Introducción a las Redes de Computador{ae}s y Comunicación de Datos

Solución – febrero de 2012

(ref: sirc1202.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.
• 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).
• 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) El campo Rcv Window permite implementar el *control de flujo* en TCP. De acuerdo al RFC 793: *"TCP provides a means for the receiver to govern the amount of data sent by the sender. This is achieved by returning a "window" with every ACK indicating a range of acceptable sequence numbers beyond the last segment successfully received. The window indicates an allowed number of octets that the sender may transmit before receiving further permission."*

b) Diferentes técnicas, desarrolladas por Van Jacobson y documentadas en el RFC 2001 implementan el control de congestión, a saber: Slow Start, Congestion Avoidance, Fast Retransmit y Fast Recovery. En su conjunto representan una combinación de medidas distribuidas, que de forma cooperativa, tratan de repartir de forma equitativa el ancho de banda disponible entre las conexiones que lo utilizan.

c) No, UDP no implementa control de flujo o de congestión alguno. UDP busca, con el mínimo overhead posible, brindar acceso a los servicios crudos que brinda IP de conectividad end-to-end. UDP agrega el nivel de multiplexado brindado por los puertos, pero no ofrece control de flujo, siendo responsabilidad de la aplicación su implementación en caso de ser requerido.

Pregunta 2 (puntos)

a)

Paso	Origen	Destino	Información
1	host1.mydomain.com.uy	dns.mydomain.com.uy	Query: ¿IP asociada a www.google.us?
2	dns.mydomain.com.uy	root server	Query: ¿IP asociada a www.google.us?
3	root server	dns.mydomain.com.uy	Response: Consultar a TLD de us. Su IP es X.Y.W.Z
4	dns.mydomain.com.uy	X.Y.W.Z	Query: ¿IP asociada a www.google.us?
5	X.Y.W.Z	dns.mydomain.com.uy	Response: Consultar a dns.google.us. Su IP es A.B.C.D
6	dns.mydomain.com.uy	A.B.C.D	Query: ¿IP asociada a www.google.us?
7	A.B.C.D	dns.mydomain.com.uy	Response: es E.F.G.H
8	dns.mydomain.com.uy	host1.mydomain.com.uy	Response: es E.F.G.H

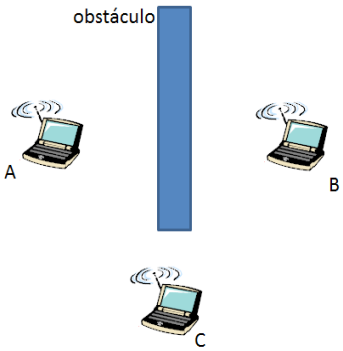
b)

Paso	Origen	Destino	Información
1	host1.mydomain.com.uy	dns.mydomain.com.uy	Query: ¿IP asociada a host2.google.us?
2	dns.mydomain.com.uy	A.B.C.D	Query: ¿IP asociada a host2.google.us?
3	A.B.C.D	dns.mydomain.com.uy	Response: es I.J.K.L
4	dns.mydomain.com.uy	host1.mydomain.com.uy	Response: es I.J.K.L

Pregunta 3 (puntos)

a) User Agents y Mail Servers.
User Agent: Permite componer, leer y editar mensajes de correo electrónico. Envía y recibe correos hacia y desde los Mail Servers
Mail Servers: Contiene mailboxes donde se guardan los mensajes destinados a cada usuario definido en el dominio de correo electrónico que gestiona. Manejo de colas de correos para el envío a otros Mail Servers, a los User Agents y para distribuir a los mailboxes propios.
b) SMTP y Mail Access Protocols: POP3, IMAP, HTTP
c) SMTP: envío de correo desde el user agent hacia el mail server y, entre mail servers. POP3: para la recepción de mensajes en el User Agent desde el Mail Server. Permite bajar los mensajes y eventualmente dejar copia en el Server. IMAP: mayores prestaciones al anterior, al poder organizar carpetas en el Server y sin la necesidad de bajar los correos al programa cliente. HTTP: para el acceso a servcicios Webmail. Técnica que se ha masificado en los últimos años. Permite el envío y recepción de correos, organización en carpetas, entre otras funcionalidades.

Pregunta 4 (puntos)



El problema de la estación oculta ocurre en redes inalámbricas cuando hay más de dos nodos. El nodo C escucha al nodo A y al nodo B. Pero como hay un obstáculo en el medio, los nodos A y B no se escuchan entre sí. Por lo tanto pueden enviar información a la vez e interferirse y no tienen forma de darse cuenta.

Pregunta 5 (8 puntos)

a) El primer motivo es el contar con un mayor espacio de direcciones (al usar direcciones de 128 bits en vez de 32). Además, podrá deshacerse parte de la complejidad a nivel de routing por volver a routing jerárquico. La conectividad end-to-end también está limitada actualmente, algo que podremos obtener utilizando IPv6. Procesamiento más simple de encabezados y opciones que permiten agregar calidad de servicio son valores agregados adicionales.

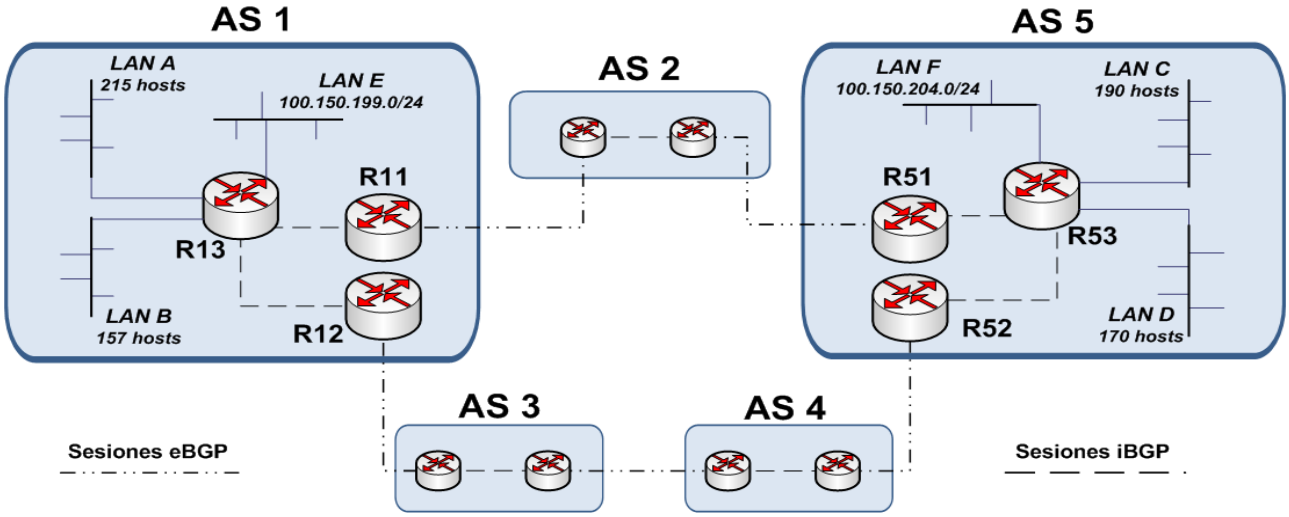
b) El agotamiento de direcciones IP existe desde antes de hablar de IPv6. CIDR y la utilización de máscaras en el ruteo abordó el problema de agotamiento de direcciones IP. Para cuando se hizo inminente la necesidad de un nuevo protocolo, se popularizaron diferentes técnicas para optimizar el uso de direcciones IP. Se definieron los conceptos de direcciones IP privadas y públicas. Esto permitió

conectar redes completas tras una única dirección IP pública. Esto se acompañó con la implementación de NAT y PAT, así como, proxies y gateways para protocolos específicos. También se avanzó con la implementación de nuevos servicios y protocolos que evitan la conectividad end-to-end directa (como skype) y de todas formas, permiten la prestación de servicios.

c) **Link Local Unicast** – identifica una única interfaz y es alcanzable en el dominio de broadcast de la misma
Unique Local Unicast – identifica una única interfaz, y es alcanzable en unidades administrativas que provean el routing adecuado
Global Unicast – identifica una única interfaz y es alcanzable en Internet (v6)

Problemas Prácticos

Problema 1 (30 puntos)



a)
Lan A 100.150.200.0/24
Lan B 100.150.201.0/24

Lan C 100.150.202.0/24
Lan D 100.150.203.0/24

b)
AS 1 anuncia 100.150.200.0/23 y 100.150.199.0/24
AS 5 anuncia 100.150.202.0/23 y 100.150.204.0/24

c)
Los mensajes BGP recibidos en R11 y R12, de UPDATE son:

En R11:

SubRed	**Next-AS**	**AS-Path**
100.150.204.0/24	AS2	AS2-AS5
100.150.202.0/23	AS2	AS2-AS5

En R12:

SubRed	**Next-AS**	**AS-Path**
100.150.204.0/24	AS3	AS3-AS4-AS5
100.150.202.0/23	AS3	AS3-AS4-AS5

d) El camino por AS2. Porque tiene el AS-PATH mas corto.

e) Si un router ve que su número de AS esta contenido en la lista, no aceptará el anuncio.

Problema 2 (30 puntos)

a)

- **`echo request`**: se envía uno en cada paso hacia el nodo destino pero comenzando con ttl=1 y aumentando en 1.
- **`ttl expired`**: un router intermedio devolverá este mensaje cuando el ttl del mensaje ICMP haya expirado, se devuelve este mensaje cuando aún no se llegó al nodo destino.
- **`echo response`**: una vez que se alcanza el nodo destino, devuelve este mensaje.

b)

```
traceroute(destino: direccionIP, maxHops: int, timeoutIntento: int) {
   bool fin = false;
   int hopsIntento = 1;
   while (!fin && hopsIntento <= maxHops) {
      try {
         char* echoRequest = armarMensajeICMP(myIP, destino, 8, 0, hopsIntento, "");
         iniciarTimer(timeoutIntento);
         enviarDatagramaRed(echoRequest);
         bool llegaRespuesta = false;
         while (!llegaRespuesta) {
            char* mensaje = obtenerDatagramaRed(obtenerTiempoRestanteTimer());
            if (esMensajeICMP(mensaje))
            {
               int tiempoTranscurrido = timeoutIntento - obtenerTiempoRestanteTimer();
               direccionIP origen;
               direccionIp destino;
               int tipo;
               int codigo;
               int ttl;
               char* datos;
               obtenerDatosMensajeICMP(
                     mensaje, origen, destino, tipo, codigo, ttl, datos);
               if (tipo == 11 && codigo == 0 && destino == myIP
                     && es_prefijo(datos, echoRequest) {
                  // time exceeded
                  print(hopsIntento + " " + origen + " " + tiempoTranscurrido);
                  llegaRespuesta = true;
               } else if (tipo == 0 && codigo == 0 && destino == myIP) {
                  // echo reply
                  print(hopsIntento + " " + origen + " " + tiempoTranscurrido);
                  llegaRespuesta = true;
                  fin = true;
               }
               // de lo contrario, el mensaje no era uno de los esperados, se descarta
            }
         }
         detenerTimer();
      } catch (TimeoutException) {
         // el router de este paso no responde
         print(hopsIntento + " * *");
      }
      hopsIntento++;
   }
}
```

c) Se debe enviar un datagrama UDP a la IP destino, indicando un número de puerto no utilizado comunmente (por ejemplo 33434). Los datagramas comienzan con TTL=1 y luego aumentando en uno. Los mensajes ICMP que envían los routers intermedios son iguales: time exceeded. Sin embargo, cuando el datagrama llega al nodo destino, no responderá con echo reply, sino con port_unreachable, debido a que el puerto indicado no debería estar en uso.

Se necesita un parámetro extra: el puerto UDP, ya que si este estuviera en uso en el nodo destino, el nodo no responderá con port unreachable. Por lo tanto se debería permitir enviar como parámetro el puerto a utilizar.