Solución Examen – 27 de febrero de 2021

Nota
El examen se tomó en modalidad virtual a través de la plataforma EVA.
Consistió de tres partes, la primera de 40 minutos y las siguientes de 35 minutos. Cada parte estuvo separada por un descanso de 5 minutos.
La primera parte consistió en 5 preguntas de un set de preguntas que se sortearon de forma aleatoria para cada estudiante.
Las partes 2 y 3, consistieron en ejercicios también con diferentes versiones. Este documento contiene solo una de estas versiones para cada parte.

Parte 1

Pregunta 1 (8 puntos)

V1
Un técnico de una empresa recibe el siguiente reclamo de uno de sus clientes: “el portal web de vuestra empresa está caído”. Para diagnosticar la situación el técnico decide ejecutar en su computadora un ping basado en ICMP dirigido a la dirección IP del servidor web de la empresa, y en función de la respuesta, determinar si es correcta la afirmación del cliente, o no.

a) Analice la decisión del técnico y corríjala si corresponde.
b) ¿Se modifica su respuesta de la parte anterior si el ping está basado en UDP? Justifique.

Solución V1

a) La decisión del técnico de la empresa respecto a cómo probar el correcto funcionamiento del portal web no es correcta, pues a través de dicho comando intentará verificar la conectividad en Capa de Red, la que sea exitosa o no, nada se podrá concluir respecto al servicio: si es exitosa, ello no permite afirmar que el tráfico de una conexión http (o https) con dicho servidor pueda viajar entre el cliente y el servidor; si fracasa, las razones pueden ser diversas (por ejemplo debido a que los mensajes ICMP asociados al comando PING, concretamente los tipos Echo y Echo Reply, estén filtrados, e igualmente es posible que el tráfico “web” se esté cursando correctamente por la red.
Un análisis más adecuado de la situación debería involucrar analizar qué ocurre cuando se intercambia tráfico “web” (http y/o https) con el servidor referido, e incluso también el tráfico de Capa de Transporte asociado (por defecto, aquel tráfico TCP que involucra el puerto 80 y/o el puerto 443 del servidor). Para ello, diferentes acciones se pueden tomar:

- “Sniffear” el tráfico TCP hacia/desde los puertos 80 y 443 del servidor.
- “Sniffear” el tráfico http y https hacia/desde el servidor.
- Generar tráfico hacia los puertos TCP 80 y 443, y analizar las respuestas. Se puede combinar con la primera.
- Generar tráfico http y https y analizar las respuestas. Se puede combinar con la primera y la segunda.
- Observar el comportamiento de un cliente (browser) al momento de intentar cargar el contenido web desde el servidor.
- Considerar en todas las acciones anteriores cuál es el otro extremo de la conexión.
- De ser posible, analizar la situación del propio servidor: servicio web levantado, conectividad, estado de las conexiones al servidor, etc.

b) No, no se modifica. Su esencia es la misma. Con dicha prueba (ICMP basado en UDP) nada se puede concluir respecto al funcionamiento del servidor web. La justificación a plasmar aquí es la misma que se incluyó en la parte a).

V2

Un técnico de una empresa recibe el siguiente reclamo de uno de sus clientes: “el servicio DNS de vuestra empresa está caído”. Para diagnosticar la situación el técnico decide ejecutar en su computadora un ping basado en ICMP dirigido a la dirección IP del servidor DNS de la empresa, y en función de la respuesta, determinar si es correcta la afirmación del cliente, o no.

a) Analice la decisión del técnico y corríjala si corresponde.

b) ¿Se modifica su respuesta de la parte anterior si el ping está basado en UDP? Justifique.

Solución V2

a) La decisión del técnico de la empresa respecto a cómo probar el correcto funcionamiento del portal web no es correcta, pues a través de dicho comando intentará verificar la conectividad en Capa de Red, la que sea exitosa o no, nada se podrá concluir respecto al servicio: si es exitosa, ello no permite afirmar que el tráfico vinculado al servicio DNS con dicho servidor pueda viajar entre el cliente y el servidor; si fracasa, las razones pueden ser diversas (por ejemplo debido a que los mensajes ICMP asociados al comando PING, concretamente los tipos Echo y Echo Reply, estén filtrados, e igualmente es posible que el tráfico “DNS” se esté cursando correctamente por la red.

Un análisis más adecuado de la situación debería involucrar analizar qué ocurre cuando se intercambia tráfico “DNS” (fundamentalmente vía UDP al puerto 53, pero también vía TCP al mismo puerto) con el servidor referido, e incluso también el tráfico de Capa de Transporte asociado (por defecto, aquel tráfico TCP que involucra el puerto 53). Para ello, diferentes acciones se pueden tomar:

- “Sniffear” el tráfico hacia/desde los puertos UDP 53 y TCP 53 del servidor.
- “Sniffear” el tráfico DNS hacia/desde el servidor.
- Generar tráfico hacia los puertos UDP 53 y TCP 53, y analizar las respuestas. Se puede combinar con la primera.
- Generar consultas de DNS dirigidas al servidor, y analizar las respuestas. Se puede combinar con la primera y la segunda.
- Utilizar herramientas de diagnóstico específicas del servicio en cuestión (dig, nslookup), generar diferentes tipos de consultas y analizar las respuestas. Se puede combinar con las 2 primeras.
- Considerar en todas las acciones anteriores desde dónde se generan las queries.
- De ser posible, analizar la situación del propio servidor: servicio DNS levantado, conectividad, estado de las consultas al servidor, registros disponibles, estado del cache, etc.

b) No, no se modifica. Su esencia es la misma. Con dicha prueba (ICMP basado en UDP) nada se puede concluir respecto al funcionamiento del servidor DNS. La justificación a plasmar aquí es la misma que se incluyó en la parte a).

Pregunta 2 (8 puntos)

V1

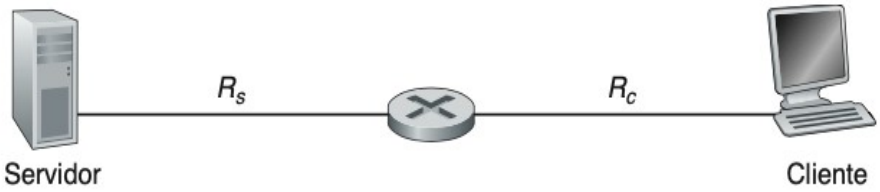
Teniendo en cuenta el escenario planteado en la figura y tomando a Ri como la velocidad del link i responda las siguientes cuestiones:

a) ¿Cuál sería la tasa de transferencia media de cierto archivo del Servidor al Cliente?

b) Plantee un escenario para que el router introduzca un retardo de cola a los paquetes.

c) Suponiendo que las colas del router son infinitas y conociendo la velocidad media a la que llegan los paquetes a la cola ¿que se tiene que cumplir para que el retardo de cola

tienda a infinito?



Solución V1

a) La tasa de transferencia de un archivo va a depender de cuanto tarde el archivo en ser recepcionado completamente. Esto incluye no solo el retardo de transmisión dado por Rs y Rc sino también de los retardos de cola, propagación y procesamiento que se puedan introducir. Por lo tanto, si la transferencia dura T segundos (incluyendo todos los retardos) hasta que el host B recibe el archivo y el archivo consta de F bits, la tasa media de transferencia del archivo será de F/T bits/segundo.
Un análisis correcto pero incompleto, consiste en considerar solo el retardo de transmisión, en este caso la tasa de transferencia será el mínimo entre Rs y Rc.

b) Si la velocidad de transmisión del servidor sobre el enlace con el router es considerablemente mayor que la velocidad de transmisión del router en el enlace con el cliente (Rs>>Rc), se van a estar encolando paquetes. Por lo tanto va a existir un retardo de cola en el router para los paquetes que viajan del servidor al cliente.

c) Sea *a* la velocidad media a la que llegan los paquetes a la cola (paquetes/segundo). *R* es la velocidad de transmisión; es decir, es la velocidad (en bits/segundo) a la que los bits salen de la cola. Supongamos también que todos los paquetes constan de *L* bits. Entonces, la velocidad media a la que llegan los bits a la cola es igual a *La* bits/segundo. Dado que la cola es infinita, el cociente *La/R*, determina la intensidad de tráfico. Si $La/R > 1$, entonces la velocidad media a la que los bits llegan a la cola excede la velocidad a la que los bits pueden ser transmitidos desde la cola. En esta situación, la cola tenderá a aumentar sin límite y el retardo de cola se aproximará a infinito.

V2

Imagine que dos endpoints A y B tienen una conexión TCP a través de una red con alta redundancia de caminos posibles para alcanzar uno a otro. Además, estos caminos cuentan con diferentes rendimientos en cuanto a throughput y latencia.

a) ¿Puede generar algún inconveniente en la conexión que al receptor TCP le lleguen paquetes de la misma conexión por muchas rutas diferentes?
b) ¿De qué manera regula el emisor su velocidad de transmisión para evitar congestionar la red? Describa detalladamente.

Solución V2

a) Bajo el supuesto que se utilizan los múltiples caminos en el forwarding, el receptor TCP podría recibir los segmentos en desorden. Esto produciría que el receptor pase demasiado tiempo reordenando los paquetes; además, debido a las diferencias en los rendimientos de los caminos y posibles retardos, el emisor estaría enviando retransmisiones innecesarias, lo que llevaría a una creciente congestión en la red.

b) El emisor TCP regula su velocidad de transmisión utilizando el control de congestión que brinda TCP. Este método consiste en que cada emisor limite la velocidad a la que transmite el tráfico a través de su conexión en función de la congestión de red percibida. Si un emisor TCP

percibe que en la ruta entre él mismo y el destino apenas existe congestión, entonces incrementará su velocidad de transmisión; por el contrario, si el emisor percibe que existe congestión a lo largo de la ruta, entonces reducirá su velocidad de transmisión. Para esto hace un seguimiento de la variable ventana de congestión. Esta ventana, indicada como VentCongestion, impone una restricción sobre la velocidad a la que el emisor TCP puede enviar tráfico a la red. Específicamente, la cantidad de datos no reconocidos en un emisor no puede exceder el mínimo de entre VentCongestion y VentRecepcion, es decir: UltimoByteEnviado – UltimoByteReconocido min{VentCongestion, VentRecepcion}

V3

Para los protocolos pipelined con esquema GBN (Go-Back-N) y SR (Selective Repeat) conteste y justifique las siguientes preguntas:

a) Para cada esquema con una ventana de tamaño N, ¿cuántos paquetes sin ser reconocidos puede enviar el sender?
b) Suponiendo una ventana de tamaño 8 (0..7), y que se han enviado y aceptado los 2 primeros mensajes, para cada esquema: ¿Qué identificador tiene el último paquete reconocido en cada esquema?, ¿Qué identificador tiene el próximo paquete esperado? ¿Qué identificadores puede enviar sin recibir aceptación? Justifique sus respuestas.
c) Para cada esquema, ¿cuál es el máximo valor aceptable para N en caso de representar el número de secuencia con 8 bits?

Solución V3

a) Para ambos casos se pueden enviar hasta N paquetes sin ser reconocidos. Esta es la definición de ventana deslizante de estos protocolos.

b) Si se considera un tamaño de ventana de 8 (como dice la letra), para ambos casos, el último identificador reconocido es 1. Se espera el identificador con 2. El envío sin recibir reconocimiento son los números de secuencia 2, 3 ,4 ,5 ,6, 7, 0, 1

Sin embargo, como los números de secuencia disponibles son de 0 a 7, también son válidas respuestas que tengan en cuenta esto y decidan usar una ventana mas chica.

c) Para el protocolo Go-Back-N visto en el curso (donde no se almacenan en el buffer del receptor los paquetes fuera de orden), se puede utilizar una ventana de tamaño k-1 paquetes (donde k es la cantidad de números de secuencia distintos). De esta forma se evita que el receptor pueda confundir un paquete nuevo con una retransmisión en el caso de que se pierdan todos los ACKs de una ventana. Por lo tanto, con 8 bits se puede representar entre 0 y 255, por lo que k corresponde a 256 (diferentes valores posibles), entonces el tamaño de ventana máximo es 255.

Para SR se puede utilizar una ventana de tamaño parte_entera(k/2) paquetes (donde k es la cantidad de números de secuencia distintos). De esta forma se evita que en caso de perderse todos los ACK de una transmisión, las ventanas del emisor y receptor se superpongan produciendo que el receptor confunda un nuevo paquete con una retransmisión (dilema del receptor). Por lo tanto, con 8 bits se puede representar entre 0 y 255, por lo que k corresponde a 256 (diferentes valores posibles), entonces el tamaño de ventana máximo es 128.

Pregunta 3 (8 puntos)

V1

Imagine que accede a su correo electrónico utilizando POP3.

a) Suponga que un cliente de correo POP desea descargar y luego eliminar los mensajes. Complete la siguiente transacción entre el cliente y el servidor:

C: list
S: 1 498
S: 2 912
S: .
C: retr 1
S: bla bla ...
S: .....bla
S: .
???

b) Suponga que un cliente de correo POP desea descargar y guardar los mensajes. Complete la siguiente transacción entre el cliente y el servidor:

C: list
S: 1 498
S: 2 912
S: .
C: retr 1
S: bla bla ...
S: .....bla
S: .
???

c) Suponga que luego de la transacción del apartado anterior el cliente se desconecta y cinco minutos más tarde vuelve a acceder otra vez a POP. Suponga que en ese intervalo de cinco minutos ha recibido un nuevo mensaje de correo que el cliente desea recuperar. Proporcione una transcripción de esta segunda sesión de POP.

Solución V1

a)
C:dele 1
C:retr 2
S:(blah blah …
S:.....blah)
S:.
C:dele 2
C:quit
S:+OK POP3 server signing off

b)
C:retr 2
S:blah blah …
S:.....blah
S:.
C:quit
S:+OK POP3 server signing off

c)
C: list
S: 1 498
S: 2 912
S: 3 968

S: .
C: retr 3
S: bla bla ...
S: .....bla
S: .
C:quit
S:+OK POP3 server signing off

V2

Dada la jerarquía de DNS mostrada en la figura, y suponiendo que no existe información en el cache, indique, de forma detallada, todas las consultas realizadas por el DNS local para resolver el registro A del dominio gaia.umass.edu. El DNS local realiza las consultas de forma iterativa.

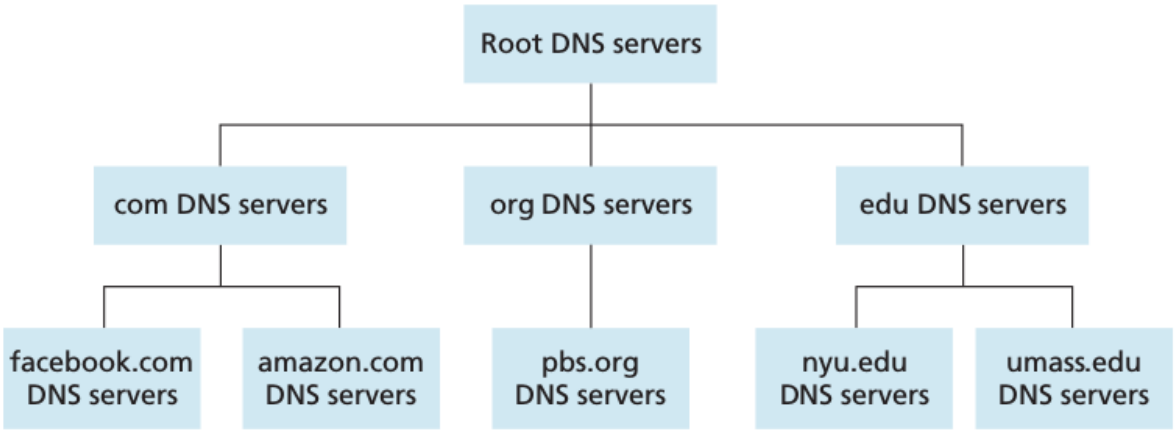


Figure 2.17 ♦ Portion of the hierarchy of DNS servers

Solución V2

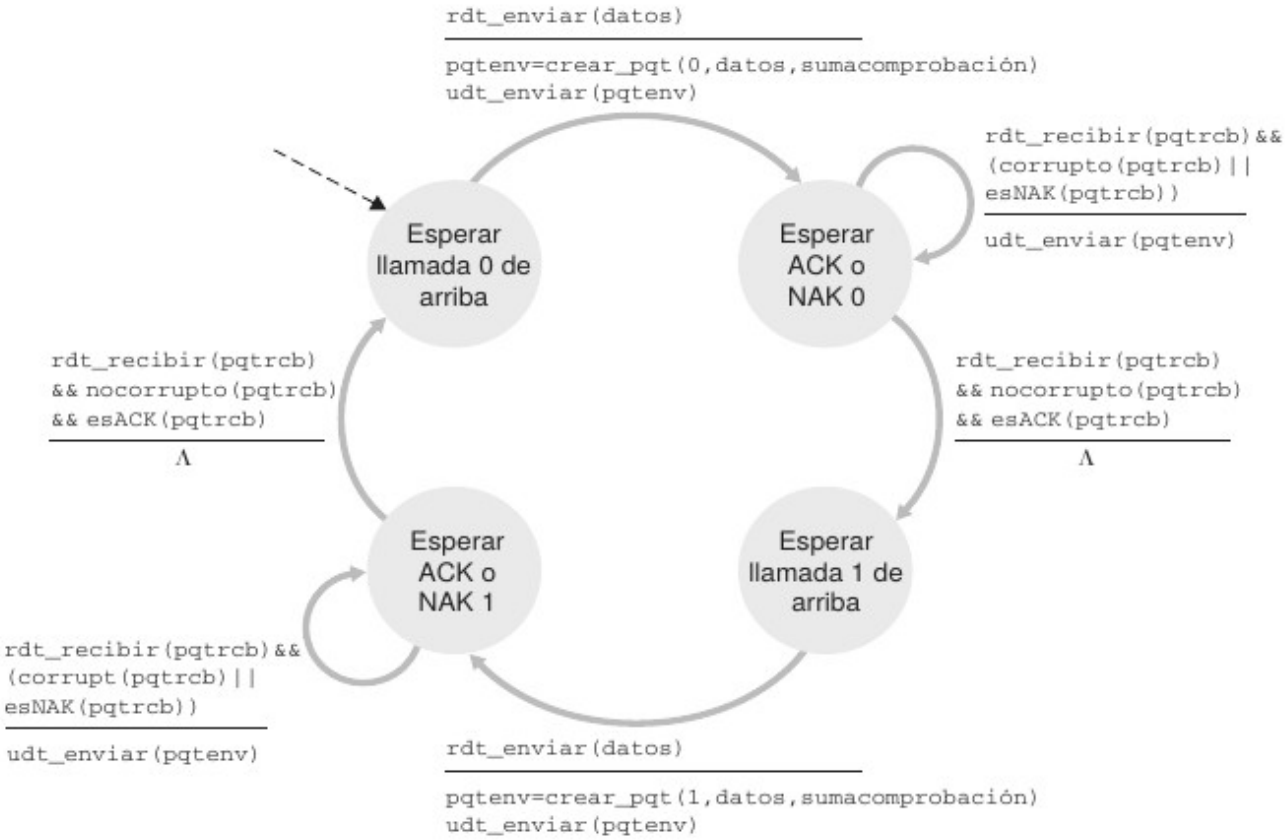
Los mensajes de consulta contienen el nombre de host a traducir, y tipo A para el caso, gaia.umass.edu.
1- El servidor DNS local reenvía el mensaje de consulta a un servidor DNS raíz.
2- El servidor DNS raíz toma nota del sufijo edu y devuelve al servidor al DNS local una lista de direcciones IP para los servidores TLD responsables para edu. La respuesta contiene registros NS. En caso de no contener los registros A de los NS devueltos. Debe hacerse la consulta de los mismos.
3- El servidor DNS local reenvía el mensaje de consulta a uno de estos TLD servidores.
4- El servidor de TLD toma nota del sufijo umass.edu y responde con la dirección IP del servidor DNS autorizado de umass, por ejemplo, dns.umass.edu. La respuesta contiene registros NS. En caso de no contener los registros A de los NS devueltos. Debe hacerse la consulta de los mismos.
5- Finalmente, el servidor DNS local reenvía el mensaje de consulta directamente a dns.umass.edu, que responde con la dirección IP de gaia.umass.edu.

Pregunta 4 (8 puntos)

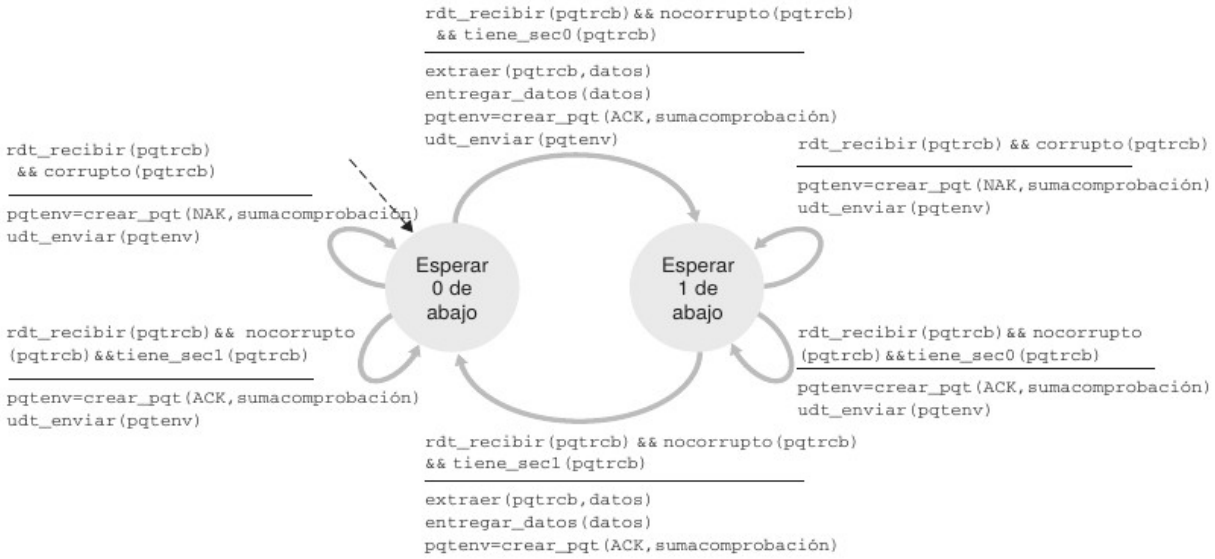
V1

Dada la máquina de estados de la figura, que representa un protocolo de transferencia confiable, se pide:
a) Indique el comportamiento en caso de recibir un mensaje de datos corruptos y un mensaje de ACK/NACK corrupto.
b) Indique ventajas y desventajas del protocolo.
c) ¿Este protocolo soporta pérdida de mensajes? Justifique

EMISOR:



RECEPTOR:



Solución V1

a) Caso de mensaje de datos corrupto: el receptor envía un NACK, lo que genera el envío nuevamente del paquete.
En caso de mensaje ACK o NACK corrupto, el emisor repite el envío y el receptor repite el envío del ACK

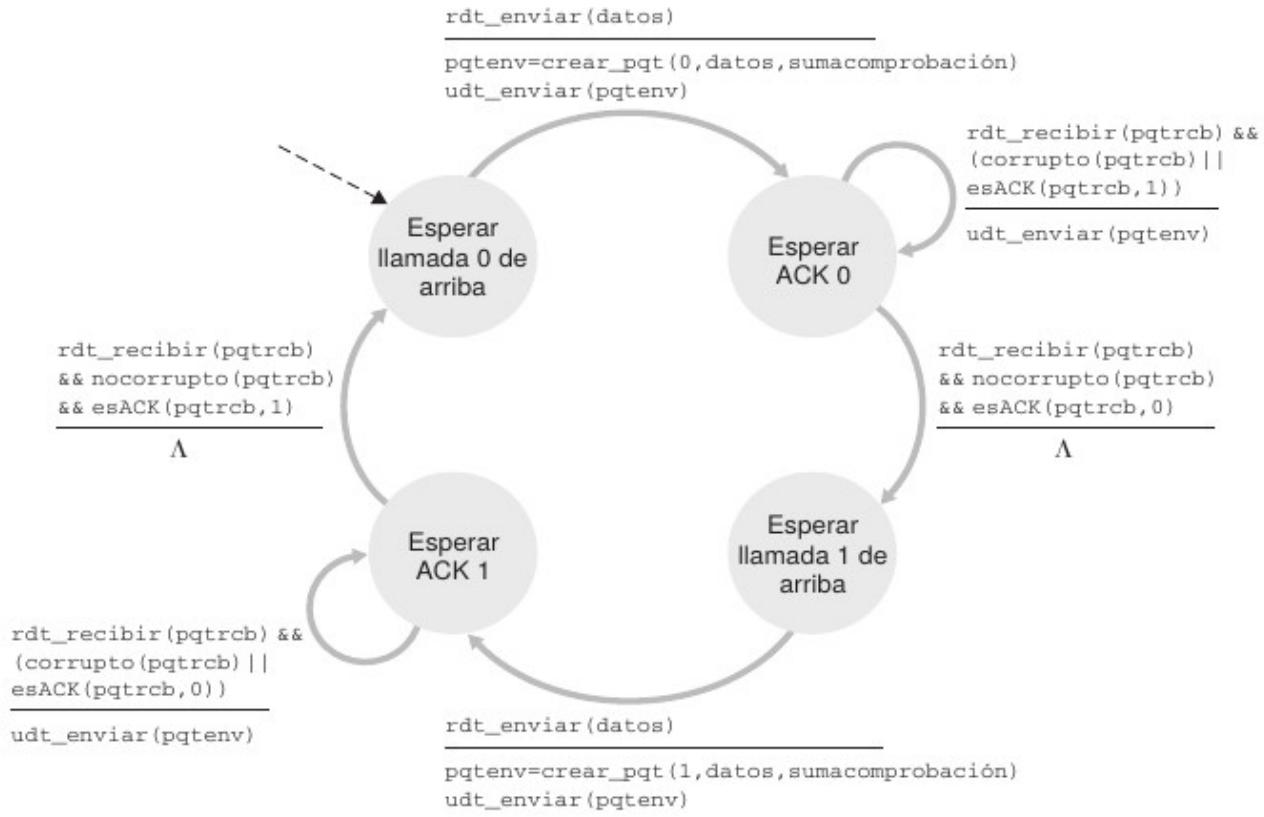
b)Ventajas:
-Plantea solución para el caso de que los paquetes de datos y de control llegan corruptos.
-Mediante el nro. de secuencia le permite al receptor detectar duplicados de paquetes.

Desventajas:
-Es un protocolo Stop-and-Wait, mientras espera por paquetes ACK o NACK, no puede recibir llamadas de la capa superior y por lo tanto no envía nuevos datos hasta asegurarse de que el paquete emitido llegó correctamente.
-Se asume que todos los paquetes se reciben y en el orden en que fueron enviados

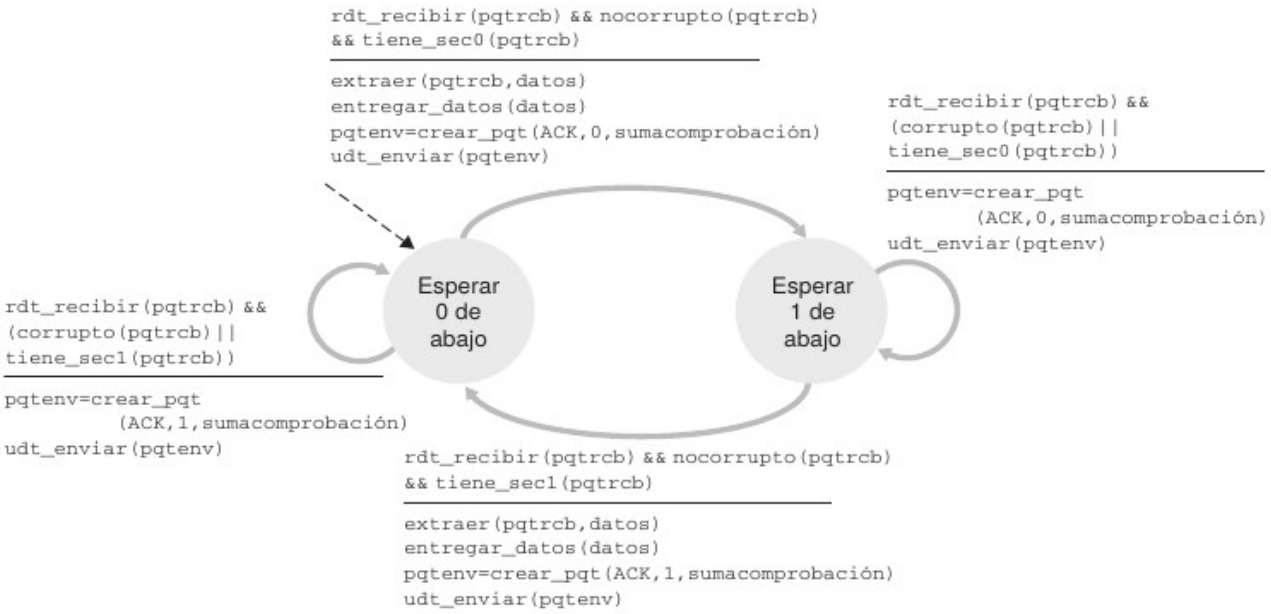
c) No soporta, dado que en caso de pérdida de ACK, no reenvía el dato.

V2
Dada la máquina de estados de la figura, que representa un protocolo de transferencia confiable, se pide:
a) Indique el comportamiento en caso de recibir un mensaje de datos corruptos y un mensaje de ACK corrupto.
b) Indique ventajas y desventajas del protocolo.
c) ¿Este protocolo soporta pérdida de mensajes? Justifique

EMISOR:



RECEPTOR:



Solución V2

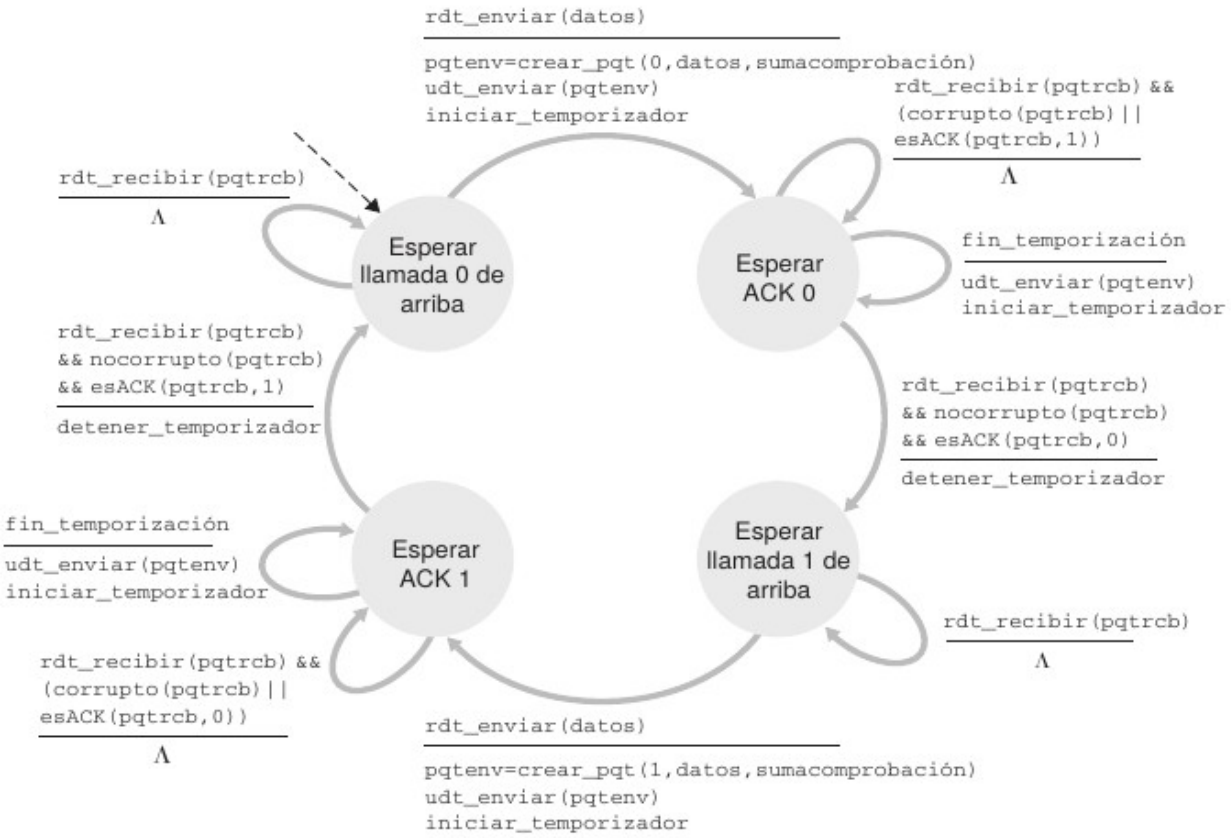
a) Caso de mensaje de datos corrupto: el receptor envía un ACK del número de secuencia anterior, lo que genera el envío nuevamente del paquete.
En caso de mensaje ACK corrupto, el emisor repite el envío y el receptor repite el envío del ACK

b)
Ventajas:
- Introduce la idea de nros de secuencia sobre todos los paquetes de datos y de control.
- Permite determinar si el receptor recibe un paquete nuevo o retransmitido, e identificar que el ACK[i] corresponde al paquete de dato SP[i]. Sin perder funcionalidad al reemplazar el mecanismo de NACK.

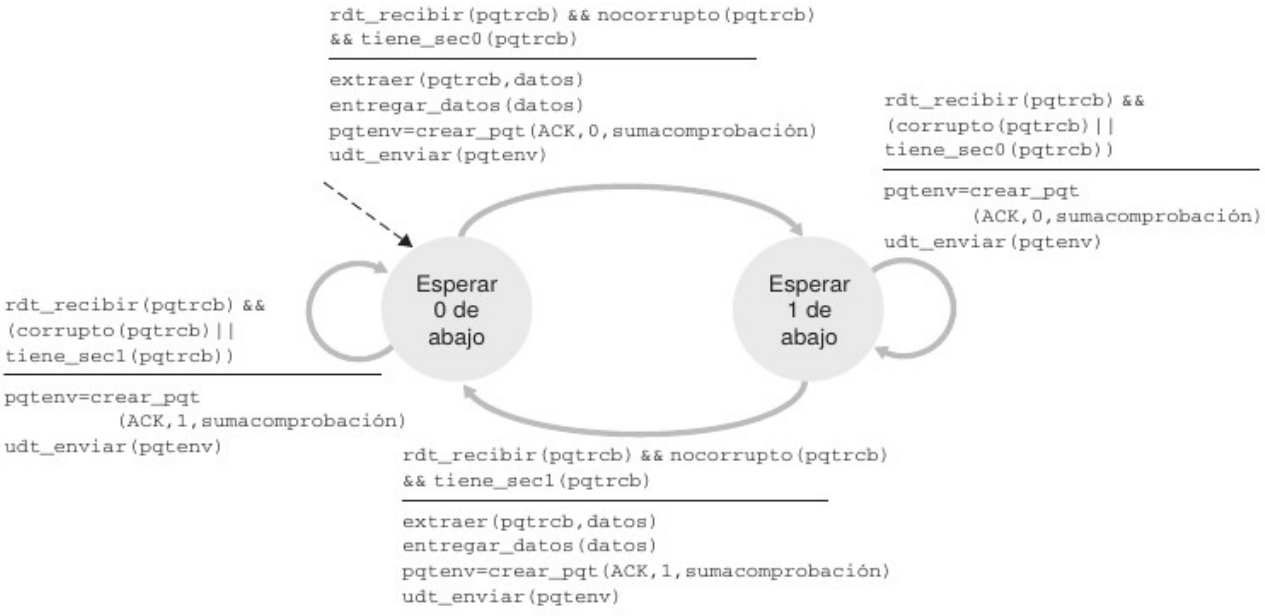
Desventajas:
- Es un protocolo Stop-and-Wait, mientras espera por paquetes ACK o NACK, no puede recibir llamadas de la capa superior y por lo tanto no envía nuevos datos hasta asegurarse de que el paquete emitido llegó correctamente.
- Se asume que todos los paquetes se reciben y en el orden en que fueron enviados.

c) No soporta, dado que en caso de pérdida de ACK, no reenvía el dato.

V3
Dada la máquina de estados de la figura, que representa un protocolo de transferencia confiable, se pide:
a) Indique el comportamiento en caso de recibir un mensaje de datos corruptos y un mensaje de ACK corrupto.
b) Indique ventajas y desventajas del protocolo.
c) ¿Este protocolo soporta pérdida de mensajes? Justifique
EMISOR:



RECEPTOR:



Solución V3

a) Caso de mensaje de datos corrupto: el receptor envía un ACK del número de secuencia anterior.
En caso de mensaje ACK corrupto, el emisor no hace nada con el objetivo que se venza el timer.

b)

Ventajas:

• Plantea una solución para un canal subyacente inseguro por pérdida de paquetes o paquetes corruptos.

• Introduce la idea del timer con un tiempo límite. El cuál debe ser calculado mediante probabilidad de pérdida.

Desventajas:

• Timers con límite de tiempo corto introducen duplicados de paquetes.

• Es un protocolo Stop-and-Wait. Es decir, mientras espera por paquetes ACK, no puede recibir llamadas de la capa superior y por lo tanto no envía nuevos datos hasta asegurarse de que el paquete emitido llegó correctamente. No tiene buen rendimiento

c) Soporta, dado que en caso de pérdida de ACK, tiene un timer que implementa el reenvío el dato y el receptor lo reconocerá como ya recibido.

Pregunta 5 (8 puntos)

V1

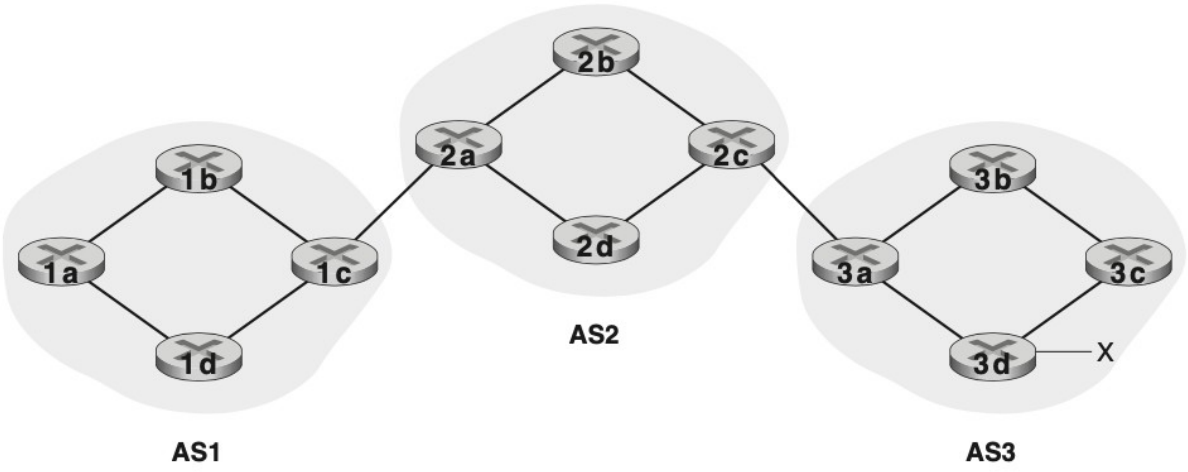
Suponga una red que cuenta con tres sistemas autónomos AS1, AS2 y AS3 como se muestra en la figura.

a) Plantee un escenario donde se utilicen sesiones iBGP y eBGP.

b) De un ejemplo de selección de ruta donde el enrutamiento de la “papa caliente” decida sobre dos rutas diferentes. Justifique.

c) Describa brevemente el funcionamiento de OSPF y compárelo con iBGP

Para los ejemplos puede incluir la infraestructura que desee.



Solución V1

a)

iBGP: el router borde 1c le distribuye el prefijo X con AS-PATH AS3-AS2-AS1 al router 1a

eBGP: el router borde 3a le anuncia el prefijo X con AS-PATH AS3 al router 2c

b) Para que la decisión del algoritmo de BGP utilice el enrutamiento de la papa caliente antes debió haber evaluado el valor de la preferencia local y la ruta de la secuencia de sistemas autónomos. Por este motivo las dos rutas deben tener el mismo valor de preferencia local y el mismo largo en la secuencia de ASs.

Un ejemplo sería el siguiente: imaginemos que existe ahora un enlace entre los routers 2d y 1d. Por lo tanto los routers 1b y 1a pueden llegar al prefijo X por los routers borde 1c y 1d.

Desde 1a se quiere enrutar un paquete con una ip destino en el rango X. Imaginemos que las preferencias locales son siempre las mismas, entonces 1a va a tener las rutas
LOCAL PREF 1 ; AS1-AS2-AS3 ; 1c
LOCAL PREF 1 ; AS1-AS2-AS3 ; 1d
que fueron aprendidas por iBGP. Como se puede observar ambas rutas tienen el mismo valor de preferencia local y el mismo largo en los AS PATHs, por lo tanto al aplicar el algoritmo de la papa caliente se va a quedar con la ruta que le ofrece el router borde 1d, pues 1d está a un salto mientras que 1d a dos.

c) OSPF es un protocolo de estado de enlaces que utiliza la técnica de inundación de información de estado de los enlaces y un algoritmo de la ruta de coste mínimo de Dijkstra. Con OSPF, un router construye un mapa topológico completo (es decir, un grafo) del sistema autónomo entero. A continuación, cada router ejecuta localmente el algoritmo de la ruta más corta de Dijkstra para determinar un árbol de rutas más cortas a todas las subredes, con él mismo como nodo raíz.
Mientras que OSPF resuelve el enrutamiento interno al sistema autónomo las sesiones iBGP son utilizadas para distribuir rutas externas al AS a los nodos internos.

V2

Sean las siguientes direcciones IP:

A. 0.0.0.0
B. 10.127.30.20
C. 127.0.0.1
D. 127.10.20.30
E. 172.10.20.30
F. 172.20.10.30
G. 217.30.20.10
H. 712.30.10.20

De acuerdo a lo visto en el curso, que se basa en el RFC 1918 - Address Allocation for Private Internets, donde se definen los espacios de direcciones privadas y el RFC 5735 - Special Use IPv4 Addresses, donde se definen las direcciones IP para usos especiales, para cada dirección usted deberá: indicar si es una dirección pública de internet, privada o reservada para otro uso. Brinde un ejemplo breve de en qué caso puede ser utilizada.

Solución V2

A. 0.0.0.0 – reservada.
B. 10.127.30.20 – privada. Puede ser usada para numerar un host en una LAN
C. 127.0.0.1 – reservada. Usada como dirección de loopback
D. 127.10.20.30 – reservada. Usada como dirección de loopback
E. 172.10.20.30 - pública. Puede ser usada para numerar un host en Internet (el prefijo privado es 172.16.0.0/12)
F. 172.20.10.30 - privada. Puede ser usada para numerar un host en una LAN
G. 217.30.20.10 - pública. Puede ser usada para numerar un host en Internet
H. 712.30.10.20 – dirección no válida

V3

a) Describa el mecanismo por el cual el switch utiliza las direcciones MAC mostradas en la figura para almacenarlas en una tabla.
b) Diseñe una prueba para poder demostrar esta funcionalidad del switch, partiendo de un escenario donde nunca existió comunicación en dicha red.

Solución V3

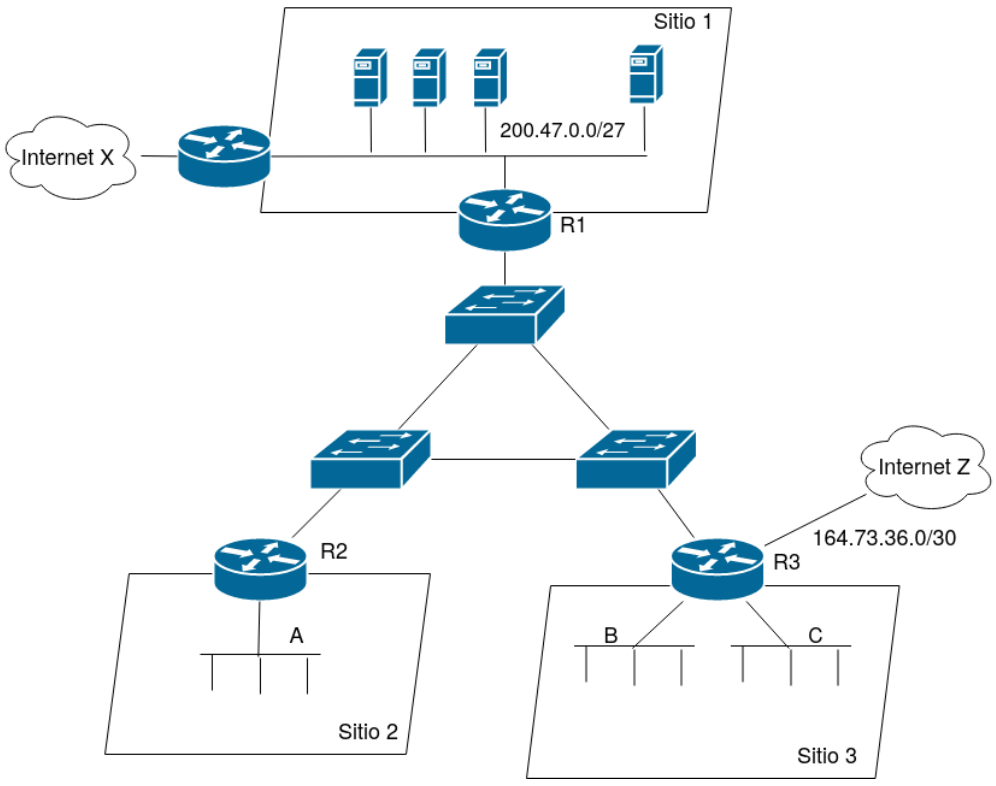
a) Los switches tienen la propiedad de que su tabla se construye de forma automática, dinámica y autónoma (auto-aprendizaje). Esta capacidad se lleva cabo de la forma siguiente:
1. Inicialmente, la tabla de conmutación está vacía
2. Para cada trama entrante recibida en una interfaz, el switch almacena en su tabla (1) la dirección MAC especificada en el campo dirección de origen de la trama, (2) la interfaz de la que procede la trama y (3) la hora actual. De esta forma, el switch registra en su tabla el segmento de la LAN en la que reside el emisor. Si todos los hosts de la LAN terminan enviando una trama, entonces todos los host terminarán estando registrados en la tabla.
3. El switch borra una dirección de la tabla si no se recibe ninguna trama con esa dirección como dirección de origen transcurrido un cierto periodo de tiempo (el tiempo de envejecimiento). De esta forma, si un PC es sustituido por otro (con un adaptador diferente), la dirección MAC del PC original será eliminada de la tabla de conmutación.

b) Una prueba para comprobar esta funcionalidad partiendo del escenario en cuestión es la siguiente:
1- Capturamos tramas en modo promiscuo en todas las interfaces mostradas en la figura, por ejemplo con tcpdump.
2- Enviamos una trama de uno de los hosts al router
3- Miramos las capturas
4- Enviamos una trama de respuesta (del router al host)
5- Miramos las capturas

En el punto 3 deberíamos observar que la trama llega a todos los demás host y al router, dado que el switch no tiene ninguna asociación MAC-puerto para dicha trama (por lo tanto lo envía por todas las bocas). Mientras que en punto 5, solo deberíamos observar la trama en el host destino, pues en el paso anterior el switch agregó la asociación MAC_HOST - PUERTO_HOST - TTL.

Parte 2 (30 puntos)

Suponga el siguiente esquema de red de una empresa que cuenta con empleados distribuidos en dos sitios remotos y organizados en tres departamentos: A, B y C.



A reside en un local propio (Sitio-2) y B y C comparten edificio (Sitio-3), pero están asignados en diferentes segmentos de red.
Además se cuenta con un tercer sitio (Sitio-1), donde residen los servidores de la empresa. La red de servidores tiene asignado un rango de direcciones IP públicas asignadas por el proveedor X. Las redes de los departamentos A, B y C son privadas con un rango definido por la propia empresa. Estas redes tienen acceso a Internet a través de una conexión ubicada en el Sitio-3 brindada por el proveedor Z.

El Departamento A cuenta con cincuenta y cinco (55) empleados, cada uno de los cuales dispone de un terminal de trabajo (PC) y un teléfono IP. Además, se instala una impresora de red cada cinco (5) puestos de trabajo.
El departamento B consta de treinta (30) empleados con los mismos requerimientos que A. Por último el departamento C solo tiene dos impresoras y seis empleados con PC más teléfono IP cada uno. Además, el departamento C requiere dieciséis (16) direcciones IP para numerar equipamiento de desarrollo y testing.

a) Proponga un plan de numeración para toda la red, indicando específicamente red/máscara en cada segmento.
b) Muestre cómo sería la tabla de forwarding de R2, R3 y un equipo del sitio 1 de forma que los departamentos A, B y C tengan conectividad entre sí, a los servidores alojados en el Sitio-1 y a Internet a través del proveedor Z. A los servidores se debe acceder a través de la red interna evitando hacerlo por Internet. Numere todas las interfaces necesarias para completar las tablas correctamente.
c) Indique mediante una tabla todos los paquetes intercambiados en la red cuando un host del departamento C realiza un ping a un servidor del Sitio-1. Asuma que todas las tablas dinámicas en todos los equipos están vacías. Para cada paquete debe indicar información de Capa 2, Capa 3 y la descripción que considere necesaria.

Solución Parte 2

a) El departamento A contará con 55 PCs, 55 teléfonos IP y 11 impresoras. Además, debemos reservar una IP para la interfaz del router y para direcciones de red y broadcast. Por lo tanto son necesarias 124 IPs.
Por lo tanto, necesitamos un prefijo /25.
Para el departamento B necesitamos 66 IP para equipos mas la del router, de red y de broadcast. Por lo tanto 69 IPS, lo que implica también un /25.
Para el departamento C necesitamos 14 para impresoras y equipos, 16 para otro equipamiento más router, red y broadcast, lo que nos da 33 direcciones. Por lo tanto, necesitamos un /26.
Propongo utilizar el prefijo 192.168.0.0/25 para el departamento A, el 192.168.1.0/25 para el departamento B y el 192.168.1.128/26 para el departamento C.

Además, será necesario numerar la red entre routers. Para esto son necesarias 3 direcciones para cada router mas red y broadcast. Por lo tanto necesitamos un /29. Propongo utilizar el prefijo 192.168.1.196/29

b)
R1 tiene direcciones 200.47.0.2 (eth0) y 192.168.1.197 (eth1)
R2 tiene direcciones 192.168.1.198 (eth0) y 192.168.0.1 (eth1)
R3 tiene direcciones 192.168.1.199 (eth0), 192.168.1.1 (B, eth1), 192.168.1.129 (C, eth2) y 164.73.36.2 (Internet, eth3)

R2

Prefijo destino	--	Gateway	--	Interfaz	
192.168.0.0/25	--	DC	--	eth1	
192.168.1.196/29	--	DC	--	eth0	
200.47.0.0/27	--	192.168.1.197	--	eth0	
0.0.0.0/0	--	192.168.1.199	--	eth0	(redes B y C incluidas en esta ruta)

R3

Prefijo destino	--	Gateway	--	Interfaz
192.168.1.0/25	--	DC	--	eth1
192.168.1.128/26	--	DC	--	eth2
192.168.1.196/29	--	DC	--	eth0
164.73.36.0/30	--	DC	--	eth3
200.47.0.0/27	--	192.168.1.197	--	eth0
192.168.0.0/25	--	192.168.1.198	--	eth0
0.0.0.0/0	--	164.73.36.1	--	eth3

Host

Prefijo destino	--	Gateway	--	Interfaz
200.47.0.0/27	--	DC	--	eth0
0.0.0.0/0	--	200.47.0.1	--	eth0

c)

MAC origen	MAC destino	IP origen	IP destino	Desc
MAC_PC_C	FF:FF:FF:FF:FF:FF	--	--	ARP Req. se consulta MAC de 192.168.1.129
MAC_R3_2	MAC_PC_C	--	--	ARP Resp. se responde MAC_R3_2
MAC_PC_C	MAC_R3_2	192.168.1.130	200.47.0.3	ICMP echo request
MAC_R3_0	FF:FF:FF:FF:FF:FF	--	--	ARP Req. se consulta MAC de 192.168.1.197
MAC_R1_1	MAC_R3_0	--	--	ARP Resp. se responde MAC_R1_1
MAC_R3_0	MAC_R1_1	192.168.1.130	200.47.0.3	ICMP echo request
MAC_R1_0	FF:FF:FF:FF:FF:FF	--	--	ARP Req. se consulta MAC de 200.47.0.3
MAC_SERV	MAC_R1_0	--	--	ARP Resp. se responde MAC_SERV
MAC_R1_0	MAC_SERV	200.47.0.1	200.47.0.3	ICMP echo request
(observar que R1 hace NAT)				
MAC_SERV	MAC_R1_0	200.47.0.3	200.47.0.1	ICMP echo reply
MAC_R1_1	MAC_R3_0	200.47.0.3	192.168.1.130	ICMP echo reply
MAC_R3_2	MAC_PC_C	200.47.0.3	192.168.1.130	ICMP echo reply

Parte 3 (30 puntos)

Se desea implementar un sistema cliente-servidor para un servicio de mensajes de alerta en un lenguaje de alto nivel usando la API de sockets del curso. El servidor acepta conexiones TCP en la IP 100.100.0.1 en el puerto 8086.
Un cliente al conectarse activará las alertas enviando el string “1!”, y luego no transmitirá más, solo escuchará mensajes de alerta.
Una vez establecida la conexión y activadas las alertas, el servidor enviará mensajes en el siguiente formato:
Primero 1 byte indicando el largo de la alerta (llamémosle L), seguido de un string de L bytes conteniendo la alerta.

Se pide:

a) Implemente el cliente que se conecta al servidor y permanece recibiendo y decodificando mensajes. Una vez decodificado un mensaje y extraída la alerta esta se procesará con la función auxiliar (provista) desplegar_alerta(s)

b) Implemente el servidor que acepta las conexiones y envía a todos clientes activos una copia de cada alerta. El sistema operativo generará alertas invocando una función nueva_alerta(s) (que Ud. deberá implementar), donde s es un string de largo menor a 255 Bytes.

API SOCKETS

Sockets UDP
skt = socket.udp()
skt.close()
skt.bind(address, port)
ip, port = skt.gethost()
skt.sendto(datagram, address, port)
datagram, ip, port = skt.receive(timeout)

Sockets TCP
master = socket.tcp()
master.bind(address, port)
server = master.listen()
client, err = server.accept()
master.close()
server.close()
client.close()
client = master.connect(address, port)
ip, port = client.gethost()
ip, port = client.getpeer()
client.settimeout(timeout)
server.settimeout(timeout)
data, err = client.receive()
remain, err = client.send(data)

Threads
thread.new(f, param1, param2, …)

Solución Parte 3

a)

```
function cliente ()
  skt = socket.tcp()
  skt = skt.connect('100.100.0.1', 8086)

  act = '1!'
  repeat
     act, err = skt.send(act)
  until act=='' or err=='closed'

  If err==’closed’ then exit() end

  buff = ''
  repeat
     r, err = skt.receive()
     if not err then
        buff = buff..r
        l = buff.substr(1, 1).tonumber()
        if buff.length()>=l+1 then
           alerta = buff.substr(2, l+1)
           desplegar_alerta(alerta)
           buff = buff.substr(l+2, buff.length())
```

```
        end
      end
  until err=='closed'
```

b)

```
clientes = set.new()  -- almacenará los skts de los clientes activos

function servidor ()
  srv = socket.tcp()
  srv.bind('100.100.0.1', 8086)
  srv =srv.listen()

  while true do
     skt = srv.accept()
     new.thread(atiende_cliente, skt)
  end

function atiende_cliente(skt)
   msg = ''
   repeat
     r, err = skt.receive()
     if err=='closed' then   --cliente desconectó sin activarse
        clientes.remove(skt)
        return
     end
     msg=msg..r
   until msg=='1!'          --activación completa
   clientes.add(skt)
end

function nueva_alerta(s)
   msg = chr(s.length()) .. s
   for each cliente in clientes do    --para cada cliente activo...
     buff = msg
     repeat                          --...enviamos todo msg
       buff, err = cliente.send(buff)
     until buff=='' or err=='closed'
     if error=='closed' then
       clientes.remove(cliente)
     end
   end
end
```