Solución Examen – 12 de diciembre de 2024
(ref: sol_erc202412.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)

Suponga que usted es el administrador de red de la organización *examenredes* y adquirió un servidor al que le asignó la IP privada 10.1.0.10. Allí instaló un servidor web para la página web institucional.

a) ¿Es posible acceder a la página web institucional desde Internet? Justifique su respuesta.

Suponga ahora que al servidor se le asignó la IP pública 164.73.32.20. Usted adquirió el dominio *examenredes.uy* y desea que la página pueda accederse **solo** en la URL *http://www.examenredes.uy* .

b) Mencione y explique los distintos niveles de la jerarquía DNS. ¿Qué registros DNS deben insertarse en la jerarquía para que la página web sea accesible desde Internet? Suponga que la organización *examenredes* tiene un servidor DNS instalado en la dirección IP pública 164.73.32.4 pero sin ningún registro configurado.

c) ¿Es posible tener otro servidor web que sirva la misma página en la misma URL? ¿Cómo?

Solución

a) No es posible, ya que desde Internet no se puede acceder a una IP privada de una red. En particular 10.1.0.10 pertenece además al bloque de IPs 10.0.0.0/8, que es de uso exclusivo para redes privadas y sus direcciones no son enrutables en Internet (RFC 1918).

b)
La jerarquía DNS consiste de los siguientes niveles:

1. Servidores raíz – Conocidos globalmente, contienen registros NS, A y AAAA de los servidores TLD.
2. Servidores TLD (ej: com, edu, uy) – Contienen registros NS, A y AAAA de los servidores autoritativos que pertenecen al TLD (ej: el servidor TLD com tiene los registros asociados al servidor autoritativo de un dominio que termina en com)
3. Servidores autoritativos de los dominios – Contienen más registros (MX, TXT, CNAME, A, AAAA, NS) y son administrados por el propietario del dominio.
4. Servidor DNS local – Cuando los hosts hacen consultas DNS, lo hacen a su servidor DNS local, quien resuelve la consulta ya sea iterativa o recursivamente.

Para que la página pueda ser accedida en al URL solicitada, en el servidor DNS TLD de uy se agregan los siguientes registros:

i. (examenredes.uy, ns.examenredes.uy, NS)
ii. (ns.examenredes.uy, 164.73.32.4, A)

Y en el servidor DNS autoritativo de examenredes (ns.examenredes.uy por la configuración anterior) se agrega el siguiente registro:

i. (www.examenredes.uy, 164.73.32.20, A)

c) Sí, si se tienen dos servidores web con el mismo contenido, se insertan dos registros A con nombre "www.examenredes.uy" en el servidor DNS autoritativo de examenredes, con la IP de un servidor web. El servidor DNS realizará Round Robin entre los dos registros para responder la consulta, así sirviendo la misma página en dos servidores distintos en la misma URL, implementando un balanceo de carga básico.

Pregunta 2 (10 puntos)

a) Analice el rendimiento de un protocolo de transporte de tipo stop&wait.
b) Explique la relación entre números de secuencia y tamaño de ventana en protocolos de transporte en pipeline. En particular, comente si se pueden generar situaciones que impidan el correcto funcionamiento mediante un ejemplo sencillo.
c) ¿Cómo se determina la diferencia entre el último byte enviado y el último byte reconocido en TCP, teniendo en cuenta el control de congestión y el control de flujo?

Solución

a)
Vamos a usar un ejemplo con magnitudes realistas tomado del libro (p. 247 de la 7a edición en inglés).
Si consideramos dos hosts separados por aprox. por 4500km, el RTT, es decir, el doble del retardo de propagación se calcula como:
RTT = 2*4,5*10exp(6)m/3*10exp(8)m/s = 3*10exp(-2)s = 30 milisegundos

Por otro lado, si consideramos paquetes de 1000 bytes y una tasa de 1 Gbps, el retardo de trasmisión se calcula:
dTRANS = L/R = 1000*8bits/1*10exp(9)bits/s = 8*10exp(-6)s = 8 microsegundos.

Dado que se debe esperar el ACK del receptor, solo se puede enviar un paquete por cada RTT.
La utilidad o rendimiento del protocolo stop&wait se calcula como:
Utilidad = dTRANS/(dTRANS+RTT) = 0.008 milisegundos/30.008 milisegundos = 0.00027

Es decir que para las magnitudes consideradas el rendimiento es del 0.027%, o dicho de otra forma, solo podemos enviar 270 kbps en un enlace de 1 Gbps, completamente inaceptable.
Para paquetes muy grandes mejora un poco, pero siempre es inaceptable.

b)
Si tenemos una cantidad finita de números de secuencia, por ejemplo, un campo de 3 bits (0⋯7), cada tanto tendremos que reutilizar dichos números de secuencia, es decir, usaremos 0...7, 0...7 y así sucesivamente. Esto introduce el problema de poder distinguir entre diferentes instancias de los mismos números de secuencia (¿estoy en la primera, segunda, tercera instancia de 0..7?), lo que implica que la cantidad de números de secuencia posibles debe ser mayor que la cantidad de paquetes pendientes permitidos. Por ejemplo, la técnica stop&wait permite un paquete pendiente a la vez y tiene dos números de secuencia distintos (0 y 1).

Llamemos SWS (Sender Window Size) y RWS (Receiver Window Size) a los tamaños de ventana del emisor y receptor respectivamente. Supongamos que tenemos un número más en nuestro espacio de números de secuencia que paquetes potencialmente pendientes; es decir, SWS ≤ MaxSeqNum − 1, donde MaxSeqNum es la cantidad de números de secuencia disponibles. ¿Es esto suficiente? La respuesta depende de RWS. Si RWS = 1, entonces MaxSeqNum ≥ SWS + 1 es suficiente. Si RWS es igual a SWS, entonces tener un MaxSeqNum que sea solo uno mayor que el tamaño de la ventana de envío no es suficiente. Para ver esto, consideremos la situación en la que tenemos los ocho números de secuencia del 0 al 7, y SWS = RWS = 7. Supongamos que el remitente transmite los paquetes 0…6, se reciben

correctamente, pero se pierden los ACK. El receptor ahora espera los paquetes 7, 0…5, pero el remitente agota el tiempo de espera y envía los paquetes 0…6. Desafortunadamente, el receptor espera la segunda instancia de los paquetes 0…5, pero recibe la primera instancia, lo cual es erróneo y es una situación que queremos evitar.

Luego, el tamaño de la ventana de envío no puede ser más de la mitad del tamaño de la cantidad de números de secuencia disponibles cuando RWS = SWS, o dicho de manera más precisa,

SWS < (MaxSeqNum+1)/2

Intuitivamente, lo que esto quiere decir es que el protocolo de ventana deslizante alterna entre las dos mitades del espacio de números de secuencia, de la misma manera que stop&wait alterna entre los números de secuencia 0 y 1. La única diferencia es que se desliza continuamente entre las dos mitades en lugar de alternar discretamente entre ellas.

c)
LastByteSent – LastByteAcked = min{cwnd, rwnd}

Pregunta 3 (12 puntos)

a) Describa mediante un pseudo-código el algoritmo de enrutamiento de vector-distancia. ¿Qué información mantiene cada nodo?
b) Proponga un ejemplo de red donde:
   i) un cambio en los costos de los enlaces provoca conteo a infinito.
   ii) un cambio en los costos de los enlaces no provoca conteo a infinito.

   Muestre el intercambio de mensajes del protocolo para justificar la respuesta.

Solución

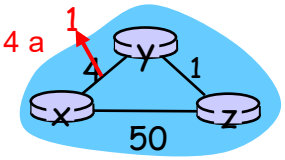
a)
En cada nodo, x:

```
1  Initialization:
2          for all destinations y in N:
3                  Dx(y)= c(x,y)/* if y is not a neighbor then c(x,y)= ∞ */
4          for each neighbor w
5                  Dw(y) = ? for all destinations y in N
6          for each neighbor w
7                  send distance vector Dx = [Dx(y): y in N] to w
8
9  loop
10         wait (until I see a link cost change to some neighbor w or
11               until I receive a distance vector from some neighbor w)
12
13         for each y in N:
14                 Dx(y) = minv{c(x,v) + Dv(y)}
15
16 if Dx(y) changed for any destination y
17         send distance vector Dx = [Dx(y): y in N] to all neighbors
18
19 forever
```

Cada nodo x mantiene la siguiente información de enrutamiento:
Para cada vecino v, el costo c(x,v) desde x hasta el vecino directamente conectado, v.
El vector de distancia del nodo x, es decir, Dx = [Dx(y): y en N], que contiene la estimación de x de su costo para todos los destinos, y, en N.
Los vectores de distancia de cada uno de sus vecinos, es decir, Dv = [Dv(y): y en N] para cada vecino

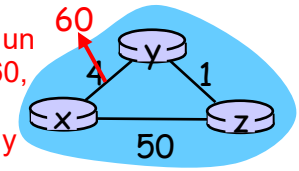
v de x.

b.ii)
Consideremos el ejemplo del libro, donde el costo de (x,y) cambia de 4 a 1.
El algoritmo DV hace que ocurra la siguiente secuencia de eventos:



- En el momento *t0*, **y** detecta el cambio de costo del enlace (el costo ha cambiado de 4 a 1), actualiza su vector de distancia e informa a sus vecinos de este cambio.
- En el momento *t1*, **z** recibe la actualización de **y** y actualiza su tabla. Calcula un nuevo costo mínimo para **x** (ha disminuido de un costo de 5 a un costo de 2) y envía su nuevo vector de distancia a sus vecinos.
- En el momento *t2*, **y** recibe la actualización de **z** y actualiza su vector de distancia. Los costos mínimos de **y** no cambian y, por lo tanto, **y** no envía ningún mensaje a **z**. El algoritmo llega a un estado de reposo.

b.i)
Consideremos ahora lo que puede suceder cuando aumenta el costo de un enlace. Supongamos que el costo del enlace entre **x** e **y** aumenta de 4 a 60, como se muestra en la figura.



1. Antes de que cambie el costo del enlace, Dy(x) = 4, Dy(z) = 1, Dz(y) = 1 y Dz(x) = 5.
En el momento *t0*, **y** detecta el cambio en el costo del enlace (el costo ha cambiado de 4 a 60). **y** calcula su nueva ruta de costo mínimo a **x** para que tenga un costo de
Dy(x) = min{c(y,x) + Dx(x), c(y,z) + Dz(x)} = min{60 + 0, 1 + 5} = 6
Por supuesto, con nuestra visión global de la red, podemos ver que este nuevo costo a través de **z** es incorrecto. Pero la única información que tiene el nodo y es que su costo directo para **x** es 60 y que **z** le ha dicho a **y** que **z** podría llegar a **x** con un costo de 5. Entonces, para llegar a **x**, **y** ahora pasaría por **z**, esperando que **z** pueda llegar a **x** con un costo de 5. A partir de *t1* tenemos un bucle de enrutamiento: para llegar a **x**, **y** pasa por **z** y **z** pasa por **y**.

2. Dado que el nodo **y** ha calculado un nuevo costo mínimo para **x**, informa a **z** de su nuevo vector de distancia en el momento *t1*.

3. Algún tiempo después de *t1*, **z** recibe el nuevo vector de distancia de **y**, que indica que el costo mínimo de **y** para **x** es 6. **z** sabe que puede llegar a **y** con un costo de 1 y, por lo tanto, calcula un nuevo costo mínimo para **x** de Dz(x) = min{50 + 0,1 + 6} = 7. Como el costo mínimo de **z** para **x** ha aumentado, entonces informa a **y** de su nuevo vector de distancia en *t2*.

4. De manera similar, después de recibir el nuevo vector de distancia de **z**, **y** determina Dy(x) = 8 y envía a **z** su vector de distancia. Luego, **z** determina Dz(x) = 9 y envía a **y** su vector de distancia, y así sucesivamente.

Este intercambio persistirá durante 44 iteraciones, hasta que **z** finalmente calcule que el costo de su ruta a través de **y** es mayor que 50. En este punto, **z** determinará que su ruta de menor costo a **x** es a través de su conexión directa a **x**.

Este problema se conoce como el problema de conteo a infinito.

Pregunta 4 (8 puntos)

a) Explique los conceptos de dominio de broadcast y dominio de colisión en redes Ethernet.
b) Dadas dos subredes A y B separadas por un router, ¿es posible hacer una consulta ARP desde un nodo de A a uno de B? Justifique su respuesta señalando las tramas intercambiadas si es necesario.

Solución

a)
Un dominio de broadcast es una subred donde todos los nodos pueden recibir una trama dirigida a la dirección de broadcast FF:FF:FF:FF:FF:FF. Esta subred puede estar compuesta de múltiples switches y otros dispositivos de capa de enlace.

Un dominio de colisión es un medio donde las tramas de los terminales pueden colisionar, por ejemplo un cable de un switch, o terminales conectadas a un hub.

b)
Las subredes están separadas por un dispositivo de capa 3, por lo tanto no es posible hacer una consulta ARP desde un nodo de la subred A a uno de la subred B, ya que ARP tiene alcance de una subred o Red de Área Local (LAN).

Problemas Prácticos

Problema 1 (30 puntos)

Suponga que deseamos disponer de un protocolo de transporte confiable de tipo *stop&wait* pero que envíe mensajes de dos en dos. Es decir, el emisor enviará una pareja de mensajes y enviará la siguiente pareja de mensajes solo cuando sepa que los dos mensajes de la primera pareja se han recibido correctamente. El emisor debe esperar hasta contar con ambos mensajes antes de enviarlos.
Suponga que el canal puede perder y corromper mensajes pero no reordenarlos.

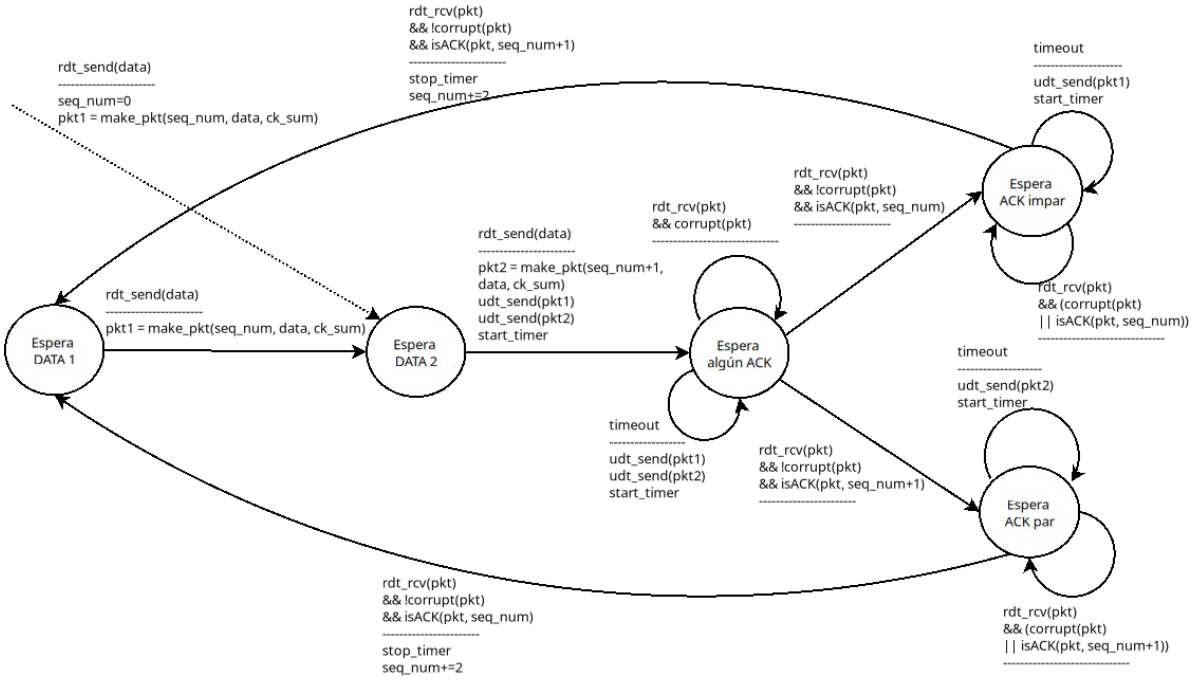
Se pide:
Diseñe el protocolo para un servicio de transferencia de mensajes fiable y unidireccional. Proporcione una descripción de las máquinas de estados del emisor y del receptor. Describa el formato de los paquetes intercambiados por el emisor y el receptor.

Nota: Si utiliza alguna llamada a procedimiento distinta de las empleadas en el curso (por ejemplo, `udt_enviar()`, `iniciar_temporizador()`, `rdt_recibir()`, etc.), defina claramente las acciones que realizan. Puede utilizar una variable global que mantenga los números de secuencia pero cualquier otra variable que utilice debe justificarla adecuadamente.

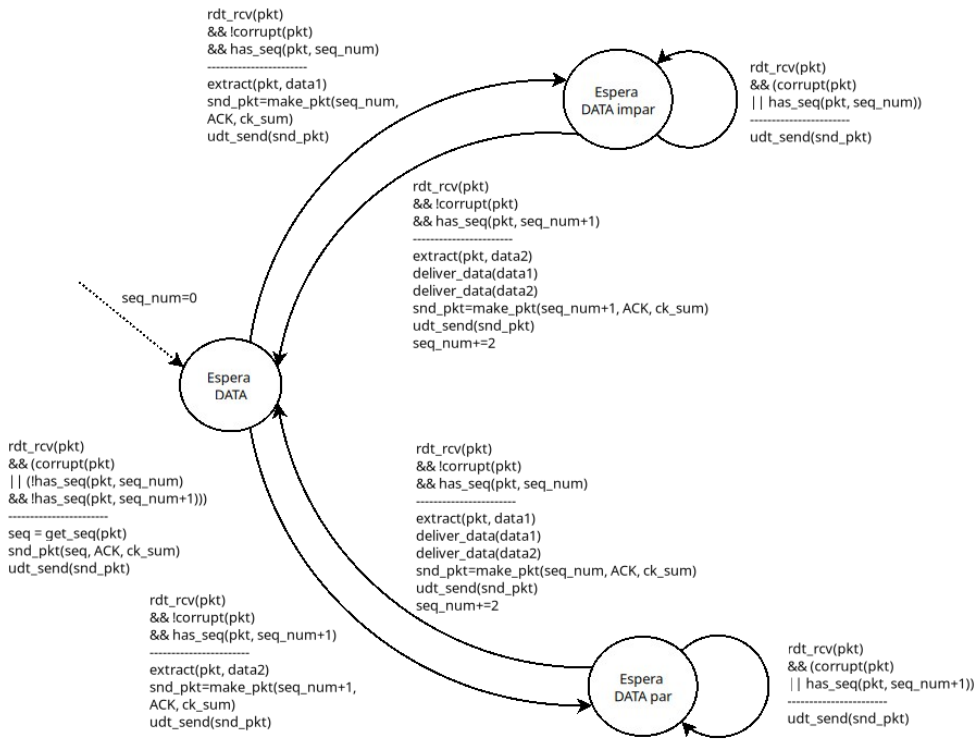
Solución

Existen dos soluciones posibles, ambas igual de válidas. En un caso se envía y espera por un ACK por cada paquete de datos (solución “a la Selective Repeat”) mientras que en la otra se envía un ACK solo cuando se recibieron ambos datos (solución “a la Go Back N”). Se presentan ambas soluciones.

Solución 1, tipo Selective Repeat

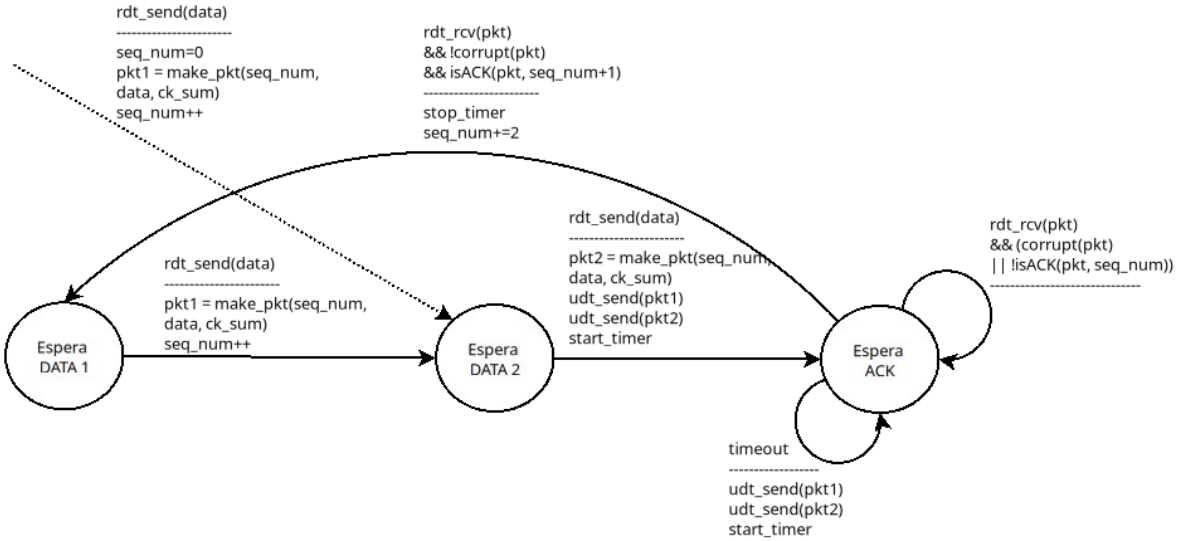


Emisor

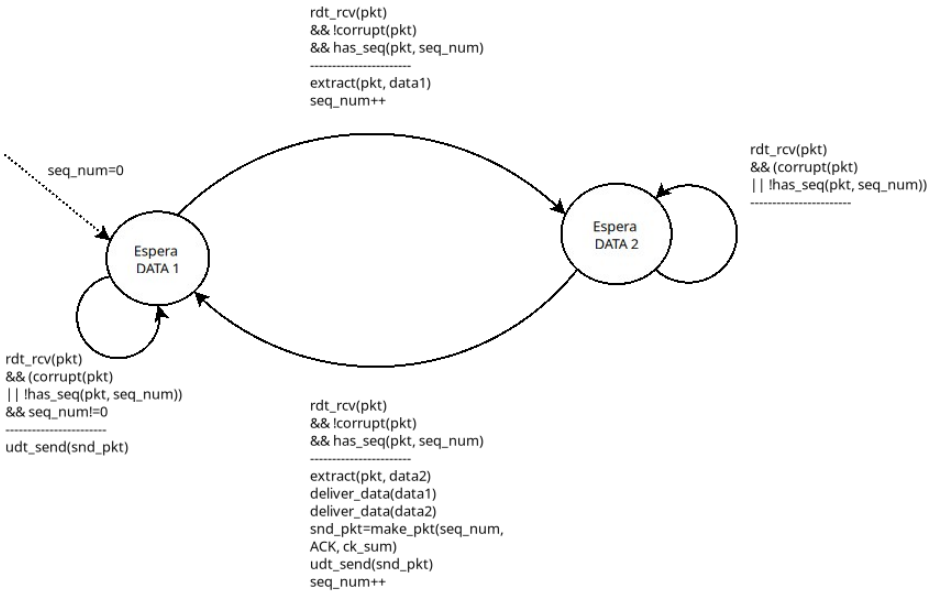


Receptor

Solución 2, tipo Go Back N



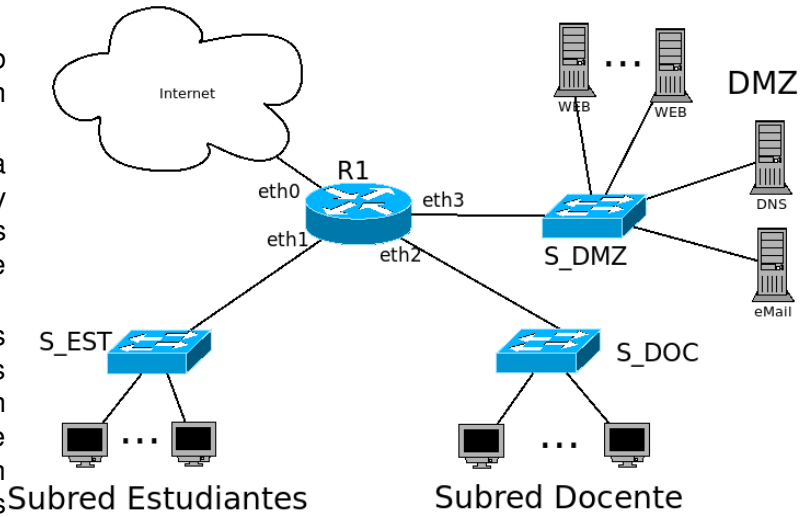
Emisor



Receptor

Problema 2 (30 puntos)

Se desea implementar la red de una institución educativa, que cuenta con 3 subredes: 1) la DMZ implementada con IPs públicas del prefijo 200.200.200.0/29, que incluye un servidor DNS, un servidor de correo, y varios servidores web, 2) subred para los docentes con 60 sistemas finales, y 3) una subred para estudiantes con 126 sistemas finales. Se cuenta con un router R1 con conexión a Internet a través de un enlace donde la dirección IP del router proveedor de internet es IP_GW.
La arquitectura de la red institucional se muestra en la siguiente figura:



Se pide:

a) ¿Cuántos servidores web diferentes se pueden conectar con los recursos disponibles?

b) Asigne prefijos de direcciones IP a las subredes de docentes y estudiantes, utilizando las máscaras de subred que más se ajusten a las necesidades.

c) Asigne direcciones IP a las interfaces de R1, e indique las tablas de forwarding de R1, de un servidor de la DMZ, de un host de la subred de estudiantes, y de un host de la subred de docentes para que se cumpla:

   i) La DMZ tiene acceso y puede ser accedida desde Internet.

   ii) Las subredes de estudiantes y docentes pueden acceder a Internet, pero no se pueden iniciar comunicaciones hacia sistemas en estas subredes desde Internet. Indique si es necesaria alguna configuración adicional en R1 para cumplir este requisito.

   Con esta configuración, ¿es posible iniciar comunicaciones desde la DMZ hacia sistemas en las subredes de docentes y estudiantes?

d) ¿Qué modificaciones se deben introducir si se requiere que sistemas de la subred de estudiantes se puedan conectar físicamente a S_DOC y de docentes a S_EST, manteniendo las restricciones de conectividad? Mencione las modificaciones necesarias para cada dispositivo relevante (switches, router).

Solución

a)
La DMZ tiene asignado el prefijo 200.200.200.0/29, es decir que soporta hasta 6 terminales, incluyendo la interfaz del router, lo que deja 5 direcciones IP útiles para servidores. Dado que se ocupan dos con los servidores de DNS y correo, se pueden conectar hasta tres servidores web.

b)
Para estas subredes vamos a utilizar direcciones privadas.

La subred para los docentes tiene hasta 60 sistemas finales, a los que debemos sumar la interfaz del router. Por lo tanto necesitamos un prefijo /26, por ejemplo 10.0.1.0/26
La subred para estudiantes tiene hasta 126 sistemas finales, a los que debemos sumar la interfaz del router. No alcanza con un prefijo /25 ya que si bien tiene 128 direcciones, debemos restar la dirección de red y la de broadcast, quedando 126 direcciones utilizables, pero necesitamos 127. Por lo tanto necesitamos un prefijo /24, por ejemplo 10.0.2.0/24.

c)
Interfaces de R1:

eth0: IP_LINK
eth1: 10.0.1.1
eth2: 10.0.2.1
eth3: 200.200.200.1

Tabla de forwarding de R1:

PREFIJO	NEXT-HOP	INTERFAZ
200.200.200.0/29	DC	eth3
10.0.1.0/26	DC	eth2
10.0.2.0/24	DC	eth1
subred_LINK/30	DC	eth0
0.0.0.0/0	IP_GW	eth0

Tabla de forwarding de servidor en la DMZ:

PREFIJO	NEXT-HOP	INTERFAZ
200.200.200.0/29	DC	eth0
0.0.0.0/0	200.200.200.1	eth0

Tabla de forwarding de sistema final en Subred Estudiantes:

PREFIJO	NEXT-HOP	INTERFAZ
10.0.2.0/24	DC	eth0
0.0.0.0/0	10.0.2.1	eth0

Tabla de forwarding de sistema final en Subred Docentes:

PREFIJO	NEXT-HOP	INTERFAZ
10.0.1.0/26	DC	eth0
0.0.0.0/0	10.0.1.1	eth0

Se cumple la regla i) porque la DMZ tiene direcciones IP públicas.
En cuanto a la regla ii), la numeración privada no permite iniciar conexiones desde Internet hacias las subredes de estudiantes y docentes. Para que los sistemas finales de estas subredes puedan conectarse a Internet se debe implementar NAT en R1, donde la dirección IP pública que se utiliza es la del enlace de R1 con Internet, que denominamos IP_LINK (eth0).

En cuanto a la posibilidad de iniciar conexiones desde la DMZ hacia sistemas en las subredes de docentes y estudiantes, la respuesta está en la tabla de forwarding de R1. Los servidores de la DMZ pueden iniciar comunicaciones hacia cualquier red hacia la que R1 pueda reenviar paquetes. Dado que R1 puede reenviar paquetes hacia las subredes con direccionamiento privado (ver la tabla de forwarding), entonces la respuesta es afirmativa: es posible iniciar comunicaciones desde la DMZ hacia sistemas en las subredes de docentes y estudiantes.

Notar que las direcciones IP privadas solo están restringidas FUERA de la propia red (podría ser un AS entero), pero que dentro de la red, son direcciones IP alcanzables como cualquiera.

d)

Para que más de una subred se pueda conectar en el mismo dispositivo físico (switch), se necesita la tecnología de VLANs (Virtual LANs), es decir, soporte del estándar 802.1Q. Esto permite que los puertos de los switches pertenezcan a cualquiera de la VLAN definidas.

Además, para mantener las restricciones de conectividad, el router R1 debe implementar también el estándar de VLANs. La conectividad física se debe modificar, conectando uno solo de los switches mediante un trunk a R1, que debe configurar dos sub-interfaces con direcciones IP de c/u de las subredes.

Además, los switches se deben conectar entre sí mediante un trunk.