Introducción a las Redes de Computadoras

Obligatorio 1 – 2010

Facultad de Ingeniería
Instituto de Computación
Departamento de Arquitectura de Sistemas

Nota previa - IMPORTANTE

Se debe cumplir íntegramente el "Reglamento del Instituto de Computación ante Instancias de No Individualidad en los Laboratorios", disponible en `http://www.fing.edu.uy/inco/pm/uploads/Ense%f1anza/NoIndividualidad.pdf`

En particular está prohibido utilizar documentación de otros grupos, de otros años, de cualquier índole, o hacer público código a través de cualquier medio (news, correo, papeles sobre la mesa, etc.).

Forma de entrega

Una clara, concisa y descriptiva documentación es clave para la evaluación de los trabajos entregados.

La entrega del obligatorio consiste en un único archivo `obligatorio1.tar.gz` que deberá a su vez contener los siguientes archivos:

- Un documento llamado `obligatorio1.pdf` donde se documente todo lo solicitado en el presente obligatorio.
- Los archivos correspondientes a la/s capturas de tráfico realizadas.

La entrega se realizará a través del sitio Web del curso, en la página `http://www.fing.edu.uy/inco/cursos/redescomp/entrega.html`

Fecha de entrega

Los trabajos deberán ser entregados antes del domingo 21 de marzo a las 23:30 horas. No se aceptará ningún trabajo pasada la citada fecha y hora. En particular, no se aceptarán trabajos enviados por e-mail a los docentes del curso, ni entregados en medios magnéticos en el instituto.

El sistema de entregas soporta múltiples entregas por grupo, llevando un histórico de las mismas. Se recomienda realizar una entrega vacía con tiempo, a los efectos de verificar que su sistema le permite entregar correctamente.

Observaciones

Todas las ejecuciones deberán ser realizadas en las máquinas virtuales distribuidas como parte del material del curso.

Toda vez que se pida la ejecución de un comando y una respuesta analice dichos resultados; la ejecución del mismo, incluyendo su invocación deberá ser parte de la respuesta.

Objetivo del Trabajo

Familiarizarse con conceptos básicos sobre redes e Internet y manejar herramientas para diagnóstico y *debug* de la red.

Herramientas

El obligatorio se desarrollará en un entorno GNU/Linux, para lo cual se dispone de máquina virtual. Este entorno tiene las herramientas necesarias ya instaladas, tales como:

- `ping`
- `traceroute`
- `wireshark` [1]
- `dig`

Se pide

1) Comando ping

Una manera de probar que se puede alcanzar otro *end system* es mediante la utilización del comando `ping`.

1. Investigue y documente el principio de funcionamiento del comando ping: `man ping`. ¿Qué protocolo utiliza?

2. Pruebe los siguientes comandos

```
ping -c 5 www.debian.org
ping -c 5 www.google.com
ping -c 5 www.adinet.com.uy
ping -c 5 www.presidencia.gub.uy
```

   Utilice *copiar-y-pegar* de la salida de cada uno de los comandos y conteste de forma fundamentada:

   a) ¿Cuál es el servicio con mejor tiempo de respuesta?
   b) Para cada instancia, ¿todas las salidas fueron iguales? de no ser así, ¿cómo explica las diferencias?
   c) Ejecute el primer comando pero ahora más de una vez. ¿Qué conclusión puede sacar de lo observado?

3. Tamaño de las pruebas

   a) ¿Cuál es el tamaño por defecto del mensaje enviado por el comando `ping`?
   b) Pruebe hacer pings con los tamaños 100, 1.000 y 10.000 a diferentes *hosts* y determine de forma fundamentada si el tamaño del mensaje incide en los tiempos observados.
   c) ¿Cuál es el tamaño máximo del mensaje enviado por el comando `ping`?

2) Comando traceroute

1. Investigue y documente el principio de funcionamiento del comando `traceroute`: `man traceroute`. ¿Qué protocolo/s utiliza?

2. Ejecute `traceroute` a cada uno de los hosts anteriores (punto 2 del apartado anterior).
   Utilizando *copiar-y-pegar* de la salida de los comandos fundamente cual es el host o router más próximo a su punto de acceso a la red, considerando la distancia basada en la cantidad de *hops* o saltos que atraviesan sus mensajes para llegar a c/*hop*. ¿Qué destinos fue posible alcanzar con la prueba `traceroute`?, ¿cómo podría explicar dicho comportamiento?

3. ¿Puede correlacionar los tiempos de respuesta medidos con el comando `ping` con la distancia medida en *hops*? Fundamente su respuesta.

4. Si comparamos las salidas de los comandos:

```
traceroute www.google.com
traceroute www.i.com.uy
```

¿Puede asociar a un *hop* particular la diferencia de los tiempos de respuesta?, ¿cómo explica este comportamiento?

5. Ejecute el comando:

```
traceroute -n www.google.com
```

¿Las diferentes líneas de la salida del mismo se despliegan a la misma velocidad con y sin la opción ***-n***?, ¿ello se puede relacionar con los tiempos de ida y vuelta de los paquetes?, ¿cómo explica este comportamiento?

6. ANTEL es el *ISP* nacional utilizado en las pruebas. ¿Qué otros *ISPs/carriers* internacionales utilizan sus pruebas? Fundaméntelo con las salidas de los comandos anteriores.

7. Un servidor *Looking Glass* es un *end system* que ejecuta un software que permite ver información de enrutamiento, permitiendo al usuario realizar pruebas como si estuviera localizado en dicho servidor.

   Realice pruebas del comando `traceroute` pero ahora seleccionando dos *Looking Glass* a su elección de [2], de manera de primero tomar uno como origen y el segundo como destino y viceversa.
   Documente los resultados obtenidos y trate de explicar las diferencias de comportamiento de las pruebas en un sentido y en el otro. Por ejemplo podría usar `Registro.br(AS22548)` (Brasil) e `Iber-X(AS12769)` (España) para las pruebas.

3) Comando dig

1. Investigue y documente el principio de funcionamiento del comando `dig`: `man dig`.

2. Ejecute el comando

```
dig www.fing.edu.uy @164.73.32.2
```

Utilice *copiar-y-pegar* de la salida del comando y analice el resultado. ¿Qué otro nombre tiene el servidor Web de facultad? ¿Cómo lo indica el DNS?

3. ¿Con qué comando puede obtener la dirección de red de el o los servidores de correo de Gmail? Proponga de que formas se podría utilizar el DNS para balancear la carga de correo u otro servicio.

4. Analizando nuevamente la salida de la parte 2, ¿cuáles son los servidores de nombres del dominio `fing.edu.uy`? Las respuestas obtenidas, ¿son autoritativas? Justifique su respuesta.

5. Compare e interprete las salidas de los siguientes comandos

```
dig www.fing.edu.uy @200.40.220.254
```

```
dig www.fing.edu.uy @200.40.220.245
```

6. ¿Con que comando puede obtener el nombre del *host* cuya dirección IP es 200.40.30.218?

4) Captura de tráfico con Wireshark

1. ¿Cuál es la funcionalidad del software `Wireshark`?

2. Utilizando `Wireshark`, capture el tráfico generado cuando utiliza un navegador para acceder a la página `http://www.fing.edu.uy` (con el `Wireshark` y el navegador corriendo dentro de la máquina virtual).

3. Analice la captura de tráfico del punto anterior, ¿cuántas conexiones TCP se realizaron?

4. ¿Qué método HTTP se invocó?

5. Utilizando `Wireshark` para analizar el archivo de tráfico suministrado, responda las siguientes preguntas:
   a) ¿Qué agente se utiliza para navegar?
   b) ¿Qué objeto/URL no puede ser retornado por falta de privilegios?
   c) ¿Se utiliza siempre el mismo navegador o más de uno?

NOTA:
Para facilitar los análisis con la herramienta `Wireshark`, pruebe las herramientas de análisis provistas (filtros).

Referencias y Bibliografía Recomendada

[1] Analizador de Tráfico Wireshark. Accesible en línea: `http://www.wireshark.org/`. Última visita: Marzo 2010.

[2] Listado de servidores *Looking Glass*. Accesible en línea: `http://www.traceroute.org/#Looking%20Glass`. Última visita: Marzo 2010.