Solución - Examen – 20 de diciembre de 2012

(ref: eirc1212.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.**
- **Sólo se contestarán dudas de letra. No se aceptarán dudas de ningún tipo los últimos 30 minutos del examen.**
- **El examen es individual y sin material. Apague su celular mientras este en el salón del examen.**
- **Es obligatorio responder correctamente al menos 15 puntos en las preguntas teóricas y 20 de los problemas prácticos.**
- **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)

a) Explique que se entiende por el mecanismo de *self learning*, aplicado por los switches.

Es el mecanismo por el cual los switches construyen de forma automática, dinámica y autónoma su tabla. Los detalles están en la sección 5.6.2 Kurose 5a. Edición.

b) ¿En qué capa opera un hub? ¿Y un switch? Explique por qué se afirma que un switch al ser encendido se comporta como un hub y luego evoluciona al comportamiento típico de un switch.

Un hub opera en la capa física y un switch en la capa de enlace. El hub actua sobre los bits individuales en lugar de sobre las tramas como lo hace el switch, simplemente replicando la señal en todos los puertos, excepto el origen. Cuando se enciende un switch tiene su tabla de <MAC,puerto,tiempo> vacías, y por lo tanto, de acuerdo al mecanismo de self-learning, comienza a difundir tramas en todos los puertos menos el origen, y a medida que va llenando la tabla mencionada deja de utilizar difusión hasta tener destinos específicos.

c) ¿Es posible tener colisiones en una red implementada sólo con hubs? ¿Y si la red pasa a estar implementada sólo con switches?

Si es posible ya que el hub cada bit que recibe lo envía inmediatamente a cada una de sus interfaces, por lo que por ejemplo si un hub recibe tramas procedentes de dos interfaces distintas al mismo tiempo se produce una colisión.
En el caso de utilizar switches no habrá colisiones ya que los switches almacenan las tramas en buffer y nunca transmiten mas de una trama a un segmento simultáneamente.

Pregunta 2 - RC (6 puntos)

Considere el protocolo TCP; ¿para qué es necesario estimar el Round Trip Time (RTT)?

Para fijar el valor del timeout de retrasmisión. Este timer es importante en los mecanismos de control de congestión. Los detalles están en la sección 3.5.3 y 3.7 Kurose 5a. Edición.

Pregunta 2 - IRC (7 puntos)

Explique el protocolo de acceso múltiple con evitado de colisiones (CSMA/CA) utilizado en las redes inalámbricas IEEE 802.11 (Wi-Fi) trabajando en modo infraestructura.

Se trata de un protocolo que ofrece la posibilidad que la estación que desea transmitir una trama de datos, primero reserve el medio (el aire) antes de hacerlo. Para ello se utilizan dos tramas de control, RTS (Request To Send) y CTS (Clear To Send), la primera enviada por quien desea enviar la trama de datos y la segunda enviada por el destino inmediato de dicha trama de datos, el AP (no tiene porqué ser el destino final), en respuesta a la primera. Si este intercambio ocurre de manera exitosa, se envía la trama de datos y se queda a la espera de una

tercera trama de control, ACK (Acknowlegment) si la misma fue recibida correctamente; ésta también es enviada por el destino inmediato de la trama de datos.

Frecuentemente se dice que las tramas RTS y CTS "limpian" el medio (aire). Ello se debe a que quienes escuchan al menos una de ellas deben "permanecer en silencio" (sin intentar acceder al medio) por un tiempo de al menos el informado por la trama escuchada. El tiempo de reserva del medio es informado en la trama RTS, pues quien la emite conoce cuánto durará el handshake y quien emite la trama CTS calcula el tiempo que informa a partir del que contiene la trama RTS. El uso de "reserva del medio" es opcional pero su respeto es obligatorio, caso contrario, se incumple la especificación del estándar.

Pregunta 3 - RC (6 puntos)

¿Por qué, en capa de enlace, se implementan protocolos con los que se sustentan servicios similares a los provistos en la capa de transporte?

Porque la capa de enlace se encarga de resolver la comunicación entre dos nodos, al igual que la capa de transporte, salvo que en la primera es entre dos nodos adyacentes (que no tienen porqué ser los nodos terminales) y en la segunda es entre los nodos terminales (extremos) de la comunicación.

Pregunta 3 - IRC (5 puntos)

En un contexto broadcast, describa un proceso de flooding, y explique como se puede transformar en flooding controlado.

Cada nodo que recibe un paquete de broadcast, lo duplica y reenvía a todos sus vecinos (excepto al vecino del que ha recibido el paquete). Este esquema logra entregar copias del paquete a todos los nodos en un grafo conexo, pero si hay ciclos, se pueden producir tormentas de broadcast. Se puede hacer flooding controlado usando varias técnicas, por ejemplo agregando números de secuencia a los paquetes o utilizando RPF (Reverse Path Forwarding): solo se reenvía el paquete si ha llegado por el enlace del camino (unicast) más corto al origen.

Pregunta 4 (10 puntos)

a) ¿Qué eventos son considerados por los mecanismos de control de congestión de TCP?

Eventos de pérdida: timeout o triple ACK duplicado
Eventos de cruce de umbral
Eventos de llegadas de ACK

b) ¿Cuál de estos eventos tiene mayor impacto en el tamaño de la ventana de congestión, y por qué?

Los eventos de pérdida: el timeout lleva al TCP al estado "slow start" y el triple ACK duplicado causa una reducción del tamaño de la ventana a la mitad y el cambio al estado de "recuperación rápida".

Pregunta 5 (8 puntos)

a) Describa las diferencias fundamentales entre el protocolo Neighbor Discovery y ARP para la resolución dinámica del mapeo entre direcciones de capa 2 y capa 3.

ND utiliza Multicast (IPv6), mientras que ARP usa broadcast (Ethernet).
ND forma parte de los mecanismos de base de IPv6, mientras que en IPv4 se utilizan diferentes mecanismos para alcanzar funcionalidades similares: ARP, ICMP *router discovery*, e ICMP *redirect*.
ND cumple más funciones que ARP, como por ejemplo encontrar routers y permitir a éstos publicar prefijos (autoconfiguración).

b) Analice, desde el punto de vista de la robustez y seguridad, las mejoras de Neighbor Discovery e indique si considera que es mejor o peor protocolo de forma fundamentada.

Si bien realizan funciones similares, se pueden señalar algunos aspectos:

- El mecanismo *neighbor unreachability detection* de IPv6 mejora la entrega de paquetes en presencia de routers y/o enlaces con fallas, y también soporta nodos en los que cambian las direcciones link-local. Por ejemplo, no se producen problemas equivalentes a los fallos de caches de ARP por nodos móviles. IPv4 no tiene ningún mecanismo similar a *neighbor unreachability detection*.
- Dado que Neighbor Discovery realiza la resolución de direcciones a nivel ICMP, es menos dependiente del medio que ARP, y por lo tanto se pueden utilizar los mecanismos de seguridad y autenticación estándares para IP.

Problemas Prácticos

Problema 1 (30 puntos)

Se considera la red presentada en la figura, correspondiente a una empresa que cuenta con dos departamentos (Técnico y Ventas) con subredes separadas, y direcciones IP públicas. Las direcciones IP asignadas a las interfaces Ethernet1/0 y Ethernet 2/0 del *Router_ppal*, son las primeras de cada rango de direcciones asignadas a cada una de las subredes. Los PCs de los departamentos, tienen como *default gateway* a la interfaz correspondiente de *Router_ppal*, y la máscara de subred de las interfaces de los PCs es /25.

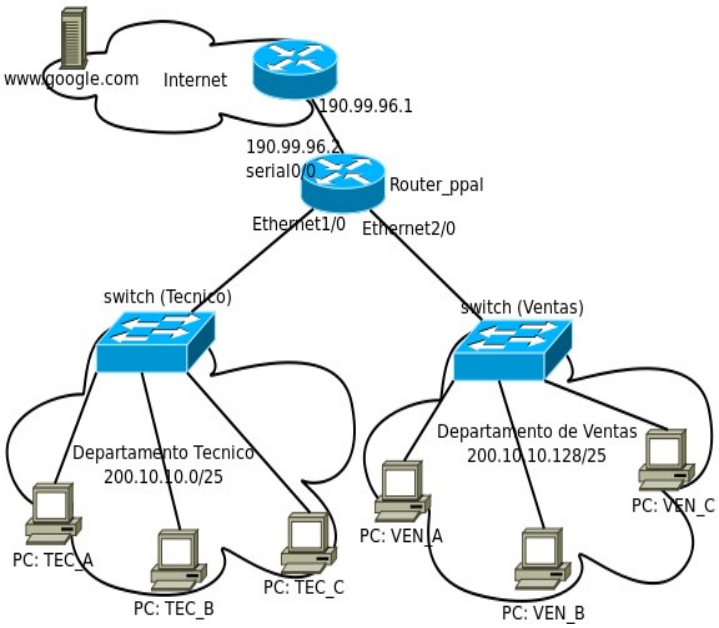
Se pide:

a) ¿Qué dirección IP tienen asignadas las interfaces de interconexión con el router *Router_ppal* (Ethernet1/0 y Ethernet2/0) para cada una de las subredes?

b) ¿Cuántos dispositivos de red (sin contar *Router_ppal*) pueden conectarse en cada una de las subredes asignadas a los Departamentos?

c) Suponiendo que el router *Router_ppal* se encuentra configurado únicamente con rutas estáticas, especifique su tabla de *forwarding* para que permita conectividad total entre los departamentos y entre éstos e Internet. Especifique la tabla con el siguiente formato: *red destino*, *máscara de subred*, *dirección IP del gateway* e *interfaz*.

d) Suponga que la empresa utiliza un protocolo EGP (*Exterior Gateway Protocol*, por ejemplo BGP) ¿qué prefijos publicará a su proveedor, buscando minimizar el tamaño de la publicación?



e) Indique las tramas Ethernet que es necesario transmitir en la red para enviar un segmento UDP (contenido en un único datagrama IP), desde el equipo `TEC_A` con destino al equipo `VEN_C`. Para cada *trama* indique dirección MAC origen y destino, y qué función cumple. Para la o las tramas que contienen un datagrama IP en su carga útil, especifique el contenido relevante del cabezal IP. (ver nota 1).

f) ¿Qué diferencias existen para trasmitir un segmento UDP con origen el mismo equipo `TEC_A` y destino `www.google.com` en Internet?

Nota:

1. Suponga que las tablas ARP de todos los dispositivos se encuentran inicialmente vacías. El equipo `X` de Ventas tiene la dirección IP `VEN_X` y la dirección MAC `MAC_VEN_X`, y análogamente para las direcciones de los equipos del departamento Técnico. Las interfaces del Router_ppal tienen las direcciones MAC `MAC_rppal_<nombre interfaz>`.

Solución:

a) `Ethernet1/0: 200.10.10.1 porque es la interfaz que conecta con la subred 200.10.10.0/25 y según la letra se debe elegir la dirección mas baja de la subred para esta interfaz. Ethernet2/0: 200.10.10.129 es la interfaz que conecta con la subred 200.10.10.128/25 Como se indica en las notas, la dirección más baja del rango, es la utilizada como dirección de red`

b) `Se pueden conectar 125 dispositivos. Como las subredes son /25 hay un total de 128 direcciones disponibles de la cuales dos se utilizan para la direccón de red y de broadcast y una para el router.`

c)

Red destino	máscara de subred	gateway	interfaz
200.10.10.0	255.255.255.128	*	Ethernet1/0
200.10.10.128	255.255.255.128	*	Ethernet2/0
default	0.0.0.0	190.99.96.1	serial0/0

d) Publica 200.10.10.0/24 sumarizando las dos subredes /25 en una /24 y de esta manera minimizando el tamaño de la publicación ya que publica un solo prefijo en lugar de dos. Esto puede realizarse por ser las redes /25 contiguas.

e) Se quiere enviar un segmento UDP desde TEC_A a la IP VEN_C.
Como en la tabla de forwarding de TEC_A solo hay una entrada default hacia Ethernet1/0 la trama se debe enviar con destino la MAC de Ethernet1/0 y para esto debo utilizar ARP para obtener esta dirección.
A continuación se muestran las tramas que se envían en la red:

1 – MAC origen MAC_TEC_A, MAC destino FF:FF:FF:FF:FF:FF. Mensaje ARP request preguntando por la MAC de la IP 200.10.10.1
.
2 – MAC origen MAC_rppal_Ethernet1/0, MAC destino MAC_TEC_A. Mensaje ARP reply respondiendo que la IP 200.10.10.1 pertenece a la MAC MAC_rppal_Ethernet1/0

3 – MAC origen MAC_TEC_A, MAC destino MAC_rppal_Ethernet1/0. Datagrama IP (que contiene el segmento UDP) con origen TEC_A y destino VEN_C.
Este datagrama es obtenido por el router y viendo su tabla de forwarding decide que debe enviarlo por la interfaz Ethernet2/0. Para esto, además, debe obtener la MAC del host con IP VEN_C.

4 – MAC origen MAC_rppal_Ethernet2/0, MAC destino FF:FF:FF:FF:FF:FF. Mensaje ARP request preguntando por la MAC de la IP VEN_C.

5 - MAC origen MAC_VEN_C, MAC destino MAC_rppal_Ethernet2/0. Mensaje ARP reply respondiendo que la IP VEN_C pertenece a la MAC MAC_VEN_C.

6 - MAC origen MAC_rppal_Ethernet2/0, MAC destino MAC_VEN_C. Datagrama IP (que contiene el segmento UDP) con origen TEC_A y destino VEN_C.

f) Primero debemos obtener la IP correspondiente a www.google.com mediante una consulta DNS. Con esto podemos armar el datagrama IP con la dirección obtenida como destino. Luego, el mecanismo es el mismo, se debe hacer la misma consulta ARP y enviar el datagrama IP en una trama Ethernet igual que la parte anterior.
Finalmente, el router, a partir de la entrada default de su tabla de forwarding envía el segmento por la interfaz serial0/0. Notar que como no conocemos la tecnología del enlace al ISP (PPP,HDLC,ATM...), no es posible especificar mecanismos de descubrimiento de direcciones de capa de enlace (análogos a MACs en ethernet).

Problema 2 (30 puntos)

Se considera la implementación de ARP en un host con una única interfaz Ethernet. ARP (Address Resolution Protocol) es el servicio (y protocolo) que implementa el stack TCP/IP de un sistema operativo para resolver dinámicamente el mapeo de direcciones de capa 3 a direcciones de capa 2 y viceversa.

a) Implemente el servicio ARP en base a las siguientes primitivas, asegurándose la implementación de la siguiente interfaz al Sistema Operativo:

interfaz:

```
mac getMAC(addr ip);
```

primitivas:

```
mac whatsMyMAC();
```

a)

```
char* assembleMessage(destination, source, payload);
int parseMessage(message, destination*, source*, payload*);
int sendRAW(char* message);
message* listenRAW(); //bloqueante
int getProtocol(char* message);
void setProtocol(char* message, int protocol);
sleep(int t); // t se especifica en milisegundos
```

Se deberá especificar, en un lenguaje de alto nivel, el funcionamiento de dicho servicio. También deberá especificar lo siguiente:

- los tipos de datos de los parámetros `destination` y `source` de acuerdo a su solución.
- los tipos, estructuras de datos y funciones auxiliares que necesite para implementar su solución.

La primitiva `setProtocol` interactúa con el cabezal del mensaje y modifica el campo que define como interpretar el payload de dicho mensaje.

El mapeo debe expirar a los 5 segundos.

b) Además de realizar una consulta ARP explícita para aprender las relaciones entre direcciones de capa 3 y capa 2, un *host* puede aprender estas relaciones a partir de las consultas ARP de otros *hosts.* Especifique, en lenguaje de alto nivel, las modificaciones que debe realizar a la solución de la parte a) para agregarle esa funcionalidad.

c) Describa qué riesgos de seguridad introduce su solución de la parte b).

Solución:

a) y b) Se da la solución a ambas partes en el mismo código.
La solución tiene dos componentes, una función invocada por el cliente (“requester”), y un demonio que responde paquetes ARP (“listener”).

```
Map <ip, {mac, time}> cache;

//requester
mac getMAC(addr ip) {
        if (cache[ip] && getTime()-cache[ip].time<=5) return cache[ip];
        payload p=assemble_arp_payload(whatsMyIP, ip); //func. Auxiliar arma payload ARP
        char *m=assembleMessage(MAC_BCAST, whatsMyMAC(), p);
        setProtocol(m, PROTO_ARP);
        sendRAW(m);
        char *ret;
        char *dest;
        char *source;
        repeat
                ret = ListenRAW();
                parseMessage(ret, dest, source, void *)
        until (getProtocol(ret)==PROTO_ARPRESP && dest==whatsMyMAC());
        cache[ip] = {source, getTime()};
        return source;
}

//listener
while (1) {
        char *m=ListenRAW();
        char *dest;
        char *source;
        char *payload;
        if (getProtocol(m)==PROTO_ARP && (dest==MAC_BCAST || dest==whatsMyMAC())) {
                parseMessage(ret, dest, source, payload);
                IP ipemitter = getIPemitter(payload);   //func. Auxiliar parsea el payload ARP
                IP iprequested =  getIPrequested(payload); //func. Auxiliar parsea el payload ARP
                cache[ipemitter]={source, getTime()};  // <------------------parte B
                if iprequested==whatsMyIP() {
                        char *ret=assembleMessage(source, whatsMyMAC()):
                        setProtocol(ret, PROTO_ARPRESP);
                        sendRAW(ret);
                }
        }
}
```

c) Un atacante puede generar generar solicitudes ARP indicando como IP origen la IP de otro nodo. Los que usen ese paquete ARP para inicializar su mapeo, dirigirán el tráfico destinado al IP víctima hacia el nodo atacante.