Laboratorio Niveles de Red y Enlace

Redes de Comunicaciones (TB067)

Comunicación de Datos (86.12)

Los ejercicios se deben realizar en el orden que se presentan.

1. Responda las siguientes preguntas introductorias a las aplicaciones ping y traceroute.

a) ¿Cuál es la utilidad de las aplicaciones `ping` y `traceroute`?

b) Describa el principio de funcionamiento de ambas aplicaciones.

2. Fragmentación

IMUNES. Experimento: `imunes-examples/Ping/ping.imn`

a) Antes de iniciar el experimento, cambie el MTU de las interfaces como se indica en el siguiente cuadro:

Router	Interfaz	MTU
router0	eth1	1400
router1	eth0	1400
router6	eth1	1000
router7	eth0	1000

b) Inicie el Wireshark en `pc1` y en `server`, luego ejecute los comandos:

```
ping -s 1400 -M do 10.0.8.10
ping -s 1000 -M do 10.0.8.10
```

Analice las diferencias de la respuesta a cada comando y en las capturas.

c) Con el Wireshark corriendo en `pc1` y en `server` ejecute el comando:

```
ping -c 1 -s 1500 10.0.8.10
```

Analice la fragmentación que se produjo y estudie los campos relevantes de ambas capturas.

3. Pruebas de *ping*

IMUNES. Experimento: `imunes-examples/Ping/ping.imn`

a) Corra el Wireshark en la `pc1`, y luego verifique la disponibilidad de `server` (10.0.8.10) desde `pc1` ejecutando `ping -c 5 10.0.8.10`.
b) Analice los encabezados *Ethernet*, *IP* e *ICMP Echo Request y Reply*.
c) La primera línea en la salida del ping muestra la cantidad de *data bytes*. ¿A qué se refiere esa cantidad?
d) Analice la información provista en cada prueba y el resumen final.

Información útil:

- `Display filter` útil de Wireshark "`not ripng and not rip`".
- Para más información de la aplicación ping ejecutar "`man ping`" en una terminal de comandos.

4. Pruebas de *traceroute*

IMUNES. Experimento: `imunes-examples/Traceroute/traceroute.imn`

a) Inicie el Wireshark para capturar el tráfico en `pc1`, luego utilice la aplicación `traceroute` para verificar la ruta desde `pc1` (10.0.0.21) hacia `server` (10.0.8.10) ejecutando `traceroute` 10.0.8.10. Analice la respuesta y compárelo con el diagrama de red. Compare la información de la captura con la del diagrama de red.
b) Verifique la ruta en sentido contrario al anterior, es decir, desde `server` (10.0.8.10) hacia `pc1` (10.0.0.21). Compare las direcciones IPs con las de la prueba anterior.
c) Analice las capturas de tráfico en `pc1`. Las capturas de la prueba del ítem a) muestra todos los datagramas enviados y recibidos en `pc1`, mientras que en la captura de la prueba b) solo se ven algunos datagramas. ¿Por qué?

5. **Simultaneidad utilizando traceroute**

En una PC se ejecuta dos veces en simultáneo el comando `traceroute`. ¿Cómo identifica cada proceso de `traceroute` si los mensajes ICMPs que recibe corresponden a uno u otro proceso?

6. Simultaneidad utilizando ping

IMUNES. Experimento: `imunes-examples/Ping/ping.imn`

a) Si en una PC se ejecuta dos veces en simultáneo el comando `ping 10.0.8.10`, salen de la PC mensajes ICMP generados por dos procesos diferentes. ¿Cómo

identifica cada proceso de `ping` si los mensajes ICMPs que se reciben corresponden a uno u otro proceso?

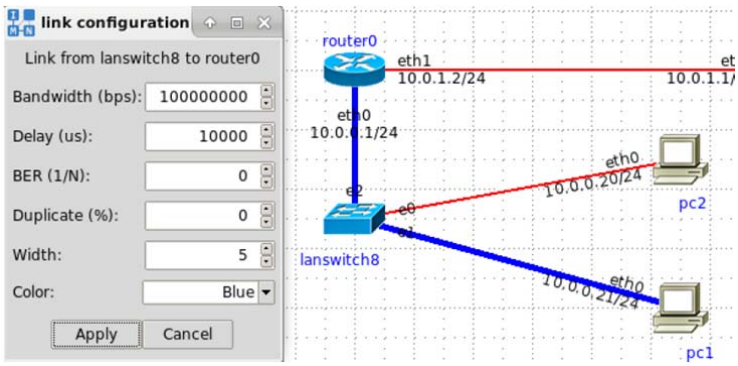
b) IMUNES: Demuestre la justificación del ítem anterior en el emulador. Corra el Wireshark en la `pc1`. Abra tres terminales, dos para ejecutar el `ping` en forma simultánea y una para ejecutar el comando `ps`.

Información útil:

- `ps` muestra información acerca de los procesos que corren en el sistema. Para más información ejecute `man ps`.

7. ARP y direccionamiento directo

IMUNES. Experimento: `imunes-examples/Ping/ping.imn`



a) Configure los links en azul como se especifica en la imagen.

b) Verifique el estado de la *tabla ARP* de `pc1` ejecutando el comando `arp -a`

c) Inicie el Wireshark en `pc1` y ejecute `ping -c 5 10.0.0.1`. Observe los tiempos de respuesta de cada prueba. ¿Por qué el tiempo de la primer prueba es mayor al resto?

d) Verifique nuevamente el estado de la *tabla ARP* de `pc1` y compárelo con la ejecución anterior.

e) Vuelva a ejecutar el comando `ping` y observe la diferencia de tiempos respecto a la ejecución anterior.

f) Compare los tiempos de respuesta de las dos ejecuciones de `ping` con los tiempos entre cada *ICMP Echo Request* y *Replay* en el Wireshark.

g) En las capturas del Wireshark, observe a qué dispositivos corresponden las direcciones MACs y las direcciones IPs del primer y segundo mensaje ICMP. Analice también el contenido de los mensajes *ARP Request* y *Reply*.

h) Borre la *tabla ARP* con el comando `arp -da`, verifique su estado y vuelva a ejecutar el comando `ping -c 5 10.0.0.1` observando específicamente el tiempo de la primer prueba.

Información útil:

- Se puede cambiar el *Time Display Format* de Wireshark con los siguientes shortcuts:
  - Ctrl+Alt+4: *Seconds Since Beginning of Capture*
  - Ctrl+Alt+6: *Seconds Since Previous Displayed Packet*
- Para más información de la aplicación `arp` ejecute `man arp`.

8. ARP y direccionamiento indirecto

a) Antes de comenzar borre la *tabla ARP*. Luego, en `pc1` inicie el Wireshark y ejecute `ping -c 5 10.0.8.10`.
b) Observe la *tabla ARP* de `pc1`. ¿Por qué la nueva entrada en la *tabla ARP* no corresponde a la de `server`? ¿A qué dispositivo corresponde y por qué?
c) En las capturas del Wireshark, observe a qué dispositivos corresponden a las direcciones MACs e IPs del primer y segundo mensaje ICMP. Analice también el contenido de los mensajes ARP Request y Reply.
d) Observe los tiempos de respuesta de cada prueba. ¿Por qué el tiempo de la primera prueba es mayor al resto?

Información útil:

- El comando `netstat -rn4` muestra la *tabla de ruteo IPv4*.

9. IPv6 autoconfiguración *stateless*

IMUNES. Experimento: `imunes-examples/ipv6.imn`

a) Ingrese al Quagga de R1 y habilite la autoconfiguración *stateless* ejecutando los siguientes comandos:

```
conf t

int eth1

ipv6 nd prefix 2001:1318:100c:1::/64

ipv6 nd ra-interval 10

no ipv6 nd suppress-ra
```

Inicie el Wireshark en la interfaz eth1 de R1.

La interfaz `eth0` de `pc1` se encuentra intencionalmente desactivada, actívela ejecutando:

```
ifconfig eth0 up
```

Confirme que la interfaz de `pc1` tiene las direcciones IPv6 local y global ejecutando:

```
ifconfig eth0
```

b) Estudie el procedimiento de autoconfiguración analizando las capturas de tráfico.
c) En pc1 ejecute `ping6 -c 5 fc00:2::10` y analice la respuesta y las capturas.
d) En pc1 ejecute `traceroute6 fc00:2::10` y analice la respuesta y las capturas.

10. IPv6-over-IPv4

IMUNES. Experimento: tunel.imn

a) Inicie el experimento y configure el túnel aplicando las siguientes configuraciones en la terminal de *bash* de los routers:

router2:

```
ip tunnel add 6bone mode sit remote 10.0.4.2 local 10.0.2.1 ttl 64
ip link set 6bone up
ip address add 3ffe:29a1:ff:fe::2 peer 3ffe:29a1:ff:fe::1 dev 6bone
ip -6 route add fc00:9::/64 via 3ffe:29a1:ff:fe::1
```

router4:

```
ip tunnel add 6bone mode sit remote 10.0.2.1 local 10.0.4.2 ttl 64
ip link set 6bone up
ip address add 3ffe:29a1:ff:fe::1 peer 3ffe:29a1:ff:fe::2 dev 6bone
ip -6 route add fc00:7::/64 via 3ffe:29a1:ff:fe::2
```

b) Corra el Wireshark en el router2 interfaz eth1. Luego verifique la comunicación entre la PC y el servicio ejecutando el siguiente comando en host5: `ping -c 10 fc00:9::1`
Analice las capturas.