24 de noviembre de 2021

Redes de Datos 1
2º parcial – 2021
Solución

Esta es una posible solución a las preguntas planteadas. Por razones didácticas normalmente contiene bastante más información que la mínima necesaria para responder la pregunta.

Pregunta 1 (6 puntos)

Explique el funcionamiento de los códigos polinómicos o Códigos de Redundancia Cíclica (CRC) vistos en el curso.
A modo de guía:

i. Identifique si se trata de un mecanismo de detección o corrección de errores.
ii. Explique cómo se construyen los mensajes en el transmisor.
iii. Explique cómo se controlan los errores en recepción.
iv. Explique en qué casos los errores pueden pasar inadvertidos.

El mecanismo de CRC es para la detección de errores.

*Se basa en tratar las cadenas de bits como polinomios cuyos coeficientes serán 0 o 1. A una trama de **m** bits se le asocia un polinomio M(x) de grado m-1 con términos que van desde x^{m-1} hasta x^0 donde el coeficiente del término x^t corresponde con el bit t de la cadena. Por ejemplo 1101 corresponde al polinomio x^3+x^2+1.*

Para utilizar este método el transmisor y receptor deben ponerse de acuerdo en un polinomio generador G(x) de grado r. Dicho polinomio deberá cumplir varias condiciones, algunas de las cuáles se mencionarán después. Por ejemplo, G(x) deberá tener el primero y el último de sus coeficientes en 1.

La idea es que el transmisor agregue bits de redundancia a los datos que desea transmitir de modo que el polinomio asociado a esa secuencia de bits sea divisible por G(x).
Supongamos que la trama a transmitir se asocia con el polinomio M(x) como se indicó anteriormente. El procedimiento en el transmisor es el siguiente:

- *Sea r el grado de G(x). Se anexan r bits en "0" al final de la trama, con lo que se obtendrá una secuencia de m+r bits que corresponderá por tanto al polinomio: $x^rM(x)$.*
- *Se divide ese polinomio $x^rM(x)$ entre G(x), usando división módulo 2 (sumas y restas son XOR sin acarreo) y se obtiene un cociente Q(x) y un resto R(x) por lo que se puede escribir que:*
  $x^rM(x) = G(x)*Q(x)+R(x)$.
- *Se resta el residuo (que tiene r o menos bits) a la cadena de bits correspondiente a $x^rM(x)$, usando resta módulo 2. Esto último es equivalente a poner los r bits del resto al final del mensaje de m bits.*
  $T(x) = x^rM(x)-R(x) = G(x)*Q(x)$
  por lo que el polinomio T(x) obviamente será divisible entre G(x) y sus coeficientes serán los bits de la trama que será enviada por el canal.
  Observar que la resta o suma módulo 2 son equivalentes a XOR, por lo que sumar o restar es equivalente y además como $x^rM(x)$ tiene los r términos de menor grado en 0 y el residuo tiene grado r o menor, la resta (suma) indicada, no es más que una concatenación de M(x) con el residuo. Esto facilita la implementación en hardware del método.

En el receptor se recibirá una secuencia de bits que corresponderá a un polinomio Q(x)=T(x)+E(x), representando E(x) el patrón de errores ocurrido en el canal y en el que serán 1 los bits alterados.
El receptor divide Q(x) entre G(x) y se toma el resto. Como T(x) es divisible por G(x), el resto obtenido será simplemente el resto correspondiente a dividir E(x) entre G(x). Por lo tanto, si la división tiene un resto diferente a cero se habrá detectado la existencia de error(es) en el canal.

El resto puede ser 0 concluyéndose que no hay errores si efectivamente no los hubo (E(x) es nulo) o si los hubo de tal forma que el E(x) resultó divisible entre G(x).
De modo que para que estos casos sean los mínimos, se trata de elegir G(x) de modo que no divida a los patrones de error más frecuentes en los canales.

Una vez verificado que no hubo errores y teniendo en cuenta que los primeros m bits corresponderán al mensaje y los últimos r bits al CRC (resto de la división), el mensaje original se reconstruye de forma sencilla tomando los primeros m bits de mensaje equivalente del polinomio T(x).

Pregunta 2 (8 puntos)

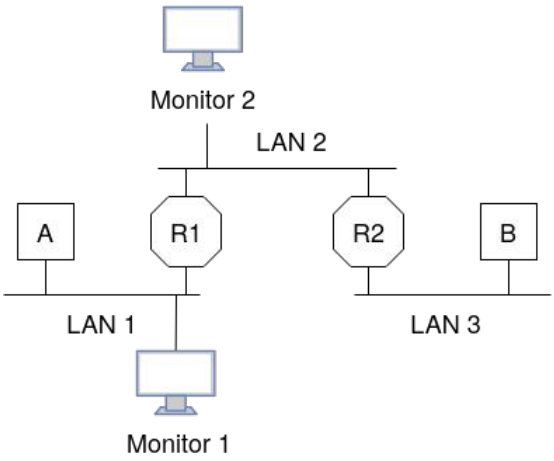
a) Explique el cometido del protocolo ARP (Address Resolution Protocol).

El protocolo ARP tiene como objetivo relacionar las direcciones de capa 3 (IP) con las direcciones de capa MAC, más precisamente permite a un equipo, dada una dirección IP, obtener la dirección de capa MAC del equipo que posee dicha IP .
Se aplica a capas de enlace de acceso múltiple, es decir aquellas donde por la misma interfaz puedo potencialmente comunicarme con múltiples equipos directamente (en capa 2). Ejemplos actuales de estas redes son las redes 802.3 (Ethernet en todas sus variantes), 802.11 (redes inalámbricas), etc.

Considere la topología de la imagen. La LAN 1 cuenta con la máquina Monitor 1 similar a las utilizadas en el laboratorio, que permite capturar todas las tramas de esa LAN; y análogamente, en la LAN 2 se cuenta con Monitor 2. Considere que no hay información en los cachés de ningún equipo y que las tablas de forwarding están bien configuradas.

b) En el equipo A se ejecuta el comando “ping -c 1 IP_B”, siendo IP_B la dirección IP del equipo B.
Recordar que la opción “-c 1” indica que se envía un solo paquete. Se asume que el comando es exitoso.
Indique las tramas que observa cada máquina Monitor.

Detalle los intercambios analizados, indicando el cometido de cada trama así como los campos más relevantes de los encabezados de los protocolos involucrados (direcciones de origen y destino a nivel de capa MAC e IP).



Observación 1: no se limite a los intercambios ARP, interesa la “captura completa” de todo el intercambio tal como se vería con el wireshark en modo promiscuo en las máquinas Monitor
Observación 2: se sugiere hacer una tabla con las tramas indicando qué Monitor ve cada una.

Cuando en A se ejecuta el comando ping, se necesitará enviar un mensaje ICMP del tipo “echo request” a IP_B, para eso A consulta su tabla de forwarding y obtiene que el próximo salto para llegar a IP_B es la IP de R1 en la LAN1 (llamémosla IP_R1_1) y por tanto debería enviar una trama en la LAN1 con dirección MAC de destino la de R1 en LAN1. Como A no conoce esa MAC, realizará una consulta ARP para averiguarla. Una vez que la averigue, A enviará una trama con MAC de origen MAC_A, MAC de destino MAC_R1_1 (MAC de la interfaz de R1 en LAN1) conteniendo el mensaje ICMP con IP de origen IP_A e IP de destino IP_B. R1 recibirá la trama (está destinada a una de sus direcciones MAC), pero como a nivel IP el paquete no está destinado a él, procederá a encaminarlo al destino.
Para realizar esto, R1 consultará su tabla de forwarding, verá que el próximo salto para llegar a IP_B es la IP de R2 en la LAN2 (llamémosla IP_R2_2). De forma similar a lo realizado por A, R1 deberá averiguar la MAC asociada a IP_R2_2 utilizando el protocolo ARP. Un procedimiento equivalente realizará R2 en la LAN3.
La siguiente tabla muestra la secuencia de mensajes que se intercambian (si bien no se pedía qué pasaba en la lan3, se incluyó por completitud):

Sequencia temporal	***Monitor***	***MAC Origen***	***MAC Destino***	***IP Origen***	***IP Destino***	***Contenido***
1	*1*	*MAC_A*	*FF:…:FF (broadcast)*	*--*	*--*	*Mensaje de protocolo ARP. Consulta por la dirección MAC de la máquina con dirección IP IP_R1_1* *El mensaje no es IP, pero a nivel del encabezado ARP aparece la correspondencia MAC_A, IP_A.*
2	*1*	*MAC_R1_1*	*MAC_A*	*--*	*--*	*Mensaje de protocolo ARP. Respuesta directa a A informando la relación entre la IP IP_R1_1 y la dirección MAC_R1_1*
3	*1*	*MAC_A*	*MAC_R1_1*	*IP_A*	*IP_B*	*Trama conteniendo el mensaje ICMP request de A a B.* *El mensaje llega a R1 y éste lo enruta hacia R2*
4	*2*	*MAC_R1_2*	*FF:…:FF (broadcast)*	*--*	*--*	*Mensaje de protocolo ARP. Consulta la dirección MAC de la máquina con IP IP_R2_2.* *El mensaje no es IP, pero a nivel del encabezado ARP aparece la correspondencia MAC_R1_2, IP_R1_2*
5	*2*	*MAC_R2_2*	*MAC_R1_2*	*--*	*--*	*Mensaje de protocolo ARP. Respuesta directa a R1 informando la relación entre IP_R2_2 y MAC_R2_21*
6	*2*	*MAC_R1_2*	*MAC_R2_2*	*IP_A*	*IP_B*	*Trama conteniendo el mensaje ICMP request de A a B.* *El mensaje llega a R2 y éste lo encamina a B*
7	*LAN3*	*MAC_R2_3*	*FF:…:FF (broadcast)*	*--*	*--*	*Mensaje de protocolo ARP. Consulta la dirección MAC de la máquina con IP IP_B* *El mensaje no es IP, pero a nivel del encabezado ARP aparece la correspondencia MAC_R2_3, IP_R2_3*
8	*LAN3*	*MAC_B*	*MAC_R2_3*	*--*	*--*	*Mensaje de protocolo ARP. Respuesta directa a R2 informando la relación entre IP_B y MAC_B*
9	*LAN3*	*MAC_R2_3*	*MAC_B*	*IP_A*	*IP_B*	*Trama conteniendo el mensaje ICMP request de A a B.*
10	*LAN3*	*MAC_B*	*MAC_R2_3*	*IP_B*	*IP_A*	*Trama conteniendo el mensaje ICMP reply de B a A.* *B no necesita usar ARP, porque la correspondencia IP_R2_3, MAC_R2_3 se incorporó a la tabla de ARP de PCB al recibir el mensaje 7.*
11	*2*	*MAC_R2_2*	*MAC_R1_2*	*IP_B*	*IP_A*	*Trama conteniendo el mensaje ICMP reply de B a A.* *R2 no necesita usar ARP, porque la correspondencia IP_R1_2, MAC_R1_2 se incorporó a la tabla de ARP de R2 al recibir el mensaje 4.*
12	*1*	*MAC_R1_1*	*MAC_A*	*IP_B*	*IP_A*	*Trama conteniendo el mensaje ICMP reply de B a A.* *R1 no necesita usar ARP, porque la correspondencia IP_A, MAC_A se incorporó a la tabla de ARP de R1 al recibir el mensaje 1.*

Pregunta 3 (4 puntos)

En los protocolos de acceso al medio compartido utilizando CSMA/CD en que se basa el funcionamiento de las redes Ethernet:

a) ¿por qué se necesita establecer un tamaño mínimo de trama?

b) ¿qué sucedería si las tramas fueran de largo menor a ese mínimo?

Justifique su respuesta.

a) *En las redes Multiacceso donde las estaciones comparten un medio (por ejemplo 802.3 sobre un bus compartido u 802.11), siempre existe la posibilidad de que dos o mas estaciones intenten utilizar el canal al mismo tiempo y ambas transmitan, esto ocasiona que la señal resultado este distorsionada y no corresponda a ninguna de las señales originales (colisión).*
Para minimizar las colisiones, se sensa previamente el canal, de modo de no interrumpir a una estación que está transmitiendo, pero esto no elimina la posibilidad de colisiones.
Por los tiempos de propagación de las señales en el medio físico, podría suceder que una estación sense el canal y lo vea libre aún cuando otra estación instantes antes haya comenzado a transmitir. En ese caso, la segunda estación podría comenzar a transmitir colisionando con lo transmitido por la primer estación.

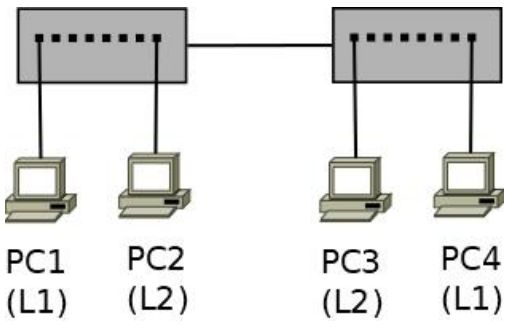
El mecanismo de detección de colisiones (CD, Collision Detection) es el mecanismo que utiliza una estación en 802.3 para saber si lo que está intentando transmitir fue colisionado por la transmisión de otra estación, verificando que lo que aparece en el canal es lo mismo que se está transmitiendo. De esa forma, la estación se asegurará que todas las demás estaciones recibieron lo que ella quiso transmitir. Si ve que lo que recibe no es lo que envió, entonces asumirá que su transmisión colisionó con los datos de otra y podrá detener su transmisión anticipadamente para no seguir ocupando el canal con señales que no serán útiles.
El peor caso para detectar si hubo o no colisión se da cuando las estaciones están lo más alejadas posibles (la distancia máxima entre estaciones en el protocolo, incluyendo repetidores) y si consideramos que el tiempo de propagación en el medio para dicha distancia máxima es T, entonces la duración mínima de la trama debería ser de 2T. Para entender esto, supongamos que A y B son estaciones que se encuentran a la distancia máxima. En el peor caso, A comienza a transmitir, y un instante antes que su señal llegue a la estación B (tiempo T - ε), B sensa el canal, detecta que está libre, y comienza a transmitir. Casi inmediatamente B detecta la colisión, pero la señal que B inyectó en el canal demorará un tiempo T en alcanzar a la estación A, por lo que para poder detectar la colisión A debe estar transmitiendo cuando dicha señal llega, 2T luego de comenzar a transmitir. Dado el retardo máximo admitido para el cable y la velocidad de serialización (bits por segundo), se puede calcular cuántos bits debería tener como mínimo una trama para asegurarnos de detectar las colisiones.

b) *Si las tramas fueran de largo menor a 2T entonces la estación terminaría de transimitir y si se produce una colisión la verá en el canal pero no podrá saber si es fruto de una colisión de otras dos estaciones estaciones entre si o si es una colisión con su propia trama.*

Pregunta 4 (7 puntos)

En una infraestructura de red como la de la figura consistente en equipos interconectados utilizando dos switches Ethernet, se desea separar el tráfico de los equipos del grupo L1 y L2, para lo que el administrador propone las siguientes alternativas:

1. Asignar a los equipos del grupo L1 direcciones IP del rango 10.1.0.0/24 y a los equipos del grupo L2 direcciones IP del rango 10.2.0.0/24
2. Definir la numeración IP de la misma forma que en la alternativa 1, pero además definir dos VLANs en los switches y asignar los equipos del grupo L1 a la VLAN1 y los equipos del grupo L2 a la VLAN2.



a) Explique si la alternativa 1 es posible y explique cómo se podría resolver la conectividad entre equipos de L1 y L2.

La alternativa 1 es posible ya que pueden coexistir diferentes rangos de redes IP sobre una misma capa 2. Cada equipo ve a nivel de capa de red a los equipos que son accesibles de acuerdo a su tabla de

forwarding. La conectividad entre equipos de diferente rango de direcciones IP debe resolverse usando un enrutador (o equipo que actúe como tal). Por tanto será necesario incluir un equipo adicional que tenga una interfaz configurada en cada uno de los rangos y que actúe como enrutador.

b) En el caso de la alternativa 2, explique qué configuración extra se requiere en el enlace entre switches.

Para que una trama de PC1 (VLAN1) llegue a PC4 (VLAN1) y no llegue a PC3 (VLAN2), la información de qué trama pertenece a qué VLAN debe intercambiarse entre los switches. Para agregar a las tramas esa información, es necesario que en el enlace entre switches se configure el protocolo 802.1Q que agrega al formato de la trama algunos campos para que circule la información de VLANs.

c) Analice las ventajas y desventajas de cada una de las alternativas propuestas.

En el caso de la alternativa 1, la separación es a nivel de capa 3, pero no hay una separación de los equipos a nivel de capa 2. Un equipo podría ver el tráfico del otro grupo y las tramas de broadcast llegarán a todos los equipos. Es una solución más simple porque no implica configuraciones a nivel de capa2.
En la alternativa 2, hay una separación del tráfico y si está todo bien configurado una estación no va a recibir tráfico del otro grupo. Tiene la complejidad de requerir switches que soporten VLANs y configurarlas adecuadamente.

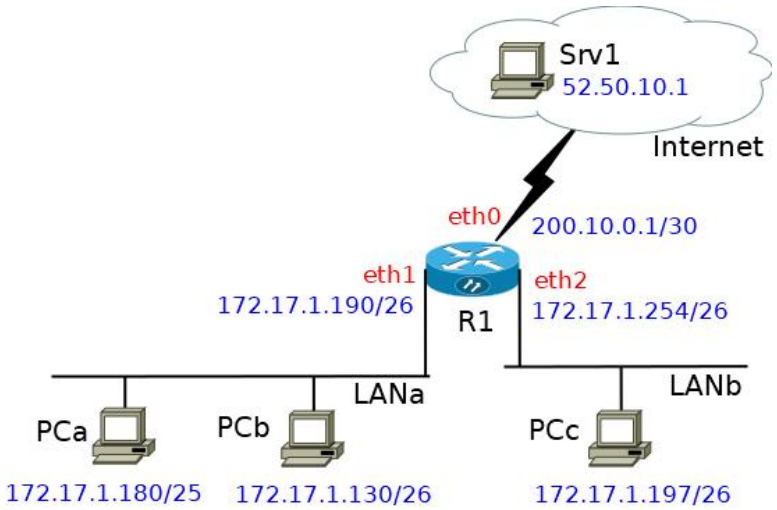
Pregunta 5 (12 puntos)

Originalmente una empresa tenía todos sus equipos internos configurados en una misma LAN, con direcciones IP privadas pertenecientes al rango 172.17.1.128/25.

Por una reorganización interna se decidió subdividir el rango original, quedando la red con la topología esquematizada en la figura.

Las direcciones de cada equipo se configuraron con las IPs y máscaras indicadas en la figura, y a los PCs se les agregó una ruta por defecto a la IP correspondiente de R1.

Luego de la reconfiguración, aparecieron reclamos por falta de conectividad parcial entre equipos internos de la red.



a) Identifique y analice cuáles comunicaciones (bidireccionales) entre los equipos PCs internos son posibles y cuáles no (verifique todas las parejas de intercambios posibles). Explique detalladamente por qué algunas comunicaciones no son exitosas.
Nota: decir que no funciona porque la máscara está mal no es una respuesta aceptable.

Al configurar la interfaz de cada equipo con una IP y una máscara, automáticamente se crea una ruta que le permite llegar a los equipos directamente conectados.
En el ejemplo, cuando a PCa se le configura la IP 172.17.1.180 y la máscara /25 (por ejemplo con el comando "ifconfig eth0 172.17.1.180/25") se agregará automáticamente una ruta para llegar a la red 172.17.1.128/25 como directamente conectada.
En el caso de PCb, cuando se le configura la IP 172.17.1.130 y la máscara /26, se agregará automáticamente una ruta para llegar a la red 172.17.1.128/26 como directamente conectada.
Análogamente, cuando se le configura la IP 172.17.1.197 y la máscara /26 a PCc, se agregará automáticamente una ruta para llegar a la red 172.17.1.192/26 como directamente conectada.
Cada equipo tendrá luego una ruta por defecto a R1. En el caso de PCa y PCb la ruta por defecto es hacia 172.17.1.190 y PCc hacia 172.17.1.254. Observar que tanto para PCa como PCb, la dirección 172.17.1.190 pertenece a su rango directamente conectado y para PCc la IP 172.17.1.254 pertenece también a su rango directamente conectado.
Analicemos todas los intercambios posibles:

i. *Si PCc quiere enviar un paquete a PCb, consultará su tabla de forwarding y como la IP de PCb 172.17.1.130 no pertenece a su rango directamente conectado 172.17.1.192/26, sabrá que tiene que usar la ruta por defecto hacia R1 (172.17.1.254) para llegar a PCb. PCc realizará ARP para encontrar la MAC de R1 y enviará el paquete a través de R1. R1 consultará su tabla de forwarding, verá que la IP de PCb pertenece al rango de su interfaz eth1 y realizará ARP consultando por la MAC asociada a la IP de PCb. PCb recibirá ese mensaje, lo responderá y por tanto R1 podrá entregarlo a PCb. Por tanto, el paquete desde PCc hacia PCb llegará exitosamente.*
ii. *Del mismo modo cuando PCb quiera enviar un paquete a PCc, consultará su tabla de forwarding y como la IP de PCc 172.17.1.197 no pertenece a su rango directamente conectado 172.17.1.128/26, sabrá que tiene que usar la ruta por defecto hacia R1 (172.17.1.190) para llegar a PCc. PCb realizará entonces ARP para encontrar la MAC de R1 y enviará el paquete a través de R1. R1 consultará su tabla de forwarding, verá que la IP de PCc pertenece al rango de su interfaz eth2 y realizará ARP consultando por la MAC asociada a la IP de PCc. PCc recibirá ese mensaje, lo responderá y por tanto R1 podrá entregarlo a PCc. Por tanto, el paquete desde PCb hacia PCc llegará exitosamente.*
iii. *Cuando PCa quiere enviar un paquete a PCb consultará su tabla de forwarding y como la IP de PCb 172.17.1.130 pertenece al rango 172.17.1.128/25 que PCa cree tener directamente conectado, sabrá que necesitará usar ARP para encontrar la MAC de PCb. PCb recibirá el broadcast y lo responderá enviando su MAC. De esta forma PCa podrá enviar exitosamente el paquete IP a PCb.*
iv. *Si PCb quiere enviar un paquete a PCa (por ejemplo la respuesta al paquete anterior), consultará su tabla de forwarding y como la IP de PCa 172.17.1.180 pertenece al rango 172.17.1.128/26 que PCb tiene directamente conectado, usará ARP para encontrar la MAC de PCa. Al igual que en el caso anterior, PCa recibirá y responderá el mensaje ARP, por lo que PCb podría enviar exitosamente el paquete a PCa*
v. *Cuando PCa quiere enviar un paquete a PCc consultará su tabla de forwarding y como la IP de PCc 172.17.1.197 pertenece al rango 172.17.1.128/25 que PCa cree tener directamente conectado, enviará un mensaje ARP para encontrar la MAC de PCc. Como PCc no está en la LANa, no recibirá el mensaje de broadcast y por tanto no responderá.* ***Por tanto PCa no podrá enviar paquetes hacia PCc.***
vi. *Si PCc quiere enviar un paquete a PCa, consultará su tabla de forwarding y como la IP de PCa 172.17.1.180 no pertenece a su rango directamente conectado 172.17.1.192/26, sabrá que tiene que usar la ruta por defecto hacia R1 (172.17.1.254) para llegar a PCa. PCc realizará entonces ARP para encontrar la MAC de R1 y enviará el paquete a través de R1.*
R1 consultará su tabla de forwarding, verá que la IP de PCa 172.17.1.180 pertenece al rango de su interfaz eth1 y realizará ARP consultando por la MAC asociada a la IP de PCa. PCa recibirá ese mensaje, lo responderá. El paquete desde PCc hacia PCa llegará exitosamente.

En resumen:
- *la comunicación bidireccional entre PCa y PCb es posible*
- *la comunicación bidireccional entre PCb y PCc es posible*
- *la comunicación bidireccional entre PCa y PCc no es posible porque PCa no puede enviar paquetes a PCc (PCc si puede mandar paquetes a PCa).*

b) Explique qué problema resuelve y cómo funciona el mecanismo de NAT/PAT (Network Address Translation/Port Address translation). En la red de la figura, explique con qué direcciones IP y puertos se verán los paquetes en la LANb y en el enlace a Internet, cuando PCc consulta una página web alojada en Srv1 (puerto 80).

El mecanismo de NAT/PAT fue creado para mitigar el problema de la escasez de direcciones IPv4. El mecanismo permite que varios equipos de una red compartan una única dirección IP pública, ahorrando por tanto direcciones públicas. La idea es mantener el uso del protocolo IP en la red interna o privada, usando direcciones reservadas para este propósito y que por tanto no tienen validez en la red pública.
Se realiza entonces una "traducción" de direcciones en el equipo de borde que implementa el NAT/PAT.
En la red de la figura si la máquina PCc envía un segmento TCP hacia Srv1, en la red interna veremos un segmento con IP de origen 172.17.1.197, IP de destino 52.50.10.1, puerto de origen X y puerto destino 80. El puerto de origen es un puerto efímero normalmente asignado por el sistema operativo.
Cuando ese segmento pase por R1 que ahora implementa NAT/PAT, se le cambiará la IP de origen por la IP pública 200.10.0.1 y para evitar posibles conflictos con otras conexiones al mismo destino, se cambiará también el puerto de origen X por un puerto Y que no esté en uso por otra conexión.
El equipo R1 almacenará en una tabla los cambios realizados al segmento (IP privada, Puerto interno, IP pública, puerto público asignado por el PAT, protocolo) para saber a qué equipo interno debe dirigir las respuestas.

Pregunta 6 (6 puntos)

a) Explique cada uno de los siguientes objetivos de la seguridad: secreto (confidencialidad), autenticación, control de integridad y disponibilidad.

En seguridad el secreto se refiere a evitar que los datos puedan ser accedidos por terceros no autorizados a hacerlo. Por ejemplo, evitar que los datos en tránsito por una red insegura puedan ser interpretados por un atacante aún cuando puedan ser interceptados
La autenticación se refiere a procedimientos diseñados para validar la identidad de un individuo o entidad que intenta acceder o utilizar algún servicio
La integridad se refiere a garantizar que los datos, ya sea almacenados o en tránsito, no puedan ser modificados por un tercero sin que dicha modificación sea detectada
La disponibilidad se refiere a que los servicios y/o datos estén accesibles y operativos para los usuarios legítimos

b) Describa los principios de funcionamiento de un algoritmo de cifrado de clave pública.
Los cifrados de clave pública se basan en la existencia de dos algoritmos, uno para cifrar y otro para descifrar, que utilizan 2 claves distintas (relacionadas), que son creadas juntas, pero que cumplen al menos que una de las claves (la que llamaremos clave privada, K_{priv}) no puede ser calculada (no es computacionalmente viable calcularla) conociendo la otra (clave pública, K_{pub}). Siendo así, podemos permitir que todos conozcan la clave pública.
Se debe cumplir:
- Que dado un mensaje M en el dominio de la función, $D_{kpriv}(E_{Kpub}(M))=M$ (donde D y M son los algoritmos de descifrado y cifrado respectivamente)
- Es útil tener también la propiedad $D_{kpub}(E_{Kpriv}(M))=M$, para funciones como la firma digital
- Que dado K_{pub} sea computacionalmente inviable encontrar K_{priv}
- Que sea computacionalmente inviable descifrar $E_{kpub}(M)$ sin conocer K_{priv}.

c) ¿Cómo se utiliza un cifrado de clave pública para obtener secreto? ¿Con qué clave debe cifrarse, y con cuál descifrarse?
Para obtener secreto (confidencialidad), se requiere que nadie más que el destinatario legítimo del mensaje pueda descifrarlo.
Utilizando cifrados de clave pública, esto se logra si el emisor cifra con la clave pública correspondiente al receptor. Es decir, si A quiere enviarle un mensaje confidencial a B, este último precisa haber generado su par de claves pública/privada, y A precisa haber obtenido la clave pública de B. Luego, para enviar el mensaje confidencial, lo cifra con la clave pública de B, con la tranquilidad que solo quien tiene la clave privada correspondiente puede descifrar el mensaje