Redes de Datos

2do parcial – 2008

Solución

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

Pregunta 1 (10 puntos)

a) En una red de área local explique por qué es útil contar con direcciones de capa de enlace (MAC) y direcciones de capa de red (IP) para intercambiar datos entre dos máquinas. ¿Cuál es la función de las direcciones de capa MAC y cuál la de las direcciones IP?

b) Por una falla o malicia (ver figura 1), se conecta en la red un equipo C que tiene la misma dirección MAC que el equipo B.
Explique qué sucede con:
   i. las tramas que A envía a B
   ii. las tramas que B envía a A
   iii. los paquetes IP que A envíe a B
   iv. los paquetes IP que C envíe a A

c) Suponga ahora que B y C son routers (figura 2) que conectan con otras subredes.
Explique qué sucede cuando:
   i. A envía un paquete IP a X
   ii. X envía un paquete IP a A (que llega por B)

Nota: En todos los casos LAN 1 esta conectada utilizando repetidores o HUBs

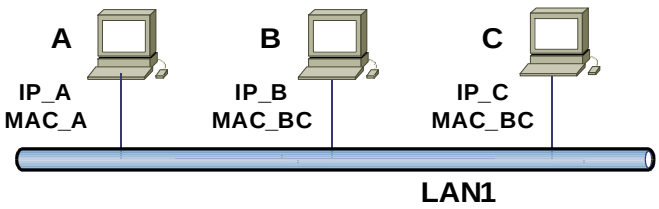

Figura 1

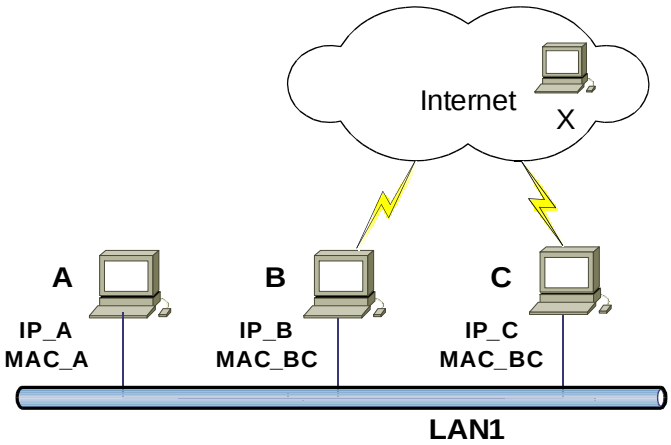

Figura 2

Respuesta 1

a) Es conveniente tener direcciones de capa MAC y de red para mantener la independencia de capas. Esto es necesario, por ejemplo, para poder utilizar varios protocolos de red (con diferentes formatos de direcciones) sobre la misma capa MAC, o la misma capa de red sobre diferentes capas MAC. De lo contrario forzaríamos a los protocolos de capa MAC y red a compartir el mismo formato y forma de distribución de direcciones, siendo que se reparten de formas distintas por cumplir distintas funciones.
La función de las direcciones de capa MAC es identificar a las distintas estaciones en el medio compartido. Para ello lo que requerimos es unicidad en una sola LAN. Como son en general pocas, no requerimos una distribución jerárquica de las mismas.
La función de las direcciones de capa de red es el direccionamiento global de las estaciones (o interfaces) en toda la red. Para ello se requiere unicidad de las direcciones en toda la red, y usualmente se hace una asignación jerárquica (o al menos en bloques) para optimizar la funcionalidad de ruteo.

b) No es extraño para un equipo que dos direcciones de red estén asociadas a la misma dirección de capa MAC, por lo que no detectarán nada extraño
   i) Las tramas que A envía a B son leídas tanto por B como por C, ya que ambas tarjetas tienen la misma dirección y la aceptan
   ii) Las tramas que B envía a A no tienen diferencia con las que enviaría si C no estuviera
   iii) Los paquetes que A envíe a B serán encapsulados en una trama con origen MAC_A y destino MAC_B. Por lo tanto ambos, B y C, leerán la trama. Al llegar a capa de red, B aceptará el paquete ya que estará dirigido a su dirección de capa de red, pero C detectará que no es para su dirección de red. En caso de estar configurado para hacer reenvío de paquetes lo reenviará a B, de lo contrario descartará el paquete (por supuesto, asumiendo que la capa de red no fue modificada maliciosamente)

iv) Los paquetes que C envíe a A tendrán como origen la IP_C y destino la IP_A, e irán encapsulados en una trama con dirección MAC origen MAC_BC y MAC destino MAC_A. Ninguna estación notará nada extraño.

c)

i) Al enviar un paquete a X, tendrá que enviarlo encapsulado en una trama con dirección MAC de destino la correspondiente al próximo salto de la ruta que me lleva a X. Supongamos que es B. Como la MAC es la misma, tanto B como C leerán la trama y pasarán el paquete a capa de red. Como ambos están configurados para enrutar, ambos reenviarán el paquete hacia X, por lo que X recibirá 2 copias del mismo paquete. Este duplicado se resolverá en capas superiores en X (si es TCP se resolverá en capa de transporte y si es UDP lo deberá resolver la capa de aplicación). Además, se estarán mal utilizando los dos enlaces a Internet, ya que todo el tráfico "subirá" por ambos.

ii) Al llegar a B, este reenviará el paquete a A encapsulado en una trama con dirección origen MAC_B y dirección destino MAC_A. Ninguna estación notará nada extraño.

Pregunta 2 (6 puntos)

a) Explique el principio de funcionamiento de los códigos de redundancia cíclica (CRC o códigos polinómicos). Indique qué información se comparte entre transmisor y receptor, cómo se construye la trama a transmitir.

b) Explique cómo se detectan los posibles errores y qué tipos de errores no se detectan con este mecanismo.

Respuesta 2

a) Los métodos de detección de errores mediante CRC se basan en tratar las cadenas de bits como polinomios cuyos coeficientes serán 0 o 1. Un marco con k bits corresponde a los coeficientes de un polinomio e grado k-1 que van desde x^k-1 hasta x^0. 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). Dicho polinomio deberá cumplir algunas condiciones, algunas de las cuáles se mencionarán después. Por ejemplo, G(x) deberá tener el primero y el último de sus coeficientes en 1.
Supongamos que el marco que se quiere transmitir corresponde al polinomio M(x). Lo que se hace es agregar una suma de comprobación al final del marco, de manera que el polinomio representado sea divisible por G(x). El procedimiento es el siguiente:
   - Sea r el grado de G(x). Se anexan r bits en "0" al final del marco, con lo que tendrá m+r bits y corresponderá al polinomio: $x^rM(x)$.
   - Se divide la cadena de bits que corresponde a $x^rM(x)$ entre la que corresponde a G(x), usando división módulo 2.
   - Se resta el residuo (de r o menos bits) a la cadena de bits correspondiente a $x^rM(x)$, usando resta módulo 2. Llamemos a este polinomio T(x), que obviamente será divisible entre G(x), y es el marco que será transmitido.

   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 en el tercer paso, no es más que una concatenación de M(x) con el residuo. Esto facilita la implementación en hardware del método.

b) En el receptor se recibirá una trama que corresponderá a un polinomio R(x)=T(x)+E(x), representando E(x) al error ocurrido en el canal. Se divide R(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 único caso en que no se detectarían los errores, es cuando E(x) es divisible entre G(x)

(Adicional al parcial) Como ejemplo, todos los errores simples siempre serán detectados, ya que se tratarán de casos en que $E(x)=x^i$, que nunca será divisible entre un polinomio G(x) que contenga al término x^0.
Los errores dobles llevarán a polinomios E(x) de la forma x^i+x^j (i>j)que es representable como $x^j(x^{i-j}+1)$. Por lo tanto una manera de detectar todo los los errores dobles es que G(x) no divida a polinomios de la forma x^k+1 para ningun k hasta la longitud máxima del marco. Existen polinomios de bajo grado que no dividen a polinomios de la forma x^k+1 para valores muy altos de k.
De esa manera se han estandarizado algunos valores de G(x) para tener en cuenta los criterios anteriores y varias otras cosas más.
Se puede encontrar más referencia a este tema en el Libro:
"Redes de Computadores" de Andrew Tanenbaum – Sección 3.2 (tercera edición).]

Pregunta 3 (8 puntos)

a) Explique el mecanismo de control de acceso al medio de 802.3 (CSMA/CD), detallando cómo se comporta en las diferentes condiciones (canal libre, canal ocupado, cuando hay colisiones).

b) Explique por qué es necesario un tamaño mínimo de trama en esta tecnología.

c) Cómo compararía el desempeño esperado en una red de área local implementada con HUBs (repetidores) frente a la misma red implementada con SWITCHES? Justifique su respuesta.

Respuesta 3

a) 802.3 utiliza CSMA/CD persistente 1. En CSMA/CD cuando se reciben datos para transmitir se escucha el canal y si el mismo está libre, se comienza a transmitir inmediatamente.
Si el canal está ocupado, se espera observando constantemente el canal y tan pronto se libera se comienza a transmitir.
Ante una colisión, CSMA/CD en todas sus variantes deja de transmitir y espera un tiempo aleatorio antes de repetir el proceso para intentar tomar el canal. Las colisiones las detecta ya que escucha el canal mientras transmite, y compara lo transmitido con lo que aparece en el canal. El tiempo aleatorio se obtiene implementado un algoritmo de retroceso exponencial binario, en donde se ranura el tiempo y se sortea el *timeslot* en el cual se envía. Se sortea entre el *timeslot* 0 y el n -1 siendo n el número de reintentos que lleva. Con esto se logra modular entre el tiempo de espera y la probabilidad de colisión. (Cuantos más colisiones, más intentan entonces hay que dividir el tiempo entre más estaciones, entonces hay que esperar más para transmitir).

b) En CSMA/CD una estación detecta si la trama que ella transmitió tuvo o no colisión escuchando el canal mientras se transmite.
Como en cualquier protocolo CSMA, las demás estaciones verifican que no haya otra transmisión en el canal antes de comenzar a transmitir. Pero puede suceder que aunque la estación A haya comenzado a transmitir, la señal desde A aún no se haya propagado hasta la posición en la red donde se encuentra B, y éste decida transmitir. En un caso así tendríamos una colisión, y precisamos que A se entere, o sea que A tiene que estar verificando el canal cuando le llegue la señal de B (si parara de transmitir antes, no sabría si la señal que le llega de B es de una estación lejana que colisionó con su trama o de una estación cercana que comenzó a transmitir en cuanto A se detuvo). Por lo tanto, precisamos para el peor caso que A transmita al menos el tiempo necesario para que la señal de A llegue a B más el tiempo en que la señal de B llegue a A. Este tiempo multiplicado por la velocidad de transmisión en bits/s nos da la longitud mínima de trama (en bits). Este tiempo depende de la distancia máxima admitida entre cualquier par de estaciones, y la velocidad de propagación de la señal electromagnética por el medio elegido.

c) En una red local implementada con repetidores, todas las estaciones tienen que competir por el canal compartido para enviar cada trama. O sea que alcanza con que dos estaciones quieran transmitir al mismo tiempo para que haya una colisión y se desperdicie ancho de banda en el medio compartido. La utilización máxima del medio sería la velocidad de transmisión de bits en el canal (10 Mbps para 802.3), pero normalmente sería mucho peor dependiendo de cuántas estaciones estén transmitiendo.
En el caso de utilizar switches, cada estación (o pequeño grupo de estaciones) tendrá su propio dominio de colisión compartido con el switch, o sea que habrá tantos dominios de colisión como puertas tenga el switch. Incluso, si tenemos una sola estación por puerto del switch y configuramos full duplex, no habrá colisiones. Esto hará que haya muchas menos colisiones en cada segmento, mejorando la eficiencia de cada uno de ellos. Además, puede haber transmisiones simultáneas en varios segmentos, por lo que el desempeño esperado es mucho mejor. Internamente un switch utiliza un bus o backplane de mayor velocidad que la interfaces de salida hacia los hosts y buffers en estas interfaces para poder realizar las mejoras antes descriptas.

Pregunta 4 (10 puntos)

La figura 3 muestra una red en la que los enrutadores (señalados como RA hasta RD) corren el protocolo de ruteo dinámico RIP utilizando horizonte dividido.

a) Explique todo el intercambio de información entre los enrutadores, desde que se prenden hasta que se llega al régimen. Una vez en régimen muestre el contenido de la tabla de ruteo de cada enrutador.
Nota: para simplificar, se pide incluir solamente la información relativa a las LAN señaladas.

b) Suponga ahora que se rompe la interfaz if0 del enrutador RA perdiendo RA la conectividad con la red LAN 3. Por la topología de la red es posible que se produzca el problema de conteo a infinito. Muestre una posible secuencia de intercambio de información de ruteo que evidencie la existencia de este problema.

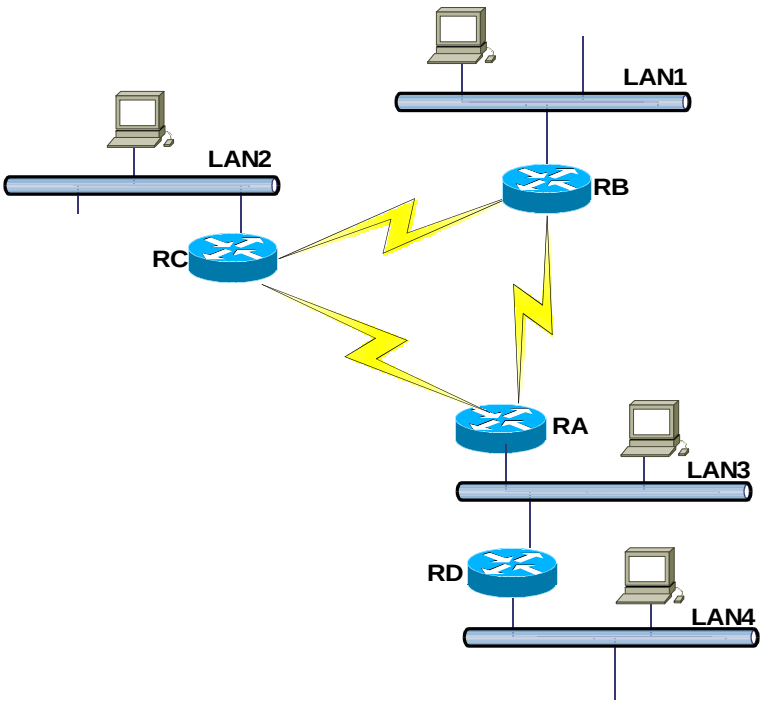

Figura 3

c) El problema anterior puede evitarse si se utiliza otro tipo de protocolo de ruteo. Explique qué protocolo o familia de protocolos de ruteo dinámico usaría para evitar el problema de conteo a infinito y fundamente de qué manera se soluciona el problema.

Respuesta 4

a) Inicialmente, los enrutadores conocen solamente las redes directamente conectadas.

Paso 1:

Rd -> Ra	Lan 4, distancia 1
	Lan 3, distancia 1
Ra -> Rd	Lan 3, distancia 1
Rc -> Ra	Lan 2, distancia 1
Ra -> Rc	Lan 3, distancia 1
Rb -> Ra	Lan 1, distancia 1
Rc -> Rb	Lan 2, distancia 1
Rb -> Rc	Lan 1, distancia 1

Paso 2:

Rd -> Ra	Lan 4, distancia 1
	Lan 3, distancia 1
Ra -> Rd	Lan 3, distancia 1
	Lan 1, distancia 2
	Lan 2, distancia 2
Rc -> Ra	Lan 2, distancia 1
	Lan 1, distancia 2
Ra -> Rc	Lan 3, distancia 1
	Lan 4, distancia 2
Rb -> Ra	Lan 1, distancia 1
	Lan 2, distancia 2
Rc -> Rb	Lan 2, distancia 1
	Lan 3, distancia 2
Rb -> Rc	Lan 1, distancia 1
	Lan 3, distancia 2

Paso 3:

Rd -> Ra	Lan 4, distancia 1
	Lan 3, distancia 1
Ra -> Rd	Lan 3, distancia 1
	Lan 1, distancia 2
	Lan 2, distancia 2
Rc -> Ra	Lan 2, distancia 1
	Lan 1, distancia 2
Ra -> Rc	Lan 3, distancia 1
	Lan 4, distancia 2
Rb -> Ra	Lan 1, distancia 1
	Lan 2, distancia 2
Rc -> Rb	Lan 2, distancia 1
	Lan 3, distancia 2
	Lan 4, distancia 3
Rb -> Rc	Lan 1, distancia 1
	Lan 3, distancia 2
	Lan 4, distancia 3

A partir de aquí, los anuncios se repiten ya que las tablas no cambian

b)

1) Ra deja de publicar la ruta hacia Lan3 y Lan4

2) (Por ejemplo) Rc, al no recibir la ruta hacia Lan3 de Ra, elige el otro camino del cual dispone (a través de Rb). Coloca en su tabla que puede llegar a Lan3 a través de Rb en 3 saltos. Como el próximo salto es Rb, NO le anuncia Lan3 a Rb, pero SI lo hace hacia Ra

3) Ra aprende que puede ir a Lan3 a través de Rc con distancia 3, por lo que lo agrega en su tabla (con distancia 4). Anuncia a Rb que Lan3 es alcanzable en 4 saltos.

4) Rb recibe la actualización de Ra, pasando la distancia a 5 en lugar de 1, y lo anuncia a Rc.

5) Rc recibe la información, actualiza su tabla (distancia 6), lo anuncia a Ra, y así continúan hasta llegar a distancia infinito

c) Los protocolos dinámicos de la familia de estado de enlace no tienen el problema del conteo a infinito, ya que todos los enrutadores aprenden la topología, y por lo tanto detectan que el destino no es alcanzable.

Pregunta 5 (7 puntos)

a) Explique cómo se firma electrónicamente un documento mediante el mecanismo de claves públicas y privadas.

b) Explique por qué este método garantiza el “no repudio”.

c) ¿Cómo se utiliza el mismo sistema de claves para garantizar el secreto de la información?

Respuesta 5

a) Para firmar digitalmente un mensaje, quien lo genera (pongamos A como ejemplo), debe encriptar con su clave privada algo que identifique “unívocamente” al mensaje. Opciones posibles son encriptar el mensaje completo, o simplemente, encriptar un MD (resumen) del mensaje.

b) Para cumplir con el principio de “no repudio”, se requiere que el emisor del o los mensajes los firme digitalmente.

B, al recibir el mensaje, verifica que la firma coincida con el mensaje (o sea, que al desencriptar la firma con la clave pública de A obtiene el mismo MD que el calculado del mensaje), y guarda el mensaje junto con la firma. Si en alguna ocasión A intentara repudiar el mensaje (decir que A no lo generó), B puede demostrar que fue firmado por alguien que tenía la clave privada de A mostrando que al desencriptar la firma con la clave pública de A se obtiene el hash correcto, y por las propiedades de los algoritmos de clave pública solo conociendo la clave privada se puede generar dicha firma, por lo que nadie más pudo generar ese mensaje (queda para la justicia resolver el caso en que A dice que le robaron su clave privada).

c) Para garantizar el secreto de la información, es necesario encriptar el mensaje con la clave pública del receptor (en un mensaje desde A hacia B, A encripta el mensaje con la clave pública de B). Por las propiedades de los algoritmos de clave pública, solamente quien posea la clave privada correspondiente podrá desencriptar el mensaje (es decir que solamente B podrá leer el mensaje encriptado con su clave pública).

Pregunta 6 (9 puntos)

a) Explique la principal función/necesidad del protocolo ARP (Address resolution protocol), indicando a qué tipos de redes se aplica

b) Explique el mecanismo conocido como “ARP gratuito”, indicando en qué situaciones es de utilidad.

c) En el esquema de la figura 4, suponga que inicialmente todos los switches están con su tabla de direcciones MAC vacía.

Se realizan las siguientes transacciones:
1. PC-A descarga una página web del Server-1
2. PC-C descarga un correo utilizando POP3 del Server-2
3. PC-C envía un echo-request a PC-B

Detallar las tablas de direcciones MAC de los switches luego de culminar estas transacciones.

Suponer las siguientes direcciones MAC: Sever-1 → Mac-1; Server-2 → Mac-2; PC-x → MAC-x

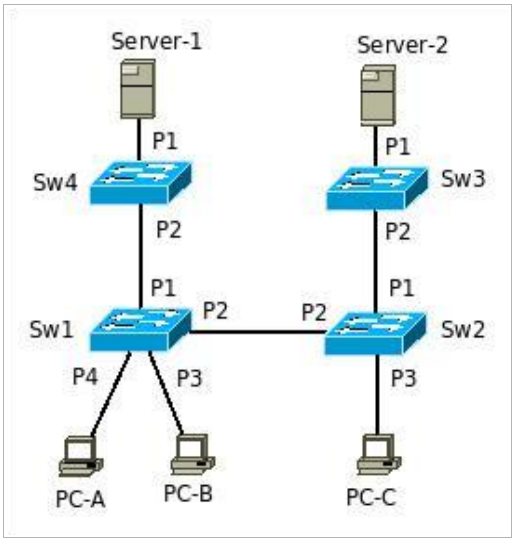

Figura 4

Nota: Suponer que los tiempos de vida en los Switches es suficiente para que no se borren entradas mientras se realizan las 3 transacciones.

Respuesta 6

a) ARP sirve para conocer la dirección MAC asociada a una determinada dirección IP. Cuando un equipo tiene que enviar un paquete IP a una máquina que está en su misma LAN (mismo rango IP y por tanto mismo dominio de broadcast) necesita conocer la dirección MAC de la máquina destino para poder armar la trama ethernet.
Como conoce la dirección IP destino, le hace falta la dirección MAC de destino y esa asociación es la que resuelve el protocolo ARP.
Supongamos que en una LAN la máquina A desea mandar un paquete IP a la máquina B. Asumamos que la máquina A tiene una dirección MAC MAC_A y una dirección IP IP_A y que la máquina B tiene una dirección MAC MAC_B y una dirección IP IP_B.
La máquina A conoce sus propios datos (MAC_A, IP_A) y quiere comunicarse con IP_B, por lo que debe averiguar MAC_B para poder enviar la trama.

b) El mecanismo conocido como ARP gratuito es realizado por un equipo al iniciarse y consiste en realizar una consulta ARP como la indicada en a) pero preguntando por su propia dirección IP. Es decir que cuando la máquina A configurada con la dirección IP IP_A y cuya interfaz ethernet tiene la dirección MAC MAC_A se enciende, realiza una consulta ARP destinada a la dirección de broadcast de capa 2 preguntando “Quién tiene la IP IP_A? y solicitando que se responda a IP_A que tiene MAC_A”.
Si las cosas están bien configuradas, no debería haber otra máquina con la IP_A asignada y por tanto nadie responderá a esa consulta. Si la IP está duplicada, entonces la máquina que acaba de encenderse detectará que hay otra máquina con la misma IP que ella y enviará un mensaje al usuario o se resistirá a configurar la red.
El ARP gratuito además de permitir la detección de IP's duplicadas, tiene por objeto actualizar las tablas de ARP de otras máquinas de la red que estuvieran anteriormente dialogando con esa IP en la eventualidad que la dirección MAC de la máquina A hubiera cambiado.
Si una máquina B de la red estaba dialogando con la máquina A antes que A se reiniciara, tendría en su caché de ARP la correspondencia entre IP_A y MAC_A. Pero si a la máquina A le falla la tarjeta de red y el administrador la cambia y luego enciende A, podría pasar que B siguiera mandando las tramas hacia IP_A a la MAC_A que ya no existe en la red. El ARP gratuito sirve entonces para que la máquina B actualice su entrada al ver una consulta iniciada por IP_A, la que contiene la nueva MAC MAC_A1.

c) Los switches aprenden dónde están las estaciones cuando reciben una trama originada por ellas. Cuando no saben dónde está la máquina destino, envían la trama por todas las bocas (menos por la que llegó). Por tanto, a medida que se van generando las tramas en las transacciones indicadas, las tablas de cada switch irán evolucionando como sigue:

	SW1		**SW2**		**SW3**		**SW4**	
PCA → Server-1	MAC-A	P4	MAC-A	P2	MAC-A	P2	MAC-A	P2
Server-1 → PCA	MAC-1	P1					MAC-1	P1
PCC → Server-2	MAC-C	P2	MAC-C	P3	MAC-C	P2	MAC-C	P2
Server-2 → PCC			MAC-2	P1	MAC-2	P1		
PCC → PCB								
PCB → PCC	MAC-B	P3	MAC-B	P2				