duplicadores graben esa secuencia y puedan vulnerar su seguridad.
Se requiere entonces modificar el sistema para que la secuencia cambie y pueda ser usada sólo una vez.

Algunas propuestas para mejorarlo:

** Usando técnica sugerida ante ataque de reproducción. En este caso se requiere ampliar el hardware para lograr comunicación bidireccional. El equipo actuador debería contar con un transmisor y el control remoto con un receptor.*
Método: Al presionar el botón de apertura, el control remoto envía una petición no cifrada de número aleatorio. El actuador responde con un número aleatorio no cifrado y no re-utilizable. El control remoto concatena este número con el código y lo encripta con la clave simétrica. El actuador descifra el mensaje y toma en cuenta el comando enviado sólo si el número aleatorio enviado coincide.
22 puntos

** Tomando idea tipo SSL (Secure Socket Layer): Además de la clave simétrica, el control remoto y el receptor pueden manejar un número de secuencia. La concatenación de ambos constituyen la nueva clave simétrica a usar para cifrar el mensaje enviado.*
El receptor usa su clave simétrica y número de secuencia para descifrar el mensaje.
Hasta aquí 15 puntos.

El mecanismo sugerido tiene un gran problema, si un niño -o por casualidad un objeto en mi bolsillo- acciona el control remoto lejos del receptor, los números de secuencia perderán la sincronía.
Una solución para esto es que el receptor intente descifrar el mensaje con números de secuencia posteriores al último, ej. 64. Al encontrar el correcto se re-sincroniza con el número de secuencia usado.
7 puntos más.