FACULTAD DE INGENIERIA
Universidad de Buenos Aires

66.62 Redes de Computadoras

Ejercicios de parcial

(para el 2do parcial)

Matsunaga, Nicolás

1.er cuatrimestre 2014

Índice

1. DNS **2**

2. Routing Protocols **3**

3. TFTP y FTP **3**

4. HTTP , Webservices **3**

5. MAIL **4**

6. SNMP **5**

7. QoS, VoIP **6**

8. Seguridad **6**

9. General **7**

10. Homework Extra Bonus **8**
10.1. FTP 8
10.2. SNMP 8

1. DNS

1. Explique sintéticamente que diferencia existe entre un servidor DNS primario y uno secundario. Cuántos puede haber de cada tipo? Ambos son autoritativos?

2. Explique como funciona la resolución inversa en DNS. Que registros se involucran? Quien es responsable de administrar esa información?

3. De un ejemplo de cómo se configura una delegación de zona `research.mit.edu` a partir de la zona `mit.edu`. Indique que registros se utilizan y cuáles son sus valores en el caso que `research.mit.edu` tenga 2 servidores DNS autoritativos.

4. Suponga que el administrador de un server DNS primario para una cierta zona realiza cambios en la información de la zona pero olvida actualizar el número de serie del registro SOA.

   a) ¿Qué problema se presenta?
   b) ¿Cómo puede percibir un cliente del DNS la situación?
   c) Si la zona tiene 4 servers autoritativos, ¿qué porcentaje de las consultas serán resueltas correctamente?

5. Explique qué es el registro SOA, qué información contiene y cuál es su función.

6. Cuándo una respuesta a una consulta DNS va a ser autoritativa? y cuándo no sería autoritativa?

7. En que difiere un Servidor Autoritativo de un Servidor No Autoritativo para una determinada Zona?

8. En que difiere una consulta Iterativa de una Recursiva?

9. De dónde obtienen la información que brindan cada uno de estos servers?

   - DNS server primario
   - DNS server secundario
   - DNS server caching-only

10. Enumere los tipos de registros RR y describa sintéticamente la función de cada uno de ellos.

11. Cual es la diferencia entre Zona y Dominio DNS?

12. Cómo podría el sistema de DNS facilitar la distribución de carga de un sitio Web? Desarrolle.

13. Qué significa que la resolución inversa una IP sea consistente (Forward-confirmed reverse DNS)? De un ejemplo de situación en la que se podría romper la consistentcia y qué buena práctica recomendaría?. Qué problemas podría traer que haya inconsistencia?

2. Routing Protocols

1. Para cada uno de los Protocolos de Ruteo, indicar si es un Interior o Exterior GP, si usa Vector-Distance o LinkState, si propaga las rutas con netmask o no, si es abierto o propietario.

	IGP o EGP	VD o LS	Netmask?	Standard?
RIP				
RIP2				
OSPF				
EIGRP				
BGP				

2. Desarrolle

   a) Desarrolle al menos 3 ventajas de Rip versión 2 respecto de Rip Versión 1

   b) Desarrolle al menos 2 ventajas de los protocolos Link State respecto de los Distance Vector

3. Qué es un sistema autónomo , en el contexto de los problemas de ruteo?

   - Una computadora que puede rutear utilizando tablas configuradas estáticamente
   - Un conjunto de redes y routers bajo una única administración que mantiene consistente el ruteo interno
   - Una interred separada de la Internet

4. Cuáles son las diferencias entre los algoritmos de ruteo Vector Distance y los del tipo Link State? Realice una comparación entre ambos y de al menos un ejemplo de un routing protocol de cada tipo.

3. TFTP y FTP

1. FTP pasivo y FTP activo, en qué casos resulta conveniente cada uno?

2. Si usted está construyendo un sistema embebido (y además debe programarlo), con un microprocesador no muy potente y necesita realizar transferencias de archivos no muy grandes, qué elegiría implementar TFTP o FTP? Por qué?

4. HTTP , Webservices

1. Qué diferencia hay entra URL y FQDN? Para acceder a un servidor web, la dirección debe comenzar con www.?

2. Describa sintéticamente 3 diferencias entre http version 1.0 y version 1.1.

3. Se puede decir que HTTP tiene las siguientes características

   - Genérico
   - Stateless
   - Orientado a Objetos

   Explique el porqué de cada una

4. Supongamos una página escrita en HTML:

```
<HTML>
<TITLE>BIENVENIDO A LA FIUBA</TITLE>
<BODY BACKGROUND ="/images/back.gif">
<H1>FACULTAD DE INGENIERIA</H1><P>
<IMG SRC ="/images/edificio.gif"><P>
<A HREF="http://www.cnn.com/forecast/">
<IMG SRC ="http://www.cnn.com/images/cloudy.gif"></A><P>
<A HREF="carreras.html">
<IMG SRC ="/images/carreras.gif"></A><P>
</BODY>
</HTML>
```

   a) ¿Cuantas conexiones TCP utiliza el browser cliente (si usa HTTP 1.0) en total para transferir la totalidad de la información desde el Server WEB ?

   b) ¿Cual de los dos end-points (Browser ó Server Web) inicia cada una de las conexiones?

   c) ¿Cómo indica el Server WEB que el objeto se transmitió completamente?

5. Qué protocolo de transporte usa el HTTP? En qué port (por default) escucha el server HTTP? Describa la sintáxis del HTTP Request y del HTTP Response. Describa el procedimiento con el cual probaría rápidamente que un servidor web está activo si dispone sólo del comando telnet.

6. Describa la sintáxis de un URL genérico. Qué indica cada componente del URL? Aclare qué servicio de nombre se suele usar para resolver la asociación del hostname con la IP address?

7. Describa la sintaxis de un mensaje HTTP request genérico. Como debe cambiar ese requerimiento si se utiliza un proxy HTTP?

5. MAIL

1. Para qué sirve y qué protocolo habla un Relay Mail Server?

2. Qué se realizó para permitir el envió de archivos binarios y caracteres especiales por e-mail?

3. Compare

a) POP3 e IMAP4

4. Describa sintéticamente cómo es el proceso y cuáles son los protocolos involucrados en cada transacción para que un usuario@dominio1.com pueda enviarle un mensaje a un destinatario@dominio2.com.ar

5. Describa sintéticamente la arquitectura y los protocolos involucrados en el sistema de mail estándar sobre IP

6. Qué debe hacerse para que el usuario juan@cia.com.ar, cuando el server de mailbox donde está su cuenta esta conectado a la internet solo un rato por día, continúe pudiendo usar su address de e-mail normalmente?

7. Qué es SMTP? Describa el diálogo protocolar SMTP entre 2 MTAs.

6. SNMP

1. Enumere las operaciones posibles en SNMP versión 2, indicando para cada caso la entidad (nms o agent) que la puede generar y las PDUs asociadas.

2. Qué es y para que se usa SMI[1]? Qué es una MIB[2] y cómo se identifican los objetos en SNMP?

3. Qué tipo de variables existen en SNMP? Cómo se recorre la información en las tablas? (por ej, la dibujada a continuación) Qué PDU utilizaría una aplicación que "baja" esta información?

ifIndex	ifDescr	ifType	ifMTU	ifSpeed	...
1					
3					
7					
11					
...					
38					

4. Qué significan las siglas SNMP y cuál es la función del mismo (por qué se lo necesita)?

5. Qué tipo de información se administra mediante SNMP?. ¿Como se llama al conjunto de elementos que la componen, en que formato se la representa, como se organiza para un fácil direccionamiento de los mismos?

6. ¿Cuáles son los posibles tipos de operación especificadas por SNMP? Explique cómo opera cada una de ellas. ¿De qué maneras puede una plataforma de network management enterarse de eventuales cambios en el contenido de la información del dispositivo a administrar ?

[1]Structure of Management Information
[2]Management Information Base

7. ¿Como funciona la validación de operaciones entre agentes y estaciones de gestión ?. ¿ Cuál es su principal falencia de seguridad ?. ¿Que propondría Ud. Para resolverlo ?.

8. Justifique por que razón el protocolo SNMP funciona sobre UDP en lugar de utilizar TCP.

7. QoS, VoIP

1. **QOS & VoIP**. ¿Qué es el *delay jitter*?, ¿Por qué es más negativo para el tráfico de VoIP que para el tráfico de HTTP? ¿Qué mecanismo debe implementarse en el receptor para compensar el *delay jitter* y permitir la correcta reproducción de audio?

8. Seguridad

1. Cómo se puede firmar digitalmente un documento ?

   - Cifrando el mensaje.
   - Cifrando un hash de su contenido con la clave pública del destinatario
   - Cifrando un hash de su contenido con la clave privada del remitente

2. ¿Qué diferencia hay entre un firewall que funcione filtrando paquetes sin memoria (sin historia, o sin seguimiento de estado) o con ella? Para qué sirve la inspección con memoria o seguimiento de estado (stateful inspection)?

3. Explique y realice un diagrama del proceso de validación de la firma digital de un mensaje M. ¿Qué servicio de seguridad no provee la firma digital? ¿Qué es un certificado de clave pública, y cual es su utilidad?

4. Explique el principio de funcionamiento de los siguientes elementos criptográficos. Para cada uno de los servicios de seguridad, que elementos se requiere?

   - Hash
   - Cifrado simétrico
   - Cifrado asimétrico

5. En un firewall alguien coloca una única regla: Se impide el paso de paquetes TCP entrantes al perímetro protegido, si tienen en 1 el bit de SYN y en 0 el bit de ACK al mismo tiempo. ¿Qué efecto tiene esta regla?

6. Porqué se utiliza un sistema simétrico junto con uno de clave pública ?

   - Porque el de clave pública no sirve para encriptar.
   - Porque no es sencillo distribuir la clave en el simétrico.

- Porque el de clave pública es muy lento cifrando

7. Cómo se puede asegurar que sólo el destinatario conozca el contenido de un mensaje ?
   - Cifrando su contenido con la clave pública del destinatario .
   - Cifrando su contenido con la clave privada del remitente
   - Calculando un hash del mensaje y transmitiéndolo.
8. Ud. desea permitir las consultas al WWW originadas en la internet y dirigidas a un server ubicado detrás de un firewall. Especifique las reglas a instalar en la interfaz externa del firewall para permitir el funcionamiento correcto del sistema
   `Ej: Regla: Protocolo=TCP; Dirección=entrante; PortTCP=80; Acción=PERMITIR`
9. Sea un datagrama de tamaño 1500 Bytes, que transporta un segmento TCP correspondiente a una conexión del WWW dirigida al server interno A. En el curso de su transito a través de la internet, el datagrama es fragmentado en 3 partes del mismo tamaño aproximadamente. Posteriormente los fragmentos deben atravesar un firewall sin memoria. Indique qué sucede con cada uno de los 3 fragmentos en los siguientes casos:
   a) Si en el firewall se coloca una regla que bloquee el tráfico de IP dirigido al server A
   b) Si en el firewall se coloca una regla que bloquee el tráfico de TCP dirigido al port 80 de cualquier server interno
   c) idem 9*a*) pero el firewall tiene funcionalidad de reensamble de datagramas previo al filtrado.
   d) idem 9*b*) pero el firewall tiene funcionalidad de reensamble de datagramas previo al filtrado.

9. General

1. **Aplicaciones en TCP/UDP** Para cada aplicación, indique el protocolo(s) de transporte utilizado, el port(s) reservado(s) y describa sinteticamente la funcionalidad que provee:

Aplicación	TCP y/o UDP	Puertos resevados	Funcionalidad
TELNET			
FTP			
TFTP			
DNS			
SMTP			
SNMP			
HTTP			
DHCP			

10. Homework Extra Bonus

Esto no es obligatorio y queda a su voluntad.

Algunas se puedan contestar utilizando sólo el sniffer Wireshark y para otras habría que usar una regla de firewall, por ejemplo para hacer caer la conexión.

10.1. FTP

1. Describa paso a paso cuál es el procedimiento que se sigue para realizar una transferencia de archivos. Si se transfieren 4 archivos, ¿cuántas conexiones TCP son realizadas en total y cuántas existen en forma simultánea?

2. ¿Qué pasa en FTP si la conexión TCP que se está usando para una transferencia de datos se cae, pero la conexión TCP de control se mantiene?

10.2. SNMP

1. Explique brevemente que problemas resuelve SNMP V2 respecto SNMP V1.