



PONTIFICIA UNIVERSIDAD JAVERIANA
FACULTAD DE INGENIERIA
DEPARTAMENTO INGENIERIA DE SISTEMAS

Comunicaciones y Redes
Período Académico 2018-30

Bogotá, 31 de agosto de 2018

PROYECTO 1

Entrega : 3 de octubre de 2018 a las 9:00AM.

Sustentación : 3 de octubre y 5 de octubre de 2018, en el horario acordado.

Identificación de Red

Objetivos

- Investigar el funcionamiento del protocolo Ethernet
- Investigar sobre métricas de red
- Poner en práctica conceptos de protocolos de capa de enlace y red

Descripción

Se va a desarrollar una aplicación que permita capturar los *frames* enviados de una máquina a otra, mostrando en detalle cada uno de los campos que los componen, de manera similar a como lo hacen los analizadores de protocolos (*sniffers*) como por ejemplo, Wireshark¹.

El analizador de protocolos debe estar en capacidad de desencapsular y mostrar cada uno de los campos que componen un mensaje ICMP, IPv4 y Ethernet, como se observa en la figura 1; por lo tanto, se deben tomar como referencia los estándares, se sugieren los siguientes pero no limitarse a ellos: RFC 792 (ICMP), RFC 791 (IP), RFC 894 (Transmisión de Datagramas IP sobre Redes Ethernet) y <https://www.ietf.org/proceedings/46/I-D/draft-kaplan-isis-ext-eth-00.txt>.

The screenshot shows the Wireshark interface with a packet capture list on the left and a detailed view of a selected packet (Frame 19) on the right. The packet list shows various protocols including ARP, NBNS, ICMP, and IP. The details pane for the selected packet (Frame 19) shows the Ethernet II header, Internet Protocol (IP) header, and Internet Control Message Protocol (ICMP) header. The ICMP header shows it is an Echo (ping) request with a sequence number of 0x00000000 and a length of 56 bytes. The packet is captured on the interface 10.6.2.158.

No.	Time	Source	Destination	Protocol	Info
15	1.825248	00:14:38:ba:bf:0b	ff:ff:ff:ff:ff:ff	ARP	who has 10.6.2.4? Tell 10.6.2.48
16	1.936636	10.6.2.106	10.6.2.255	NBNS	Name query NB ISATAP<00>
17	2.220009	10.6.2.90	10.6.2.255	NBNS	Name query NB NPFD23f4<00>
18	2.686634	10.6.2.106	10.6.2.255	NBNS	Name query NB ISATAP<00>
19	2.916337	10.6.2.158	10.6.2.66	ICMP	Echo (ping) request
20	2.916337	10.6.2.158	10.6.2.66	IP	Fragmented IP protocol (proto=ICMP 0x01, off=0)
21	2.916337	10.6.2.158	10.6.2.66	ICMP	Echo (ping) reply
22	2.916337	10.6.2.158	10.6.2.66	ICMP	Echo (ping) reply
23	2.973027	10.6.2.90	10.6.2.255	NBNS	Name query NB NPFD23f4<00>
24	3.158859	00:14:38:5b:f6:95	ff:ff:ff:ff:ff:ff	ARP	who has 10.6.2.212? Tell 10.6.2.11
25	3.161049	00:16:41:2b:c3:ad	ff:ff:ff:ff:ff:ff	ARP	who has 10.6.2.3? Tell 10.6.2.212
26	3.215402	10.6.2.66	65.55.71.180	HTTP	21797 > 1863 [ACK] Seq=64612 Win=64612 Len=0
27	3.219456	00:14:38:5b:f6:95	ff:ff:ff:ff:ff:ff	ARP	who has 10.6.2.144? Tell 10.6.2.11
28	3.220820	00:01:6c:9c:24:1d	ff:ff:ff:ff:ff:ff	ARP	who has 10.6.2.3? Tell 10.6.2.144
29	3.237705	00:01:6c:9c:24:1d	ff:ff:ff:ff:ff:ff	ARP	who has 10.6.2.3? Tell 10.6.2.144
30	3.288580	65.55.71.180	10.6.2.66	HTTP	21797 > 1863 [ACK] Seq=64612 Win=64612 Len=0
31	3.304797	00:01:6c:9c:24:1d	ff:ff:ff:ff:ff:ff	ARP	who has 10.6.2.3? Tell 10.6.2.144
32	3.476937	10.6.2.66	65.55.71.180	TCP	21797 > 1863 [ACK] Seq=64612 Win=64612 Len=0
33	3.736541	10.6.2.90	10.6.2.255	NBNS	Name query NB NPFD23f4<00>
34	3.916509	10.6.2.66	10.6.2.158	IP	Fragmented IP protocol (proto=ICMP 0x01, off=0)
35	3.916509	10.6.2.66	10.6.2.158	ICMP	Echo (ping) request

Figura 1. Captura de mensajes con el analizador de protocolos Wireshark

¹ <https://www.wireshark.org/>

Adicionalmente a la captura y visualización de los mensajes, la aplicación debe graficar el *throughput* de la red en tiempo real utilizando un odómetro, como se ve en la figura 2.

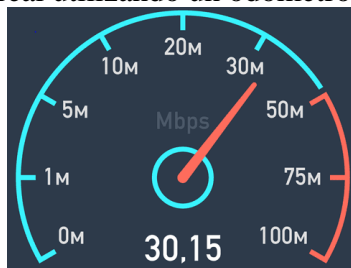


Figura 2. Ejemplo de odómetro para medir el *throughput* de la red

De la figura 2 se puede deducir que la capacidad máxima de la red es de 100 Mbps y que su uso en el momento que se realizó la captura es aproximadamente el 30%.

Al analizador de protocolos se le pueden agregar otras métricas de red que pueden dar estadísticas adicionales que le darían valor agregado al proyecto.

La sustentación se realizará en el laboratorio los días miércoles 3 y viernes 5 de octubre de 2018 en la hora de clase según franja de tiempo seleccionada por el grupo. TODOS deben entregar el proyecto en medio electrónico el miércoles 3 de octubre de 2018 a las 9:00AM.

Entrega y condiciones

Se debe entregar el código fuente con los debidos comentarios. Los archivos deben estar acompañados de un documento en PDF² que utilice la plantilla para escritura de artículos IEEE, en donde se describa el propósito de la aplicación, los protocolos utilizados, el diseño de la aplicación (Utilizar diagramas UML y descripción de los mismos), el escenario que se definió para las pruebas (variables consideradas y resultados obtenidos). Así mismo se debe contar con las conclusiones correspondientes y las referencias.

En ningún caso se considera documentación al código fuente.

La sustentación se realizará en el laboratorio de acuerdo a los horarios elegidos y deben estar presentes todos los integrantes del grupo.

El proyecto debe estar probado con anterioridad en el laboratorio, recuerden traer todos los elementos necesarios para el funcionamiento de la aplicación. La hora de sustentación no puede ser empleada para la instalación del proyecto.

El código debe corresponder al grupo, por lo tanto cualquier préstamo, intercambio, etc. que evidencie que el código o parte de él se encuentre en Internet o que haya sido realizado por alguien diferente al grupo será considerado como fraude.

² Portable Document Format

RÚBRICA

Grupo						
Desencapsulado ICMP (10%)						
Desencapsulado IPv4 (20%)						
Desencapsulado Ethernet (20%)						
<i>Throughput</i> (20%)						
Diseño de la aplicación (UML, descripción) (15%)						
Escenarios de prueba (15%)						
Resultados (10%)						