Departamento de
Automática y Computación
Automatika eta
Konputazio Saila

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

Práctica 9 – IP en LAN, fragmentación e ICMP

1- Objetivos

En esta primera sesión, se completarán conceptos básicos sobre el nivel de red en Internet relativos a la fragmentación de paquetes, Protocolo de Control de Mensajes de Internet y los efectos de la fragmentación en el tráfico de red.

2- Material

Para la realización de esta práctica necesitaremos el siguiente equipamiento de los armarios:

- 3 PCs.
- 1 Concentrador Ethernet.
- 2 cables categoría 5.

3- Avisos generales

En los ordenadores dispuestos para la realización de estas prácticas (PC A, B y C) se ha creado una cuenta de nombre `arss` y password `telemat`. Esta cuenta tiene permisos para ejecutar mediante el comando `sudo` ciertos comandos restringidos normalmente al superusuario.

Si quieren conservar cualquier fichero entre sesiones guárdenlo en una memoria USB, dado que no se asegura que los ficheros creados o modificados durante una sesión de prácticas se mantengan para la siguiente.

4- Análisis de tramas en un medio compartido

Configure en PCA y PCC una tarjeta de red, cada una con una dirección IP en el rango de direcciones 10.3.armario.0/24.

```
$ sudo ifconfig eth0 <ip> netmask <máscara>
```

Conecte PCA y PCC mediante el hub parcheado de su armario (consulte la documentación sobre los armarios):

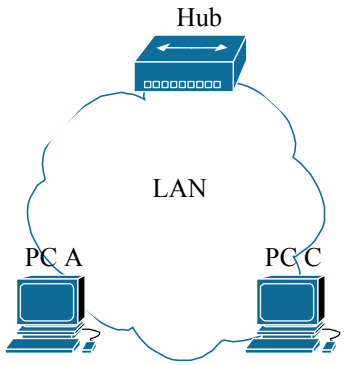

Figura 1. Conexión de 2 PCs en una misma LAN a un hub.

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

Compruebe que PCA puede hacer ping a la dirección IP de PCC, y que PCC puede hacer ping a la dirección IP de PCA.

Ponga Wireshark a capturar en PCC aplicando el filtro adecuado para ver únicamente mensajes ICMP.

Lance un ping de PCA a PCC de un único paquete. Detenga Wireshark en PCC y analice todos los campos correspondientes a la captura, utilizando la decodificación que de éstos ofrece Wireshark. Deberá ser capaz de identificar cada uno de los niveles de la pila de protocolos, indicando el tamaño de cada cabecera y su PDU.

Represente cada uno de los formatos identificados anteriormente rellenando sus campos con los valores hexadecimales capturados mediante Wireshark

Guarde estos resultados, los necesitará más adelante.

Modificando el tamaño de los paquetes

Lance un ping de PCA a PCC con un tamaño de datos de 1400bytes y otro de 1500bytes. ¿Qué diferencias encuentra entre ellos? Captúrelos mediante Wireshark y analice los resultados. ¿Qué valores han tomado ahora los Flags? Si no observa diferencias quizás debería eliminar el filtrado de mensajes ICMP que se indicó en el apartado anterior. Analice la captura realizada ayudándose de las siguientes cuestiones:

1. ¿Qué indica el campo Fragment Offset? ¿Cómo ha variado respecto el `ping` inicial?
2. Obtenga el MTU (Maximum Transfer Unit) de la interfaz de red por la que se han enviado los mensajes ICMP. ¿Tiene alguna relación el MTU con la fragmentación observada en el punto anterior? El comando `ifconfig` puede resultarle útil.
3. Para qué valor máximo del campo de datos ICMP no se produce fragmentación. Determínelo teóricamente y compruébelo de forma práctica.

Checkpoint 9.1: Realice un esquema de los formatos de tramas y datagramas en notación hexadecimal y compárelos con los resultados obtenidos anteriormente, resaltando el valor de los campos que indican fragmentación.

Para un tamaño de paquete de datos en ICMP de 17914bytes ¿Cuántos bytes se transmitirán por la red? Realice sus cálculos teóricos y verifíquelos utilizando `wireshark` o `tcpdump` para capturar un ping de PCA a PCC con un solo mensaje ICMP Request del tamaño indicado.

Calcule para este caso el throughput de la capa de enlace. ¿Coincide con el throughput teórico?¿Por qué? ¿Cuál sería el throughput para el caso de un `ping` al que no indicamos un tamaño determinado de datos ICMP?

Checkpoint 9.2: Muestre al profesor de prácticas los resultados obtenidos, indicando el número de tramas totales, los valores de los Flags y la secuencia de Fragment Offsets. Considerando la primera trama ¿Cuántos bytes corresponden a cabeceras y cúantos a datos? ¿Y en la transmisión total de los 17914bytes de datos? Calcule la eficiencia en este caso. Utilice la captura de su sniffer como ayuda.

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

6- Fragmentación y tráfico

Analice gráficamente, mediante Wireshark, el resultado de lanzar `pings` de 10 mensajes ICMP con 10 tamaños diferentes de paquetes de datos, hasta el máximo permitido por el comando `ping`.

Para ello seleccione en su menú la opción Statistics, IO Graphics. Emplee las opciones de configuración gráfica adecuadas para los ejes XY, de manera que obtenga una representación que le permita comparar resultados en relación al tráfico generado por cada tamaño de paquete enviado por ping. Pero esta representación de Wireshark ¿Corresponde a bytes de tramas Ethernet o a bytes de datos ICMP? Averígüelo.

Refleje en una tabla los distintos tamaños de paquete y el tráfico al que da lugar su fragmentación. Represente en una gráfica Tráfico(bits/seg) vs. Tamaño paquetes datos ICMP (bytes).

Consulte el manual de `ping` (`man ping`) y encuentre la forma de modificar el intervalo entre paquetes. Tabule nuevamente y represente gráficamente los resultados obtenidos. ¿Qué está pasando?

Checkpoint 9.3: ¿Cuál es el máximo tráfico que es capaz de generar con ping y la configuración de red de la figura 1? ¿Qué parámetros ha indicado a `ping` para lograrlo?

Obtenga una fórmula matemática que permita determinar el número de tramas transmitidas en el envío de un mensaje ICMP de longitud L bytes.

7- Interpretación correcta de las capturas de tramas Ethernet

Abra `wireshark` en PCA y PCC y póngalos a capturar filtrando los mensajes ICMP o los datagramas IP.

Lance un único mensaje ICMP Request de PCA a PCC con un tamaño de datos ICMP de 1475 bytes.

Detenga sus capturas y analícelas planteándose las siguientes cuestiones:

1. ¿Qué tamaño muestra la captura de Wireshark en PCA para el segundo fragmento correspondiente al ICMP Request? ¿Y en PCC? ¿Son valores diferentes?
2. ¿Qué tamaño muestra la captura de Wireshark en PCC para el segundo fragmento correspondiente al ICMP Reply? ¿Y en PCA? ¿Son valores diferentes?

Checkpoint 9.4: Muestre al profesor de prácticas a qué cree que se debe esta diferencia de bytes capturados a nivel de enlace en cada uno de los casos indicados.

Utilice como ayuda la documentación complementaria siguiente:

https://www.tlm.unavarra.es/mod/resource/view.php?inpopup=true&id=7915

Siga capturando con Wireshark tanto en PCA como en PCC y aplique el filtro adecuado para ver únicamente mensajes ICMP e IP.

Desde PCC lance un ping de 2945bytes, pero esta vez a su propia dirección IP. ¿Qué ocurre? ¿Qué interfaz deberá indicar a Wireshark para que capture los mensajes ICMP generados por el

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

comando ping? ¿Ha capturado Wireshark el mismo número de tramas que en el caso anterior? ¿Por qué? ¿En qué nivel de la pila de protocolos se está capturando realmente? ¿Qué cabeceras observa?

Checkpoint **opcional**: Muestre al profesor de prácticas los resultados obtenidos y justifíquelos. ¿Qué tamaño de paquete debería indicar a ping para que se produjera fragmentación?

8- Conclusiones

Hemos visto la importancia del tamaño de los paquetes en la eficiencia y el throughput de un canal Ethernet, así como la influencia de las cabeceras correspondientes a cada uno de los niveles de la pila de protocolos por los que discurren hasta su transmisión al medio físico.

En la siguiente sesión se plantearán distintos escenarios donde seguiremos analizando los efectos de la fragmentación y en qué medida afecta a los dispositivos de red.