



Práctica 1

Introducción al Networking y NetSim



Generado: 03/01/2025 11:04:17

1.1. Objetivos

Conocer el funcionamiento básico de la herramienta de simulación NetSim y su aplicación en el análisis de redes y protocolos de comunicaciones.

Duración: 1 sesiones

1.2. Introducción a NetSim

1.2.1. Entorno de simulación y flujo de trabajo

NetSim es una herramienta de simulación de red que le permite crear escenarios de red, modelar el tráfico, diseñar protocolos y analizar el rendimiento de la red. Los usuarios pueden estudiar el comportamiento de una red mediante combinaciones de prueba de parámetros de red. Las diversas tecnologías de red cubiertas en NetSim incluye:

- Internetworks - Ethernet, WLAN, IP, TCP
- Legacy Networks - Aloha, Slotted Aloha
- Cellular Networks - GSM, CDMA
- Mobile Adhoc Networks - DSR, AODV, OLSR, ZRP
- Wireless Sensor Networks - 802.15.4
- Internet of Things - 6LoWPAN gateway, 802.15.4 MAC/PHY, RPL
- Cognitive Radio Networks - 802.22
- Long-Term Evolution Networks – LTE
- VANETs - IEEE 1609
- 5G NR - LTE NR
- Satellite Communication Networks - TDMA
- Software Defined Networking – Open flow protocol
- Advanced Routing and Switching - VLAN, IGMP, PIM, L3 Switch, ACL and NAT
- UWAN – Slotted Aloha

La pantalla de inicio de NetSim se muestra en la Figura 1.1 ↔ Haga clic en el tipo de red que desea desea simular.

Ventana de diseño de red: un usuario ingresaría a la ventana de diseño al seleccionar un tipo de red en la pantalla de inicio. La GUI de la ventana de diseño de NetSim (ver Figura 1.2) permite a los usuarios modelar una red compuesta por dispositivos de red como conmutadores, enrutadores, nodos, etc., conectar a través de enlaces y modelar el tráfico de aplicaciones para que fluya a través de la red. Los dispositivos que se muestran en la paleta son específicos de las tecnologías de red elegidas por el usuario.

Descripción

1. **File:** para guardar el escenario de red antes o después de ejecutar la simulación en el espacio de trabajo actual.

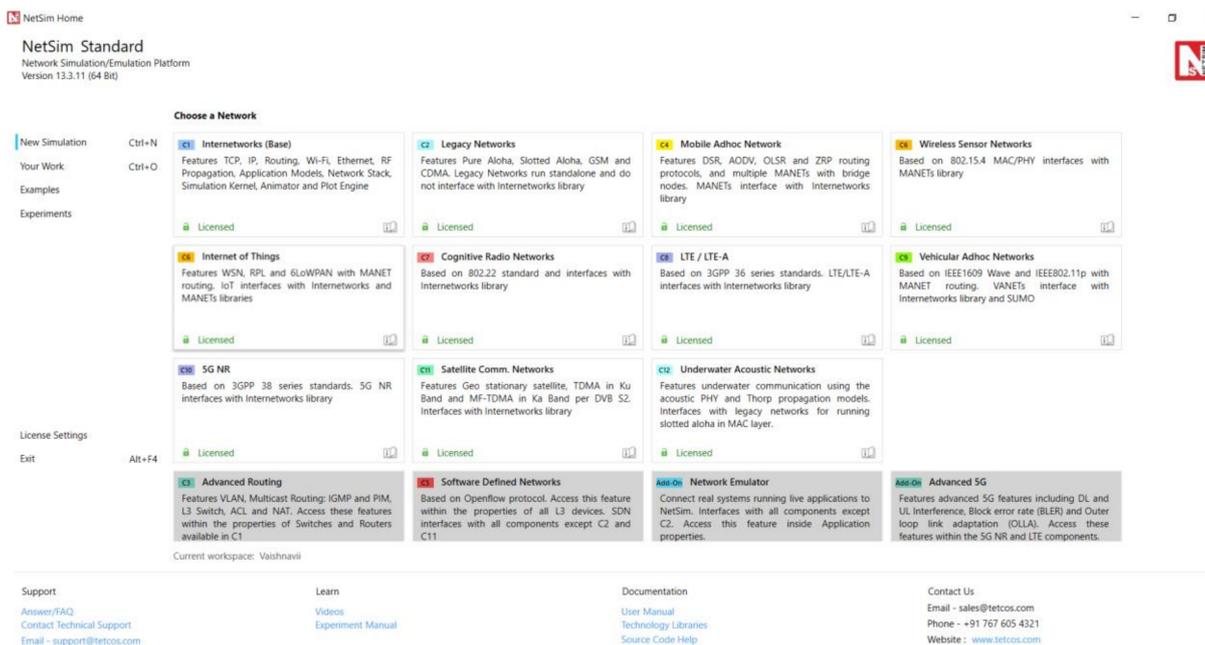


Figura 1.1: Pantalla de inicio de NetSim

- Clic **File** → **Save** para guardar la simulación dentro del espacio de trabajo actual. Los usuarios pueden especificar su propio nombre y descripción del experimento (opcional).
 - Clic **File** → **Save As** para guardar una simulación ya guardada con un nombre diferente después de realizar las modificaciones necesarias en el mismo.
 - Clic **Close** para cerrar la ventana de diseño o GUI. Lo llevará a la pantalla de inicio de NetSim.
2. Vaya a **Options** → **Grid/Map settings** y elija el tipo de entorno. Aquí hemos elegido la Cuadrícula/Mapa en forma de Cuadrícula. La opción de mapa se puede utilizar para objetivos específicos como cuando se diseñan escenarios VANET.
 3. **Help**: permite a los usuarios acceder a todas las funciones de ayuda.
 - **Tutoriales en vídeo**: ayuda a los usuarios dirigiéndolos a nuestro YouTube dedicado Canal “**TETCOS**”, donde tenemos muchas presentaciones en video que van desde cortos hasta de largo, cubriendo diferentes versiones de NetSim hasta la última versión.
 - **Respuestas/Preguntas frecuentes**: ayuda al usuario dirigiéndolo a nuestro “**Portal de soporte NetSim**”, donde se puede encontrar una “**Base de Conocimientos**” bien estructurada, compuesta por respuestas o soluciones a todas las consultas más comunes que puede tener un nuevo usuario.
 - **Generar un ticket de soporte**: ayuda al usuario dirigiéndolo a nuestro “**NetSim Support Portal**”, donde uno puede “**Presentar un ticket**” o lo que es lo mismo plantear su consulta, la cual llega a nuestro servicio de asistencia técnica dedicado y se brindará el debido soporte al usuario.
 - **Manual de usuario**: ayuda al usuario con la usabilidad de toda la herramienta y sus funciones. Facilita enormemente a un nuevo usuario con mucha información clave sobre NetSim.

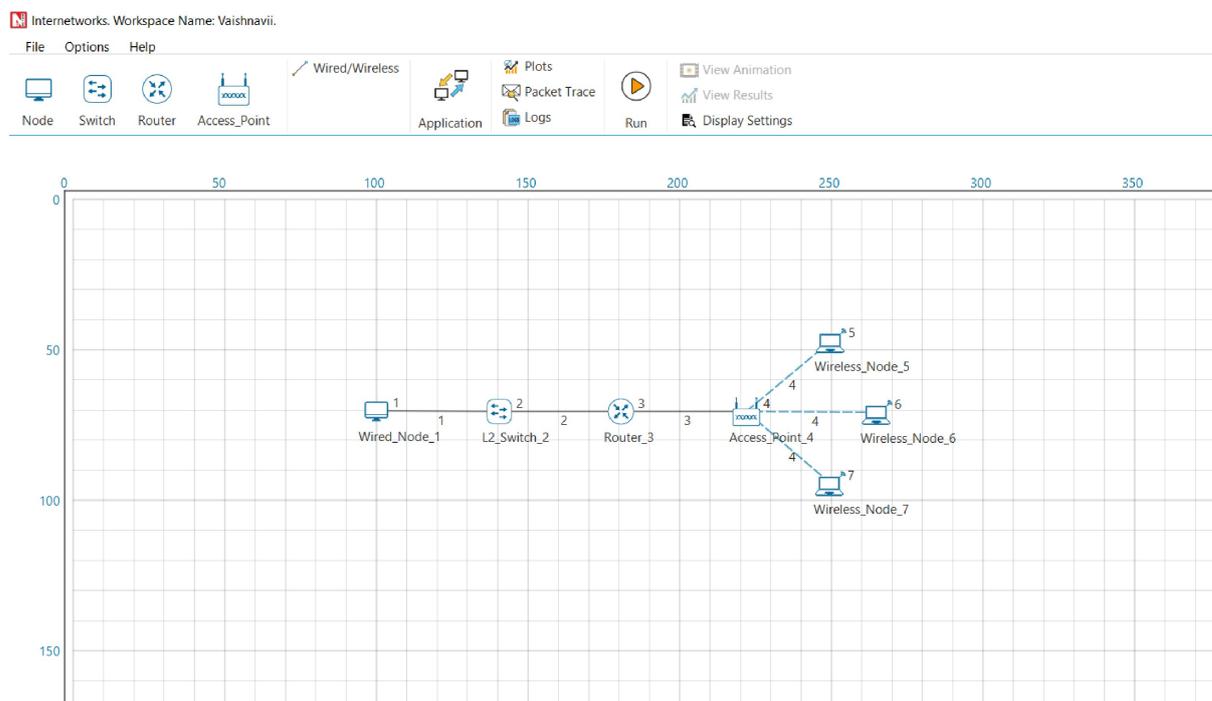


Figura 1.2: Ventana de diseño de red

- **Ayuda de código fuente:** ayuda al usuario con una documentación estructurada para “NetSim Ayuda de código fuente”, que ayuda a los usuarios que realizan su I+D utilizando NetSim con una documentación de código estructurado que consta de más de 5000 páginas con mucha facilidad de navegación de una parte del documento a otra.
- **Código fuente abierto:** ayuda al usuario a abrir todos los códigos fuente de NetSim librerías de protocolos en Visual Studio, donde se puede comenzar a iniciar el proceso de depuración o realizar modificaciones al código existente o agregar nuevas líneas de código. Visual Studio Community Edition es un IDE muy recomendado para nuestros usuarios que utilizan I+D Versión de NetSim.
- **Experimentos:** ayuda al usuario con enlaces separados proporcionados para más de 30 diferentes experimentos que cubren casi todas las tecnologías de red presentes en NetSim.
- **Bibliotecas de tecnología:** ayuda al usuario dirigiéndolo a una carpeta que consta de Archivos de biblioteca de tecnología individuales que comprenden todos los componentes presentes en NetSim.

Debajo de las opciones del menú, toda la región constituye la cinta/barra de herramientas mediante la cual se pueden realizar las siguientes acciones:

- Clic y suelte los dispositivos de red y clic derecho para editar las propiedades.
- Clic en Enlaces cableados/inalámbricos para conectar los dispositivos entre sí. Automáticamente detecta si se debe utilizar un enlace cableado/inalámbrico en función de los dispositivos que intentamos conectar.
- Clic en Aplicación para configurar diferentes tipos de aplicaciones y generar tráfico.
- Clic en Trazados, Seguimiento de paquetes y Seguimiento de eventos y haga clic en la opción de casilla

de verificación habilitar, que aparece en sus respectivas ventanas para generar métricas adicionales para mejorar analizar el rendimiento de la red.

- Clic en Ejecutar para realizar la simulación y especificar el tiempo de simulación en segundos.
- Junto a Ejecutar, tenemos las opciones Ver animación y Ver resultados. Ambas opciones permanecen oculto antes de ejecutar la simulación o si las ventanas respectivas ya están abiertas.
- La opción Configuración de pantalla se utiliza principalmente para mostrar varios parámetros como el nombre del dispositivo, IP, etc., para proporcionar una mejor comprensión, especialmente durante el diseño y la animación.

Ventana de resultados: al finalizar la simulación, estadísticas de la red o rendimiento de la red métricas reportadas en forma de gráficos y tablas. El informe incluye métricas como rendimiento, tiempo de simulación, paquetes generados, paquetes descartados, recuentos de colisiones, etc (ver la Figura 1.3 y Figura 1.4).

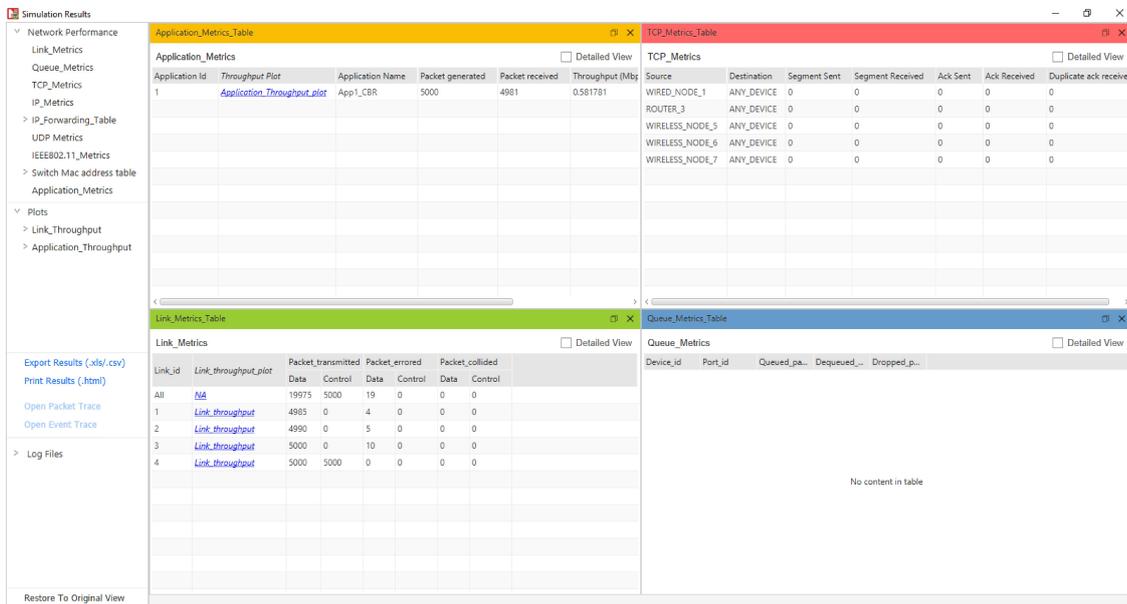


Figura 1.3: Ventana de resultados

Descripción:

1. Debajo de Resultados de la simulación, al hacer clic en una métrica en particular se mostrarán las métricas respectivas.
2. Al hacer clic en los enlaces de una métrica particular, se mostrará el gráfico en una ventana separada.
3. Al habilitar la Vista detallada haciendo clic en ella, se mostrarán las propiedades restantes.
4. Al hacer clic en Restaurar a la vista original, volverá a la vista original.
5. Haga clic en Abrir seguimiento de paquetes/Abrir seguimiento de eventos para abrir las métricas adicionales que proporcionan un análisis en profundidad de cada paquete/evento.

Ventana de animación de paquetes: cuando hacemos clic en ejecutar simulación, tenemos la opción de grabar/reproducir y grabar animación. Si esto está habilitado, los usuarios pueden ver la animación durante el tiempo de ejecución o al finalizar la simulación, consulte la Figura 1.5, los usuarios pueden ver el flujo de

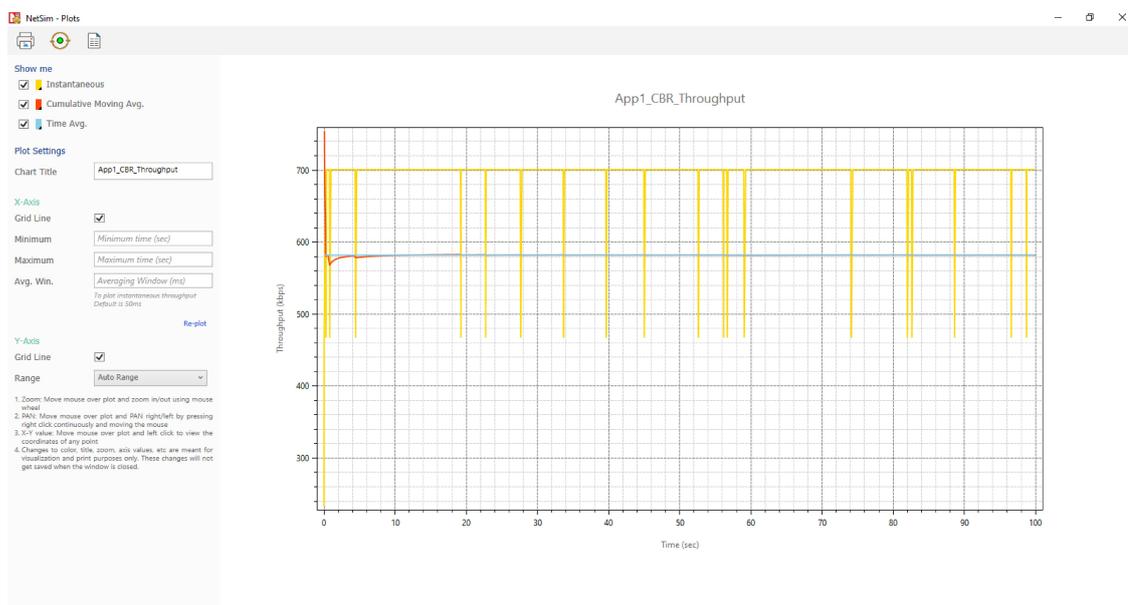


Figura 1.4: Gráfico de rendimiento de la aplicación

paquetes a través de la red. Además de esto, hay más de 25 campos de información de paquetes disponibles en forma de tabla, al final. Esta tabla contiene todos los campos registrados en el seguimiento del paquete. Además, hay opciones de animación disponibles para ver diferentes gráficos, direcciones IP y movimiento de nodos, etc.

1. Haga clic en Reproducir para ver la animación. Puedes pausar la animación en cualquier intervalo y reproducirla de nuevo.
2. Haga clic en Detener para detener la animación. Ahora haga clic en Reproducir para iniciar la animación desde el comienzo.
3. Además de eso, también tenemos controladores de velocidad para aumentar/disminuir el tiempo de simulación y Velocidad de animación.
4. La opción Ver más permite al usuario ver gráficos, rendimientos y tablas de IP durante la animación.
5. Los filtros de tabla se utilizan para filtrar la información del paquete que se muestra en la siguiente tabla durante la simulación según los requisitos del usuario.
6. Al configurar más de una aplicación, se diferencia mediante indicaciones de diferentes colores.
7. Los paquetes se indican mediante diferentes combinaciones de colores, por ejemplo, el color azul indica control paquetes, el color verde indica paquetes de datos y el color rojo indica paquetes de error.

1.2.2. ¿Cómo crea y guarda un usuario un experimento en el espacio de trabajo?

Para crear un experimento, seleccione **New Simulation** → <Cualquier red> en la pantalla de inicio de NetSim (ver Figura 1.6).

Cree una red y guarde el experimento → clic en el botón File → Save en la parte superior izquierda (ver Figura 1.7).

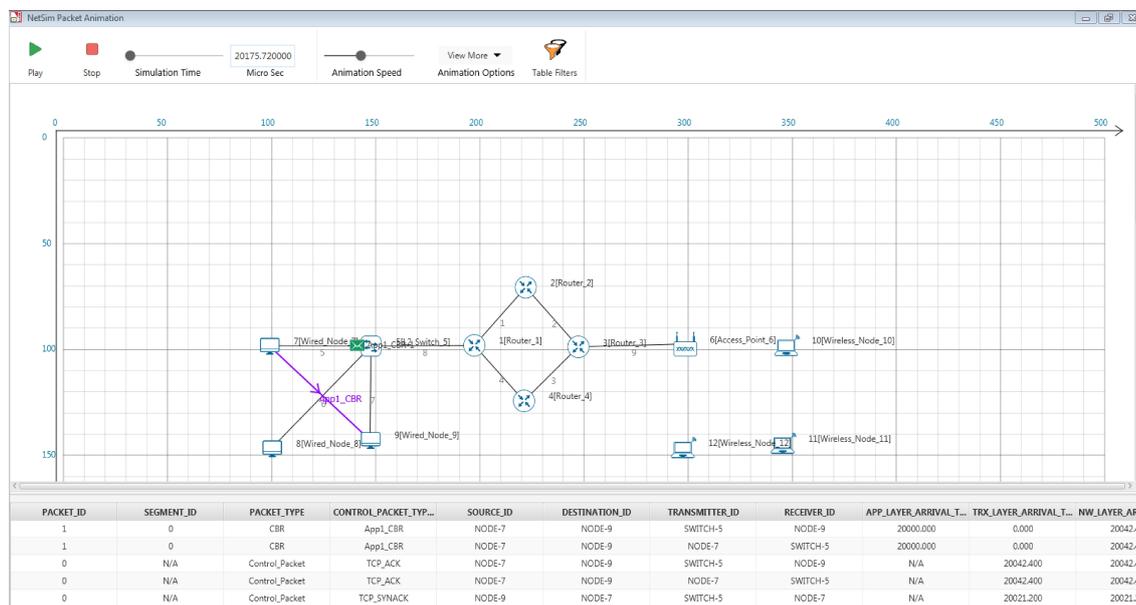


Figura 1.5: Ventana de animación de paquetes

Aparece una ventana emergente para guardar que contiene el nombre del experimento, la ruta del espacio de trabajo y Descripción (Figura 1.8).

Especifique el nombre y la descripción del experimento (opcional) y luego haga clic en Guardar. La ruta del espacio de trabajo no es editable. Por lo tanto, todos los experimentos se guardarán en la configuración predeterminada ruta del espacio de trabajo. Después de especificar el nombre del experimento, haga clic en Guardar.

En nuestro ejemplo guardamos con el nombre MANET y este experimento se puede encontrar en la ruta predeterminada del espacio de trabajo (consulte la Figura 1.9).

Los usuarios también pueden ver los experimentos guardados en el menú Su trabajo (ver Figura 1.10).

La opción "Save As" también está disponible para guardar el experimento actual con un nombre diferente.

1.2.3. Secuencia típica para realizar los experimentos en este manual

Los pasos típicos involucrados en la realización de experimentos en NetSim son:

- Network Set up: arrastre y suelte dispositivos y conéctelos mediante enlaces cableados o inalámbricos.
- Configure properties: configure las propiedades del dispositivo, protocolo o enlace haciendo clic derecho en el dispositivo o enlace y modificando parámetros en la ventana de propiedades.
- Model Traffic: Clic en el icono de la aplicación presente en la cinta y establezca los flujos de tráfico.
- Enable Trace/Plot (optional): clic en seguimiento de paquetes, seguimiento de eventos y trazados para habilitar. El seguimiento de paquetes registra el flujo de paquetes, el seguimiento de eventos registra cada evento (NetSim es un evento discreto simulador) y el botón **Plots** permite crear gráficos de varios rendimientos a lo largo del tiempo.

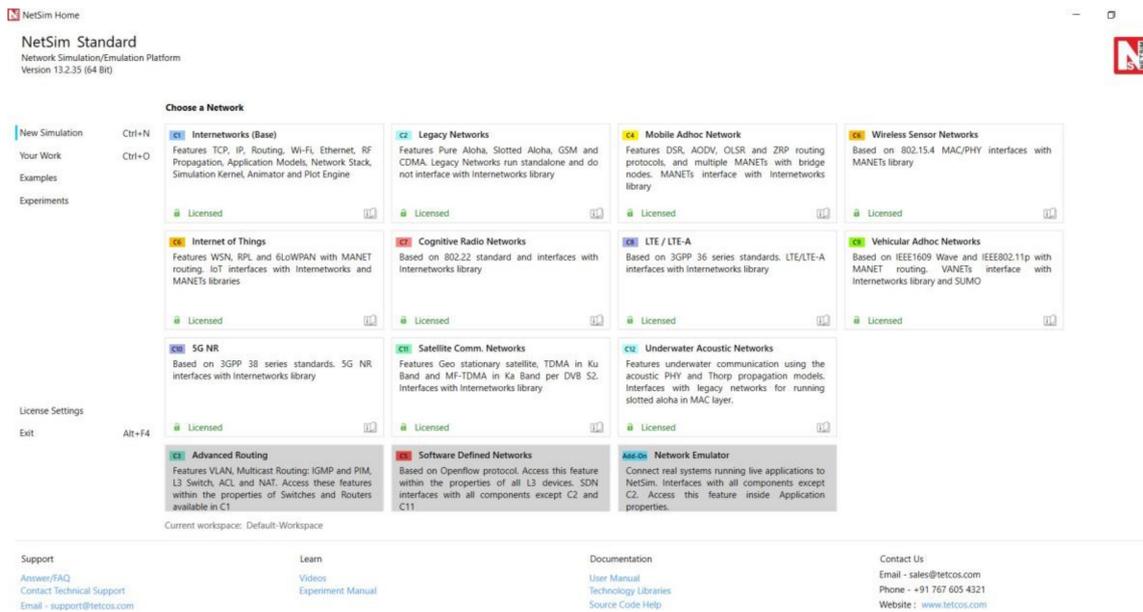


Figura 1.6: Pantalla de inicio de NetSim

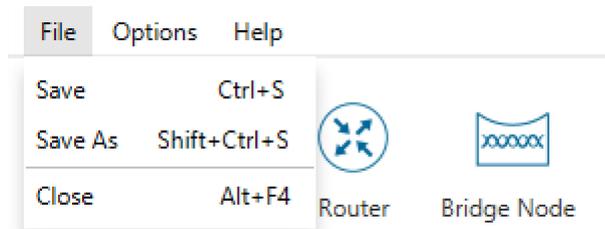


Figura 1.7: Guarde la red usando la opción de archivo

- Save/Save As/Open/Edit: clic en File → Save/File → Save As para guardar el experimentos en el espacio de trabajo actual. Los experimentos guardados se pueden abrir desde NetSim pantalla de inicio para ejecutar la simulación o modificar los parámetros y ejecutar nuevamente la simulación.
- View Animation/View Results: visualice a través del animador para comprender el trabajo, analizar resultados y sacar inferencias.

NOTA: Los archivos de configuración de ejemplo para todos los experimentos estarán disponibles donde se haya instalado NetSim. El directorio es (<NetSim_Install_Directory>Docs\Sample_Configuration\NetSim_Experiment_Manual)

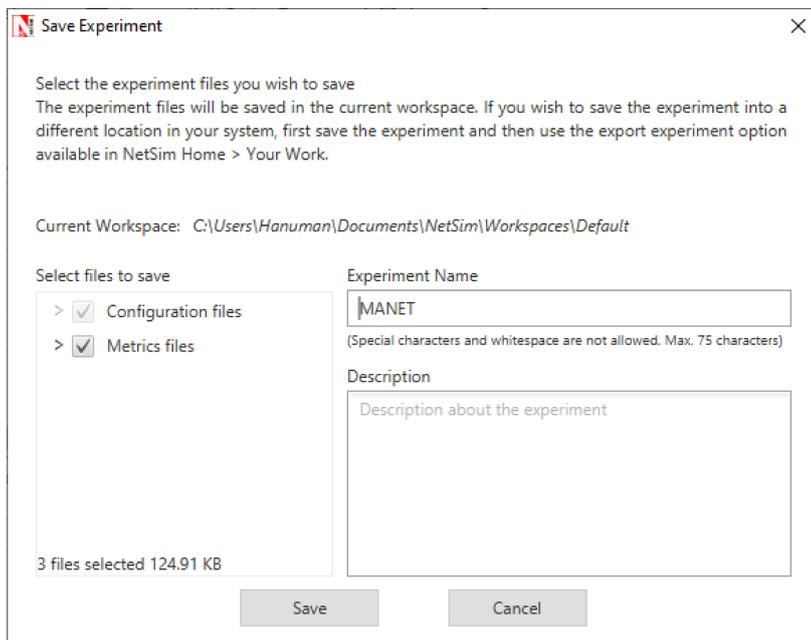


Figura 1.8: Ventana Guardar NetSim

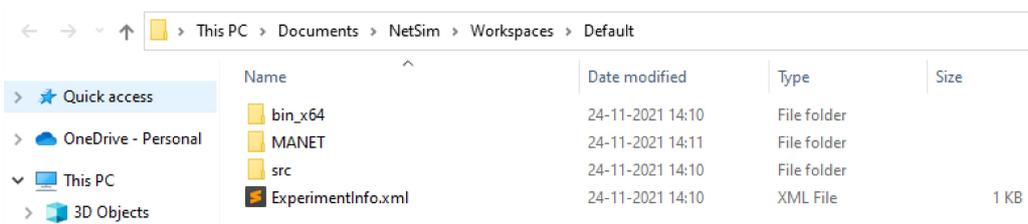


Figura 1.9: Ruta del espacio de trabajo predeterminado de NetSim

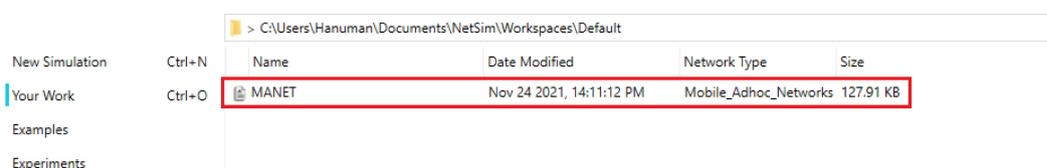


Figura 1.10: Su menú de trabajo

1.3. Informe

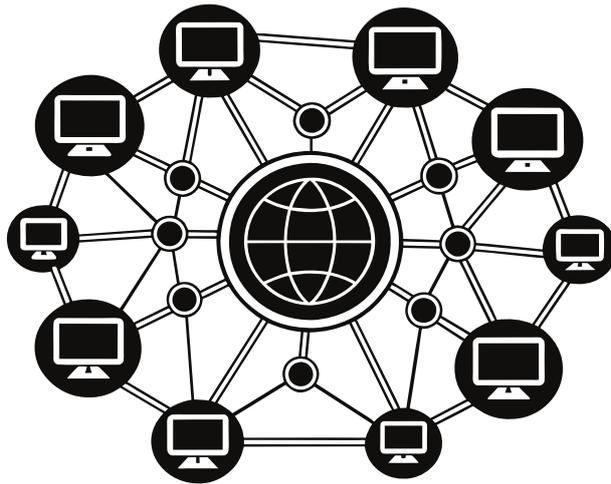
Redacta el informe con las siguientes indicaciones:

- Reproduce el experimentado mostrado en este guión.
- Realiza los comentarios, pruebas y explicaciones que consideres oportunos.
- Se valorará el contenido atendiendo a los siguientes conceptos: originalidad, organización, estética, etc.
- Además, debes indicar tu valoración personal así como los conceptos aprendidos con el desarrollo de la práctica.
- El plagio será firmemente perseguido: una vez detectado plagio, serán evaluadas a 0 tanto la copia como el original.
- Entregar las memorias en formato *pdf*.
- El fichero entregado en la tarea debe de contener vuestras siglas y número práctica. Ejemplo: **Pepito Pérez Martínez entrega la práctica 5**, entonces, el nombre de fichero debe ser: ***PPM-5.pdf***.



Práctica 2

Comandos básicos de red: Ping, agregar/eliminar/ruta, ACL



Generado: 03/01/2025 11:04:17

2.1. Objetivos

NetSim permite a los usuarios interactuar con la simulación en tiempo de ejecución a través de un socket o mediante un archivo. Las interacciones del usuario hacen que la simulación sea más realista al permitir la ejecución de comandos para ver/modificar ciertos parámetros del dispositivo durante el tiempo de ejecución.

Duración: 1 sesiones

2.2. Comandos básicos de red

2.2.1. Comando *ping*

- El comando ping es una de las utilidades de red más utilizadas para solucionar problemas.
- Puede utilizar el comando ping para probar la disponibilidad de un dispositivo de red (normalmente un computadora) en una red.
- Cuando haces ping a un dispositivo, le envías un mensaje corto a ese dispositivo, que luego envía atrás (el eco).
- Si recibe una respuesta, entonces el dispositivo está en la red. Si no la recibe, entonces el dispositivo está defectuoso, desconectado, apagado o mal configurado.

2.2.2. Comandos de ruta

Puede utilizar los comandos de ruta para ver, agregar y eliminar rutas en tablas de enrutamiento IP.

- **route print:** Para ver el contenido completo de la tabla de enrutamiento IP.
- **route delete:** Para eliminar todas las rutas en la tabla de enrutamiento IP.
- **route add:** Para agregar una ruta TCP/IP estática a la tabla de enrutamiento IP.

2.2.3. Configuración de ACL

Los enrutadores brindan capacidades básicas de filtrado de tráfico, como bloquear el tráfico de Internet con listas de control de acceso (ACL, *Access Control List*). Una ACL es una lista secuencial de declaraciones **Permit** o **Deny** que se aplican a direcciones o protocolos de capa superior. Estas listas le indican al enrutador qué tipos de paquetes debe: **PERMIT** o **DENY**. Cuando se utiliza una lista de acceso para filtrar el tráfico, se utiliza una declaración PERMIT para “permitir” el tráfico, mientras que una declaración DENY se utiliza para “bloquear” el tráfico.

2.3. Configuración de la red

Abra NetSim \mapsto **Experiments** \mapsto **Advanced Routing** \mapsto **Basic networking commands Ping Route Add/Delete/Print and ACL** \mapsto luego haga clic en el mosaico en el panel central para cargar el ejemplo como se muestra en la Figura 2.1.

NetSim UI (User Interface) muestra el archivo de configuración correspondiente a este experimento como se muestra en la Figura 2.2.

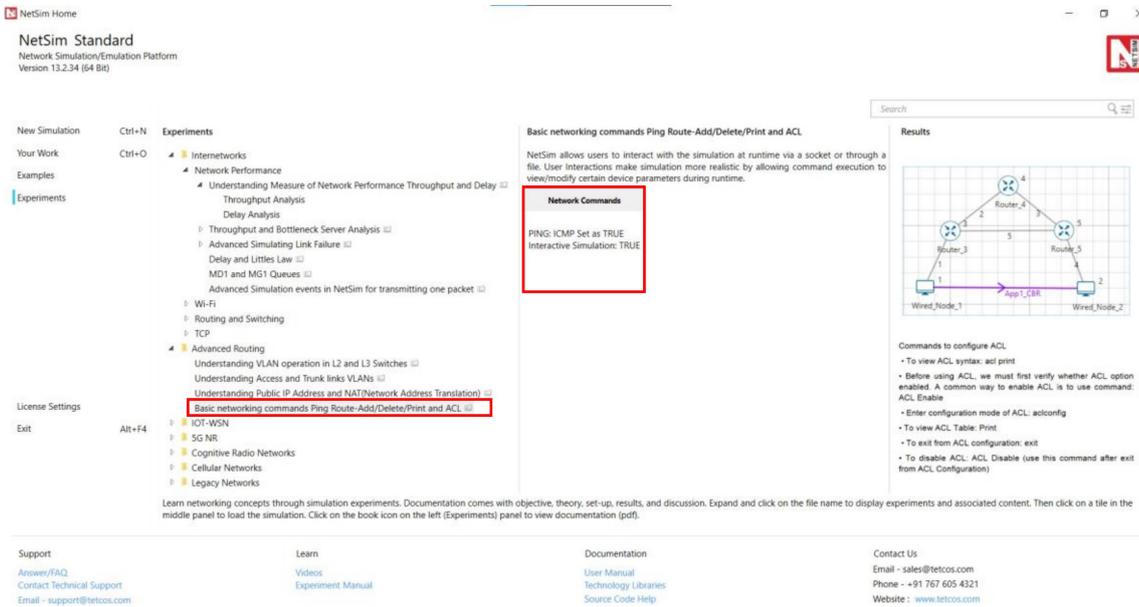


Figura 2.1: List of scenarios for the example of Basic networking commands Ping Route Add/Delete/Print and ACL

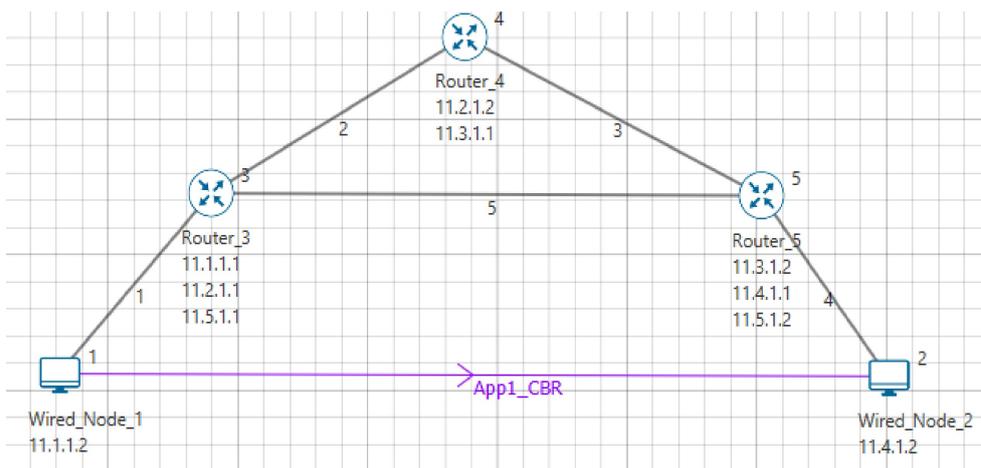


Figura 2.2: Configuración de red para estudiar los comandos básicos de red Ping Route Add/Delete/Print y ACL

2.4. Procedimiento

Se realizó el siguiente conjunto de procedimientos para generar esta muestra:

1. Se diseña un escenario de red en la GUI de NetSim que consta de 2 nodos cableados y 3 enrutadores en la biblioteca de red “Internetworks”.
2. En las propiedades de la capa de red de `Wired_Node_1`, el “**ICMP Status**” se establece como `TRUE`.

De manera similar, el estado de ICMP se establece como `TRUE` para todos los dispositivos, como se muestra en la Figura 2.3.

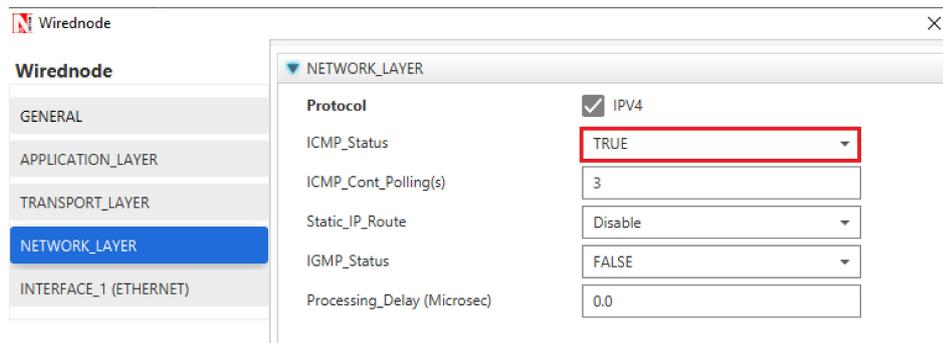


Figura 2.3: Propiedades de la capa de red de `Wired_Node_1`

3. En las propiedades generales de `Wired_Node_1`, **Wireshark Capture** está configurado como Online.
4. Haga clic derecho en Application Flow **App1 CBR** → seleccione Properties o haga clic en el Icono de aplicación presente en la cinta/barra de herramientas superior.

Se genera una aplicación CBR desde el `Wired_Node_1`, es decir, desde el origen hasta el `Wired_Node_2`, es decir, el destino, manteniendo un tamaño de paquete de 1460 bytes y un tiempo entre llegadas (*Inter Arrival Time*) de 233,6 μ s. El protocolo de transporte está configurado en UDP.

Además, el parámetro “**Start Time(s)**” se establece en 30, mientras se configura la aplicación. Este tiempo generalmente se establece mayor que el tiempo necesario para la convergencia OSPF (es decir, el intercambio de información OSPF entre todos los enrutadores) y aumenta a medida que aumenta el tamaño de la red aumenta.

5. Packet Trace está habilitado en la GUI de NetSim. Al final de la simulación, un archivo .csv muy grande que contiene toda la información del paquete está disponible para que los usuarios realicen un análisis a nivel de paquete. Los gráficos están habilitados en la GUI de NetSim.
6. Haga clic en **Run Simulation**. El tiempo de simulación está establecido en 300 segundos y en la pestaña Runtime Interaction (Figura 2.4), *Interactive Simulation* está a *True*.

NOTA: Se recomienda especificar un tiempo de simulación más largo para garantizar que haya tiempo suficiente para que el usuario ejecute los distintos comandos y vea el efecto de eso antes de que finalice la simulación.

Haga clic en **Accept** → luego haga clic en **OK**.

- La simulación (NetSimCore.exe) comenzará a ejecutarse y mostrará un mensaje “**waiting for first client to connect**” (ver Figura 2.5).

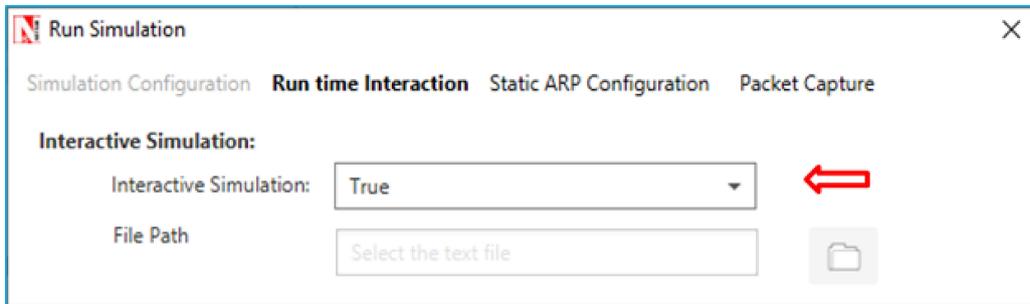


Figura 2.4: Ventana Interacción en tiempo de ejecución

```

C:\Program Files\NetSim Pro\bin\NetSimCore.exe
License Manager Output. Product>Edition>Maj_ver>Min_ver>Lic_type>Components>
netsim>pro>11>0>r1m_hw>000000000>000>

NetSim License Manager Start. Checking for licenses available (this may take upto 2 min) -

License Manager Output. Product>Edition>Maj_ver>Min_ver>Lic_type>Components>
netsim>pro>11>0>r1m_hw>111111111>110>
NetSim license validated
Installing heart-beat...
Heartbeat status = 0 (0 indicates successful)
NetworkStack loaded from path- C:\Program Files\NetSim Pro\bin\NetworkStack.dll

***
NetSim start
Network Stack loaded
Initializing simulation
Config file reading complete
License re-validation complete
Protocol binaries loaded
Stack variables initialized
Could Not Find C:\Users\TETCOS-1\AppData\Local\Temp\NetSim\Plot_*
Metrics variables initialized
Protocol variables initialized
Executing command --- DEL "C:\Users\TETCOS-1\AppData\Local\Temp\NetSim\*.pcap"
Could Not Find C:\Users\TETCOS-1\AppData\Local\Temp\NetSim\*.pcap
Emulation is disabled
CLI mode is enable...
Waiting for first client to connect. Press ctrl+c to stop connection.

```

Figura 2.5: Esperando a que se conecte el primer cliente

- Volver al escenario de red → clic en “**Display Settings**” en la cinta/barra de herramientas superior y seleccione la casilla de verificación “**Device IP**” para mostrar la dirección IP de todos los dispositivos → clic derecho en el enrutador 3 o cualquier otro enrutador y seleccione la opción “**NetSim Console**” (ver Figura 2.6).
- Ahora el Cliente (NetSimCLI.exe) comenzará a ejecutarse e intentará establecer una conexión con NetSimCore.exe. Una vez establecida la conexión, se mostrará la Figura 2.7.
- Después de ésto, la interfaz de línea de comando se puede utilizar para ejecutar todos los comandos admitidos.

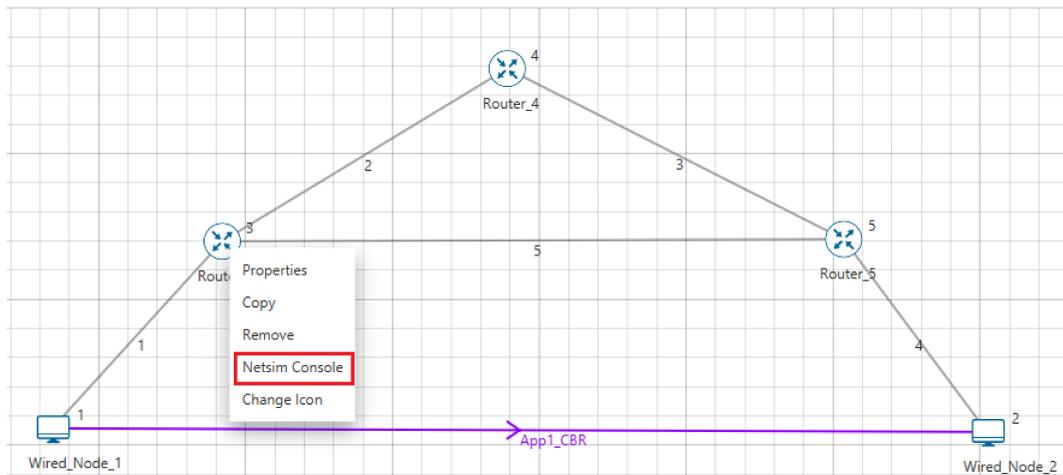


Figura 2.6: Seleccione la consola NetSim

```
C:\Program Files\NetSim Pro\bin\NetSimCLI.exe
Initialising Winsock...Initialised.
Connecting to device DESKTOP-LC53CTS.
Connection attempt: 1
Connection established.

NetSim>
```

Figura 2.7: Conexión establecida

2.5. Comandos de red

2.5.1. Comando ping

- Puede utilizar el comando ping con una dirección IP o nombre de dispositivo (ver Figura 2.8).
- ICMP_Status debe establecerse como True en todos los nodos para que funcione el ping.

```
Ping <IP address> e.g. ping 11.4.1.2 \\
Ping <Node Name> e.g. ping Wired_Node_2
```

- Para ver el contenido completo de la tabla de enrutamiento IP, utiliza el siguiente comando **route print** (ver Figura 2.9).

```
route print
```

- Verá las entradas de la tabla de enrutamiento con destinos de red y las puertas de enlace a las que los paquetes se reenvían cuando se dirigen a ese destino. A menos que ya lo hayan sido agregadas rutas estáticas a la tabla, todo lo que ve aquí se genera dinámicamente.

- Para eliminar una ruta en la tabla de enrutamiento IP, escribirá un comando usando la siguiente sintaxis

```
route delete destination_network
```

```

C:\Program Files\NetSim\Standard_v13_2\bin\NetSimCLI.exe
Initialising Winsock...Initialised.
Connecting to device PC-105.
Connection attempt: 1
Connection established.

NetSim>ping Wired_Node_2
Reply from 11.4.1.2: bytes 32 time=67us TTL=255

NetSim>ping 11.4.1.2
Reply from 11.4.1.2: bytes 32 time=209us TTL=255
Reply from 11.4.1.2: bytes 32 time=251us TTL=255
Reply from 11.4.1.2: bytes 32 time=292us TTL=255
Reply from 11.4.1.2: bytes 32 time=334us TTL=255

NetSim>_

```

Figura 2.8: Haciendo ping a Wired_Node_2

- Entonces, para eliminar la ruta con la red de destino 11.5.1.2, todo lo que tendríamos que hacer es escribir esta instrucción

```
route delete 11.5.1.2
```

- Para verificar si la ruta se ha eliminado o no, verifique nuevamente mediante el comando **route print**.
- Para agregar una ruta estática a la tabla, escribirá un comando usando la siguiente sintaxis.

```
route ADD destination_network MASK subred_mask gateway_ip metric_cost interface
```

- Entonces, por ejemplo, si desea agregar una ruta que especifique que todo el tráfico con destino la subred 11.5.1.2 fuera a la puerta de enlace en 11.5.1.1

```
route ADD 11.5.1.2 MASK 255.255.0.0 11.5.1.1 METRIC 100 IF 2
```

- Si usara el comando de impresión de ruta para mirar la tabla ahora, vería su nueva ruta estática (ver Figura 2.10).

NOTA: La entrada agregada en la tabla de IP mediante el protocolo de enrutamiento se actualiza continuamente. Si un usuario intenta eliminar una ruta a través del comando de eliminación de ruta, siempre existe la posibilidad de que el protocolo de enrutamiento vuelva a ingresar esta entrada nuevamente. Los usuarios pueden utilizar ACL/static route para anular la entrada del protocolo de enrutamiento si es necesario.

2.5.2. Configuración de ACL

Comandos para configurar ACL

- Para ver la sintaxis de ACL: **acl print**
- Antes de usar ACL, primero debemos verificar si la opción ACL está habilitada. Una forma común de habilitar ACL es usar el comando: **ACL Enable**
- Ingrese al modo de configuración de ACL: **aclconfig**

```

C:\Program Files\NetSim Standard\bin\NetSimCLI.exe
Initialising Winsock...Initialised.
Connecting to device DESKTOP-LPF533Q.
Connection attempt: 1
Connection established.

NetSim>route print
=====
IP Route Table
=====
      Network Destination  Netmask/Prefix          Gateway                Interface      Metric      Type
-----
      11.2.1.2             255.255.0.0            11.2.1.2              11.2.1.1       200        OSPF
      11.3.1.1             255.255.0.0            11.2.1.2              11.2.1.1       200        OSPF
      11.3.1.2             255.255.0.0            11.5.1.2              11.5.1.1       200        OSPF
      11.5.1.2             255.255.0.0            11.5.1.2              11.5.1.1       200        OSPF
      11.5.0.0             255.255.0.0            on-link               11.5.1.1       300        LOCAL
      11.2.0.0             255.255.0.0            on-link               11.2.1.1       300        LOCAL
      11.1.0.0             255.255.0.0            on-link               11.1.1.1       300        LOCAL
      224.0.0.1            255.255.255.255       on-link               11.1.1.1       306        MULTICAST
      224.0.0.0            240.0.0.0             on-link               11.1.1.1       306        MULTICAST
      255.255.255.255     255.255.255.255       on-link               11.1.1.1       999        BROADCAST
=====

```

Figura 2.9: Tabla de enrutamiento IP

- Para ver la tabla ACL: **print**
- Para salir de la configuración de ACL: **exit**
- Para deshabilitar ACL: **ACL Disable** (use este comando después de **exit** de **ACL Configuration**)
- Para ver la sintaxis de uso de ACL, use: **ACL print**

```
[PERMIT,DENY][INBOUND,OUTBOUND,BOTH] PROTO SRC DEST SPORT DPORT IFID
```

2.5.3. Pasos para configurar ACL

- Para crear una nueva regla en la ACL, utilice el comando para bloquear los paquetes UDP en la interface 2 e interface 3 de Router 3.
- En Application properties → Transport Protocol → UDP (ver Figura 2.11).
- Utilice el comando como se muestra en la Figura 2.12.

```

NetSim> acl enable
ACL is enable

NetSim>aclconfig

ROUTER_3/ACLCONFIG>acl print
Usage: [PERMIT,DENY] [INBOUND,OUTBOUND,BOTH] PROTO SRC DEST SPORT DPORT IFID

ROUTER_3/ACLCONFIG>DENY BOTH BOTH UDP ANY ANY 0 0 2
OK!
ROUTER_3/ACLCONFIG>DENY BOTH BOTH UDP ANY ANY 0 0 3
OK!
ROUTER_3/ACLCONFIG>print
DENY BOTH UDP ANY/0 ANY/0 0 0 2
DENY BOTH UDP ANY/0 ANY/0 0 0 3

ROUTER_3/ACLCONFIG>exit

NetSim>acl disable
ACL is disable

NetSim>

```

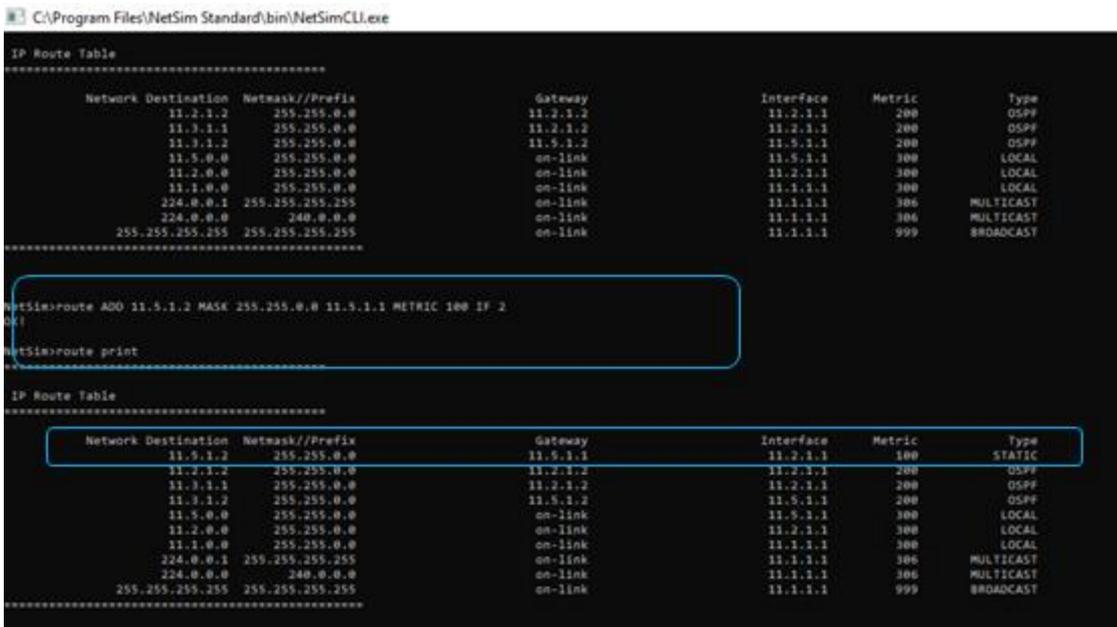


Figura 2.10: Route delete/Route add

2.5.4. Resultados del comando ping

Vaya al Panel de resultados → “Open Packet Trace” en el panel izquierdo y haga lo siguiente: establezca Filter Control Packet Type/App Name a **ICMP EchoRequest** e **ICMP EchoReply**, como se muestra Figura 2.13.

En Wireshark, aplique el filtro como ICMP. Podemos ver la petición y respuesta del ping en Wireshark (ver Figura 2.14).

2.5.5. Resultados de la ACL

El impacto de la regla ACL aplicada sobre el tráfico de simulación se puede observar en la tabla de métricas IP en la ventana de resultados de la simulación. En Router 3, la cantidad de paquetes bloqueados por el firewall se muestra en la Figura 2.15.

NOTA: el número de paquetes puede variar en el tiempo y según la ACL configurada.

Los usuarios también lo pueden observar en Packet Animation antes y después de que los paquetes hayan sido bloqueados, como se muestra Figura 2.16.

- Verifique la ventana de animación de paquetes si los paquetes se han bloqueado en Router_3 o no después de ingresar el comando ACL para denegar el tráfico UDP.
- Antes de aplicar la regla ACL hay un flujo de paquetes desde Wired_Node_1 a Wired_Node_2.
- Después de aplicar la regla ACL, el paquete fluye hasta el router_3 únicamente.

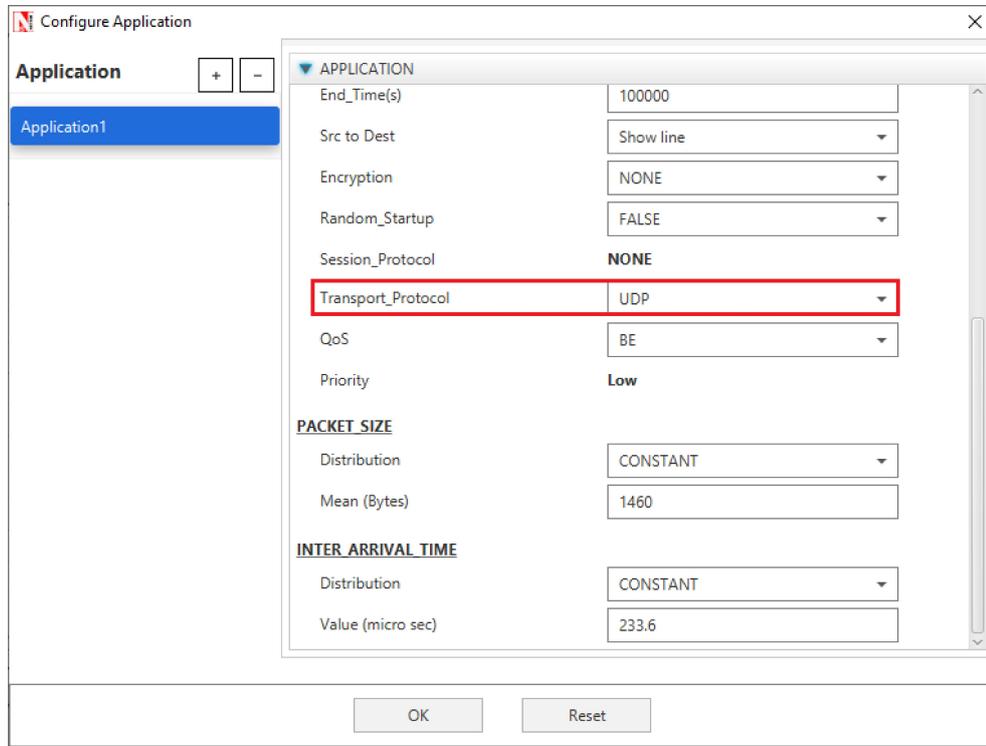


Figura 2.11: Ventana de propiedades de la aplicación

```
NetSim>acl enable
ACL is enable

NetSim>aclconfig

ROUTER_3/ACLCONFIG>acl print
Usage: [PERMIT,DENY] [INBOUND,OUTBOUND,BOTH] PROTO SRC DEST SPORT DPORT IFID

ROUTER_3/ACLCONFIG>DENY BOTH UDP ANY ANY 0 0 2
OK!
ROUTER_3/ACLCONFIG>DENY BOTH UDP ANY ANY 0 0 3
OK!
ROUTER_3/ACLCONFIG>print
DENY BOTH UDP ANY/0 ANY/0 0 0 2
DENY BOTH UDP ANY/0 ANY/0 0 0 3

ROUTER_3/ACLCONFIG>exit

NetSim>acl disable
ACL is disable

NetSim>
```

Figura 2.12: Comandos de configuración de ACL

PACKET ID	SEGMENT ID	PACKET TYPE	CONTROL_PACKET_TYPE/APP_NAME	SOURCE_ID	DESTINATION_ID	TRANSMITTER_ID	RECEIVER_ID
915	0 N/A	Control_Packet	ICMP_EchoRequest	NODE-1	ROUTER-3	NODE-1	ROUTER-3
916	0 N/A	Control_Packet	ICMP_EchoRequest	NODE-2	ROUTER-5	NODE-2	ROUTER-5
917	0 N/A	Control_Packet	ICMP_EchoReply	ROUTER-3	NODE-1	ROUTER-3	NODE-1
918	0 N/A	Control_Packet	ICMP_EchoReply	ROUTER-5	NODE-2	ROUTER-5	NODE-2
1822	0 N/A	Control_Packet	ICMP_EchoRequest	NODE-1	ROUTER-3	NODE-1	ROUTER-3
1823	0 N/A	Control_Packet	ICMP_EchoRequest	NODE-2	ROUTER-5	NODE-2	ROUTER-5
1824	0 N/A	Control_Packet	ICMP_EchoReply	ROUTER-3	NODE-1	ROUTER-3	NODE-1
1825	0 N/A	Control_Packet	ICMP_EchoReply	ROUTER-5	NODE-2	ROUTER-5	NODE-2
2726	0 N/A	Control_Packet	ICMP_EchoRequest	NODE-1	ROUTER-3	NODE-1	ROUTER-3
2727	0 N/A	Control_Packet	ICMP_EchoRequest	NODE-2	ROUTER-5	NODE-2	ROUTER-5
2728	0 N/A	Control_Packet	ICMP_EchoReply	ROUTER-3	NODE-1	ROUTER-3	NODE-1

Figura 2.13: Packet Trace - ICMP Control Packets

No.	Time	Source	Destination	Protocol	Length	Info
2	3.000000	11.1.1.2	11.1.1.1	ICMP	28	Echo (ping) request id=0x0000, seq=0/0, t...
3	3.000018	11.1.1.1	11.1.1.2	ICMP	28	Echo (ping) reply id=0x0000, seq=0/0, t...
4	6.000000	11.1.1.2	11.1.1.1	ICMP	28	Echo (ping) request id=0x0000, seq=0/0, t...
5	6.000018	11.1.1.1	11.1.1.2	ICMP	28	Echo (ping) reply id=0x0000, seq=0/0, t...
6	9.000000	11.1.1.2	11.1.1.1	ICMP	28	Echo (ping) request id=0x0000, seq=0/0, t...
7	9.000018	11.1.1.1	11.1.1.2	ICMP	28	Echo (ping) reply id=0x0000, seq=0/0, t...
8	12.000000	11.1.1.2	11.1.1.1	ICMP	28	Echo (ping) request id=0x0000, seq=0/0, t...
9	12.000018	11.1.1.1	11.1.1.2	ICMP	28	Echo (ping) reply id=0x0000, seq=0/0, t...
10	15.000000	11.1.1.2	11.1.1.1	ICMP	28	Echo (ping) request id=0x0000, seq=0/0, t...
11	15.000018	11.1.1.1	11.1.1.2	ICMP	28	Echo (ping) reply id=0x0000, seq=0/0, t...
12	18.000000	11.1.1.2	11.1.1.1	ICMP	28	Echo (ping) request id=0x0000, seq=0/0, t...
13	18.000018	11.1.1.1	11.1.1.2	ICMP	28	Echo (ping) reply id=0x0000, seq=0/0, t...
14	21.000000	11.1.1.2	11.1.1.1	ICMP	28	Echo (ping) request id=0x0000, seq=0/0, t...
15	21.000018	11.1.1.1	11.1.1.2	ICMP	28	Echo (ping) reply id=0x0000, seq=0/0, t...
16	24.000000	11.1.1.2	11.1.1.1	ICMP	28	Echo (ping) request id=0x0000, seq=0/0, t...
17	24.000018	11.1.1.1	11.1.1.2	ICMP	28	Echo (ping) reply id=0x0000, seq=0/0, t...
18	27.000000	11.1.1.2	11.1.1.1	ICMP	28	Echo (ping) request id=0x0000, seq=0/0, t...
19	27.000018	11.1.1.1	11.1.1.2	ICMP	28	Echo (ping) reply id=0x0000, seq=0/0, t...
20	30.000000	11.1.1.2	11.1.1.1	ICMP	28	Echo (ping) request id=0x0000, seq=0/0, t...

> Frame 2: 28 bytes on wire (224 bits), 28 bytes captured (224) on interface 0
 Raw packet data
 0000 45 00 00 1c 00 00 00 00 02 01 a0 dd 0b 01 01 02 E...
 0010 0b 01 01 01 08 00 f7 ff 00 00 00 00
 > Internet Protocol Version 4, Src: 11.1.1.2, Dst: 11.1.1.1
 > Internet Control Message Protocol

Figura 2.14: Paquetes de control ICMP en Wireshark

IP_Metrics_Table						
IP_Metrics <input checked="" type="checkbox"/> Detailed View						
Device Id	Packet sent	Packet forwarded	Packet received	Packet discarded	TTL expired	Firewall blocked
1	13599	0	0	0	0	0
2	99	0	3826	0	0	0
3	4007	13484	72	0	0	9651
4	74	0	74	0	0	0
5	4002	3832	74	0	0	0

Figura 2.15: Tabla de métricas IP de la ventana de resultados

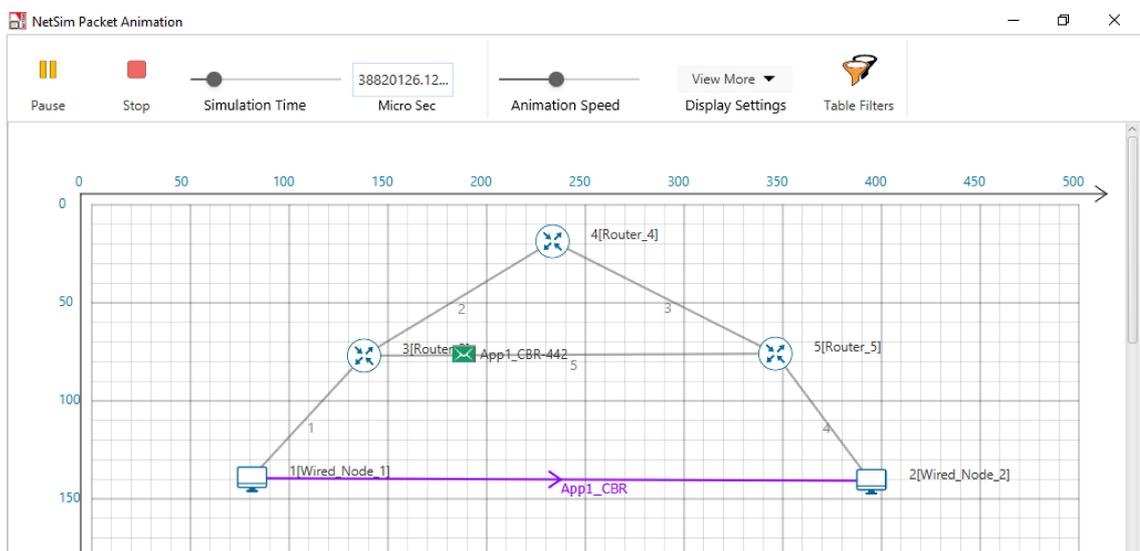


Figura 2.16: Ventana de animación, antes de aplicar las reglas de ACL

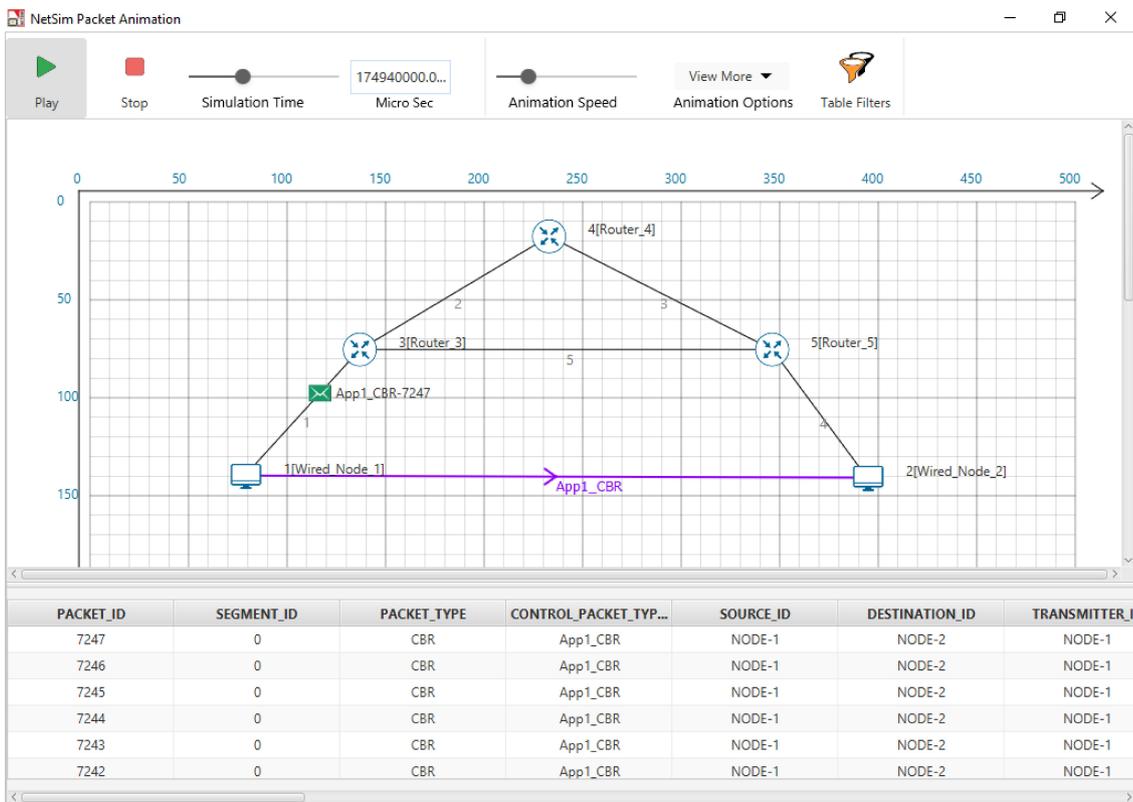


Figura 2.17: Ventana de animación, después de aplicar las reglas de ACL

2.6. Informe

Redacta el informe con las siguientes indicaciones:

- Reproduce el experimentado mostrado en este guión.
- Realiza los comentarios, pruebas y explicaciones que consideres oportunos.
- Se valorará el contenido atendiendo a los siguientes conceptos: originalidad, organización, estética, etc.
- Además, debes indicar tu valoración personal así como los conceptos aprendidos con el desarrollo de la práctica.
- El plagio será firmemente perseguido: una vez detectado plagio, serán evaluadas a 0 tanto la copia como el original.
- Entregar las memorias en formato *pdf*.
- El fichero entregado en la tarea debe de contener vuestras siglas y número práctica. Ejemplo: **Pepito Pérez Martínez entrega la práctica 5**, entonces, el nombre de fichero debe ser: ***PPM-5.pdf***.



Práctica 3

Simulador de eventos discretos de NetSim



Generado: 03/01/2025 11:04:17

3.1. Objetivos

Entender los eventos involucrados en NetSim DES (Discrete Event Simulator) en el flujo de un paquete de un nodo cableado a un nodo inalámbrico.

3.2. Introducción

Network Stack de NetSim forma el núcleo de NetSim y sus aspectos arquitectónicos se muestran esquemáticamente en la Figura 3.1. *Network Stack* acepta entradas del usuario final en forma de archivo de configuración y los datos fluyen como paquetes de una capa a otra capa en la pila de red. Todos los paquetes, cuando se transfieren entre dispositivos, se mueven hacia arriba y hacia abajo en la pila, y todos los eventos en NetSim se incluyen en una de estas diez categorías de eventos: **Physical IN**, **Data Link IN**, **Network IN**, **Transport IN**, **Application IN**, **Application Out**, **Transport OUT**, **Network OUT**, **Data Link OUT** y **Physical OUT**. Los eventos IN ocurren cuando los paquetes entran a dispositivo, mientras el OUT ocurre mientras el paquete parte hacia el dispositivo.

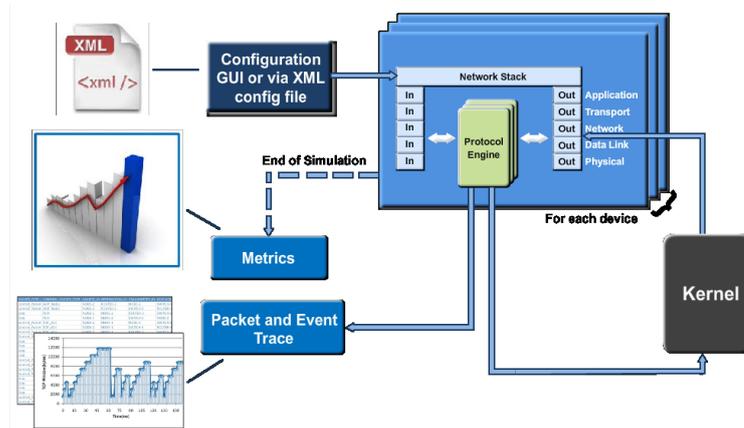


Figura 3.1: Flujo de un paquete desde un nodo cableado a otro inalámbrico

Cada dispositivo en NetSim tiene una instancia de *Network Stack*. Los conmutadores y puntos de acceso tienen una pila de 2 capas, mientras que los enrutadores tienen una pila de 3 capas. Los nodos finales tienen una pila de 5 capas.

Los motores de protocolos se llaman según la capa en la que operan los protocolos. Por ejemplo, se llama a TCP durante la ejecución de eventos Transport IN o Transport OUT, mientras que se llama a WLAN 802.11b durante la ejecución de eventos MAC IN, MAC OUT, PHY IN y PHY OUT.

Cuando estos protocolos están en funcionamiento, a su vez generan eventos para procesar por el motor de eventos discretos de NetSim. Estos se conocen como SUBEVENTOS. Todos los SUBEVENTOS caen en uno de los 10 tipos de EVENTOS anteriores.

Cada evento se agrega en el núcleo de simulación mediante el protocolo que opera en la capa particular de la *Network Stack*. Los subeventos necesarios se pasan al *Kernel*. Éstos, luego *Network Stack* recupera los subeventos para ejecutar la funcionalidad de cada protocolo. Al final de la simulación, *Network Stack* escribe archivos de traza y los archivos de métricas que ayudan al usuario a analizar las métricas de rendimiento y el análisis estadístico.

El seguimiento de eventos registra cada evento junto con información asociada, como la timestamp, ID de

evento, tipo de evento, etc. en un archivo de texto o archivo .csv que se puede almacenar en un lugar definido por el usuario.

3.3. Configuración de la red

Abre NetSim → Experiments → Internetworks → Network Performance → Advanced Simulation events in NetSim for transmitting one packet → click en el título en medio del panel para cargar el ejemplo (ver Figura 3.2).

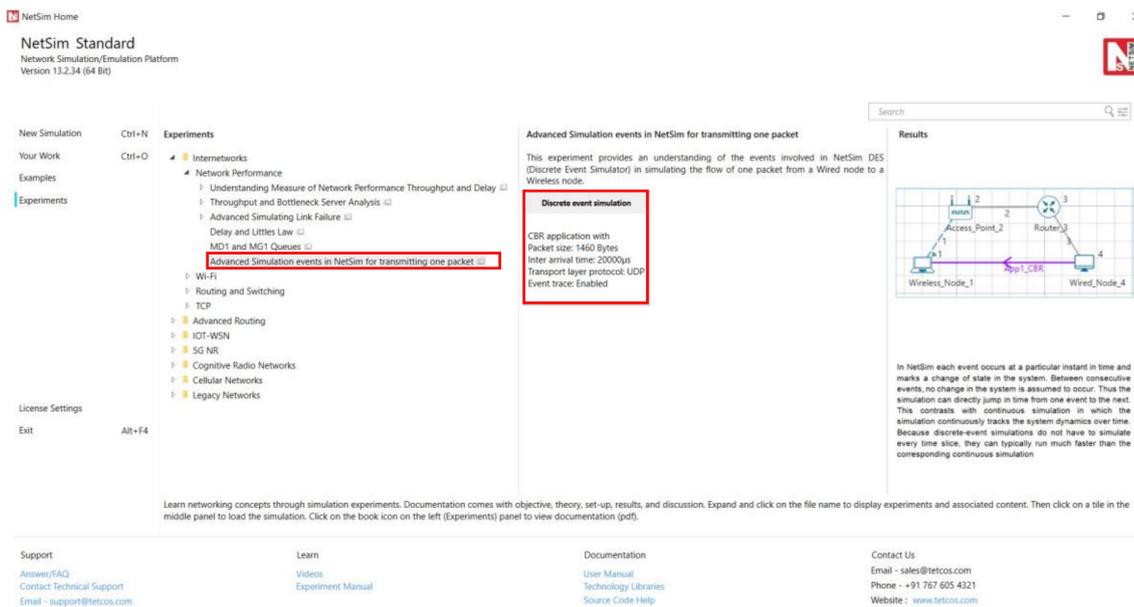


Figura 3.2: Lista de escenarios para el ejemplo de eventos de simulación avanzada en NetSim para transmitir un paquete

NetSim UI visualiza el fichero de configuración correspondiente a este experimento en la Figura 3.3.

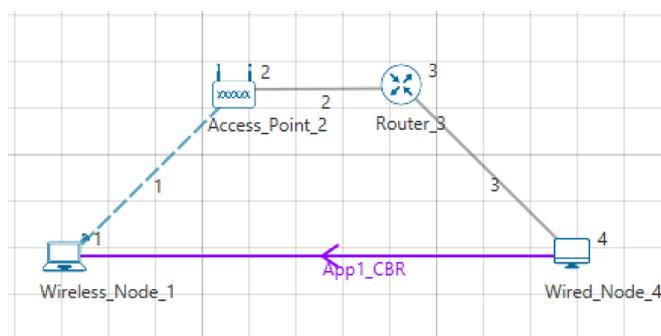


Figura 3.3: Configuración de red para estudiar los eventos de simulación avanzada en NetSim para transmitir un paquete

3.4. Procedimiento

Se realizó el siguiente conjunto de procedimientos para generar esta muestra:

1. Se diseña un escenario de red en la GUI de NetSim que consta de 1 nodo cableado, 1 nodo inalámbrico, 1 enrutador y 1 punto de acceso en la biblioteca de red "Internetworks".
2. Las posiciones del dispositivo se configuran según la tabla de la Figura 3.4

Device Positions				
	Access Point 2	Wired Node 4	Wireless Node 1	Router 3
X / Lon	150	250	100	200
Y / Lat	50	100	100	50

Figura 3.4: Posiciones de los dispositivos

3. Haga clic con el botón derecho en el ID del enlace (del enlace inalámbrico) → Properties → para acceder al enlace. Las “**Características del canal**” están configuradas en NO PATHLOSS.
4. Haga clic derecho en Application Flow **App1 CBR** → seleccione Properties o haga clic en el Icono de aplicación presente en la cinta/barra de herramientas superior.

Se genera una aplicación CBR desde `Wired_Node_4`, es decir, la fuente, a `Wireless_Node_1`, es decir, el destino, manteniendo un tamaño de paquete de 1460 bytes y un tiempo de llegada entre llegadas de 20000 μ ss.

El protocolo de transporte está configurado en UDP en lugar de TCP.

5. El seguimiento de eventos se habilita desde las opciones en la GUI de NetSim.
6. Ejecuta la simulación durante 10 segundos. Al final de la simulación, un archivo .csv muy grande contiene todos los eventos UDP IN y UDP OUT y está disponible para los usuarios. Los gráficos están habilitadas en NetSim GUI

NOTA: El seguimiento de eventos solo está disponible en las versiones NetSim Standard y Pro.

3.5. Salida

Una vez completada la simulación → Results Dashboard → en el lado izquierdo de la ventana → clic en “**Open Event Trace**”. Se abre un archivo de seguimiento de eventos como el siguiente en Excel como se muestra (Figura 3.5).

Partimos del evento `APPLICATION_OUT` del primer paquete, que ocurre en el nodo cableado y finaliza con el evento `MAC_IN` del paquete `WLAN_ACK` que llega al nodo cableado. Los eventos en la traza de eventos se registran con respecto al momento en que ocurrieron, por lo que, es posible que la identificación del evento no esté en orden (ver Figura 3.6).

3.5.1. Eventos involucrados

Los eventos se enumeran en el siguiente formato:

Event Id	Event Type	Event Time(US)	Device Type	Device Id	Interface Id	Application Id	Packet Id	Segment Id	Protocol Name	Subevent Type	Packet Size(Bytes)	Prev Event Id
1	TIMER_EVENT	0	NODE	1	0	0	0	0	IPV4	IP_INIT_TABLE	0	0
2	TIMER_EVENT	0	ROUTER	3	0	0	0	0	IPV4	IP_INIT_TABLE	0	0
3	TIMER_EVENT	0	NODE	4	0	0	0	0	IPV4	IP_INIT_TABLE	0	0
4	TIMER_EVENT	0	ACCESSPOINT	2	2	0	0	0	ETHERNET	ETH_IF_UP	0	0
5	TIMER_EVENT	0	ROUTER	3	1	0	0	0	ETHERNET	ETH_IF_UP	0	0
6	TIMER_EVENT	0	ROUTER	3	2	0	0	0	ETHERNET	ETH_IF_UP	0	0
7	TIMER_EVENT	0	NODE	4	1	0	0	0	ETHERNET	ETH_IF_UP	0	0
8	TIMER_EVENT	0	NODE	4	0	1	1	1	APPLICATION	APP_START	1460	0
9	APPLICATION	0	NODE	4	0	1	1	1	APPLICATION		0	1460
11	TRANSPORT_O	0	NODE	4	0	1	2	2	UDP		0	1460
12	NETWORK_OUT	0	NODE	4	0	1	1	1	IPV4		0	1468
13	TIMER_EVENT	0	NODE	4	1	1	1	1	IPV4	IP_PROCESSING_DELAY	1488	11
14	MAC_OUT	0	NODE	4	1	1	1	1	ETHERNET		0	1488
15	PHYSICAL_OUT	0	NODE	4	1	1	1	1	ETHERNET		0	1514
16	PHYSICAL_IN	127.08	ROUTER	3	2	1	1	1	ETHERNET		0	1514
17	MAC_IN	127.08	ROUTER	3	2	1	1	1	ETHERNET		0	1514
18	NETWORK_IN	127.08	ROUTER	3	2	1	1	1	IPV4		0	1488
19	NETWORK_OUT	127.08	ROUTER	3	2	1	1	1	IPV4		0	1468
20	TIMER_EVENT	127.08	ROUTER	3	1	1	1	1	IPV4	IP_PROCESSING_DELAY	1488	19
21	MAC_OUT	127.08	ROUTER	3	1	1	1	1	ETHERNET		0	1488
22	PHYSICAL_OUT	127.08	ROUTER	3	1	1	1	1	ETHERNET		0	1514
23	PHYSICAL_IN	253.2	ACCESSPOINT	2	2	1	1	1	ETHERNET		0	1514
24	MAC_IN	253.2	ACCESSPOINT	2	2	1	1	1	ETHERNET		0	1514
25	MAC_OUT	253.2	ACCESSPOINT	2	1	1	1	1	WLAN		0	1488
26	MAC_OUT	253.2	ACCESSPOINT	2	1	1	1	1	WLAN	CS	1488	25
27	MAC_OUT	303.2	ACCESSPOINT	2	1	1	1	1	WLAN	IEEE802_11_EVENT_DIFS_EN	1488	26
28	MAC_OUT	323.2	ACCESSPOINT	2	1	1	1	1	WLAN	IEEE802_11_EVENT_BACKOFF	1488	27
29	MAC_OUT	343.2	ACCESSPOINT	2	1	1	1	1	WLAN	IEEE802_11_EVENT_BACKOFF	1488	28
30	MAC_OUT	363.2	ACCESSPOINT	2	1	1	1	1	WLAN	IEEE802_11_EVENT_BACKOFF	1488	29

Figura 3.5: Traza de eventos

[EVENT_TYPE,	EVENT_TIME,	PROTOCOL,	EVENT_NO,	SUBEVENT_TYPE]
APP_OUT,	20000,	APP,	6,	-
TRNS_OUT,	20000,	UDP,	7,	-
NW_OUT,	20000,	IPV4,	9,	-
MAC_OUT,	20000,	ETH,	10,	-
MAC_OUT,	20000,	ETH,	11,	CS
MAC_OUT,	20000,96,	ETH,	12,	IFG
PHY_OUT,	20000,96,	ETH,	13,	-
PHY_OUT,	20122,08,	ETH,	14,	PHY_SENSE
PHY_IN,	20127,08,	ETH,	15,	-
MAC_IN,	20127,08,	ETH,	16,	-
NW_IN,	20127,08,	IPV4,	17,	-
NW_OUT,	20127,08,	IPV4,	18,	-
MAC_OUT,	20127,08,	ETH,	19,	-
MAC_OUT,	20127,08,	ETH,	20,	CS
MAC_OUT,	20128,04,	ETH,	21,	IFG
PHY_OUT,	20128,04,	ETH,	22,	-
PHY_OUT,	20249,16,	ETH,	23,	PHY_SENSE
PHY_IN,	20254,16,	ETH,	24,	-
MAC_IN,	20254,16,	ETH,	25,	-
MAC_OUT,	20254,16,	WLAN,	26,	-
MAC_OUT,	20254,16,	WLAN,	27,	DIFS_END
MAC_OUT,	20304,16,	WLAN,	28,	BACKOFF
MAC_OUT,	20324,16,	WLAN,	29,	BACKOFF
MAC_OUT,	20344,16,	WLAN,	30,	BACKOFF
MAC_OUT,	20364,16,	WLAN,	31,	BACKOFF
PHY_OUT,	20364,16,	WLAN,	32,	-
TIMER_EVENT,	21668,16,	WLAN,	35,	UPDATE_DEVICE_STATUS
PHY_IN,	21668,4,	WLAN,	33,	-
MAC_IN,	21668,4,	WLAN,	36,	RECEIVE_MPDU
NW_IN,	21668,4,	IPV4,	37,	-
MAC_OUT,	21668,4,	WLAN,	38,	SEND_ACK
TRNS_IN,	21668,4,	UDP,	39,	-
APP_IN,	21668,4,	APP,	41,	-
PHY_OUT,	21678,4,	WLAN,	40,	-
TIMER_EVENT,	21982,4,	WLAN,	43,	UPDATE_DEVICE
PHY_IN,	21982,63,	WLAN,	42,	-
MAC_IN,	21982,63,	WLAN,	44,	RECEIVE_ACK
TIMER_EVENT,	21985,	WLAN,	34,	ACK_TIMEOUT

Por ejemplo:

MAC_OUT en el punto de acceso implica subeventos como CS, IEEE802.11_EVENT_DIFS_END y IEEE802.11_EVENT_BACKOFF. Como puede ver en el archivo de seguimiento que se muestra, CS sucede en el momento del evento 20252,24. Añadiendo un tiempo DIFS de $50 \mu s$ obtiene un Subevento IEEE802.11_EVENT_DIFS en 20302,24. Además, a continuación se producen tres backoffs, dada uno de $20 \mu s$, en los instantes de evento 20322,24, 20342,24, 020362,24 respectivamente (ver Figura 3.7).

De esta manera, el seguimiento de eventos se puede utilizar para comprender el flujo de eventos en el Simulador de eventos discretos de NetSim.

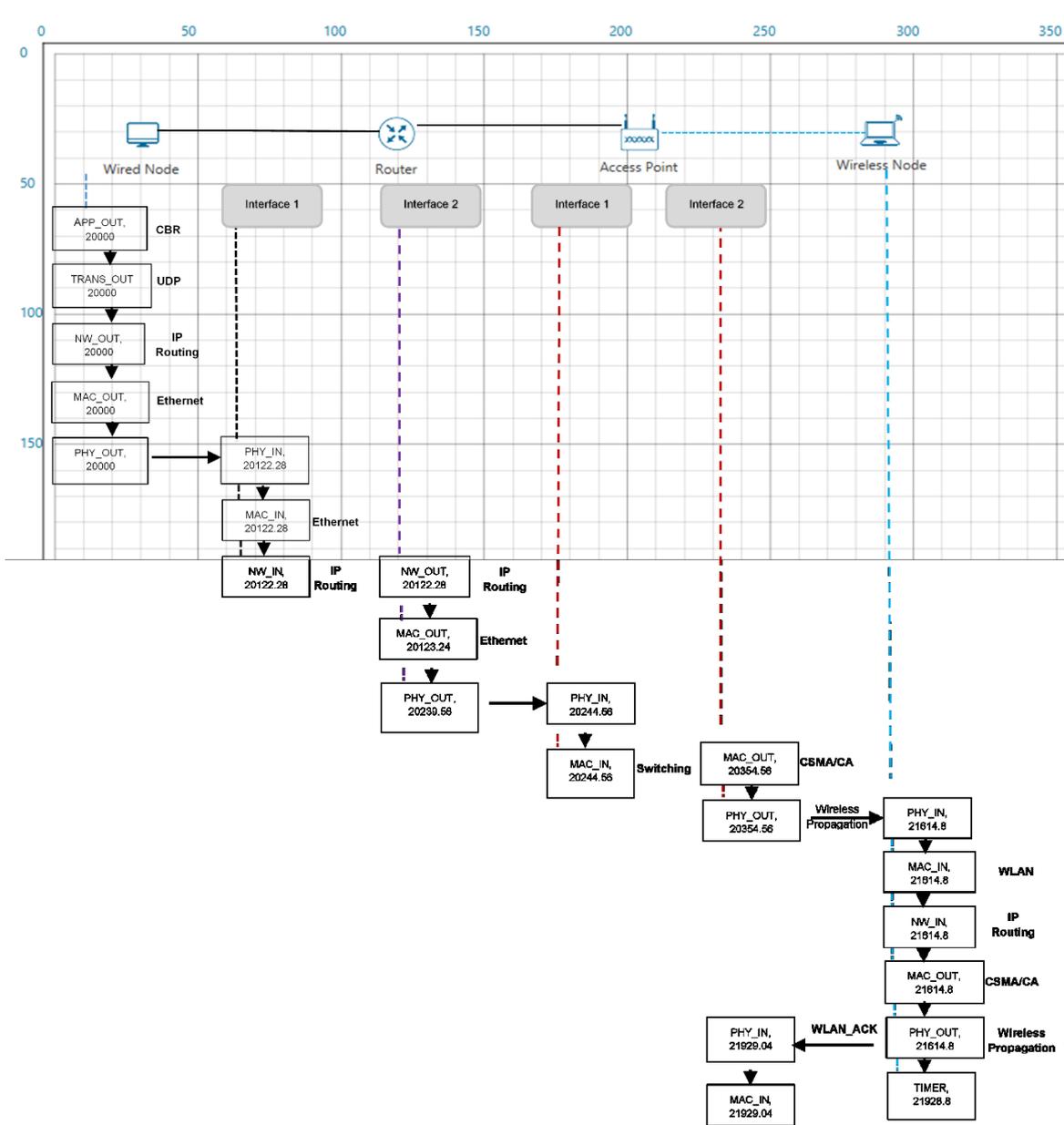


Figura 3.6: Diagrama de flujo de eventos para un paquete desde el nodo cableado al nodo inalámbrico

Event_Id	Event_Type	Event_Time(US)	Device_Type	Device_Id	Interface_Id	Applicatio	Packet_Id	Segment_Id	ProtocolName	Subevent_Type	Packet_Size	Prev_Event_Id
53	TIMER_EVENT		20126.12	ROUTER	3	1	1	2	0 IPV4	IP_PROCESSING_DELAY	1488	52
54	MAC_OUT		20126.12	ROUTER	3	1	1	2	0 ETHERNET		0	1488
55	PHYSICAL_OUT		20126.12	ROUTER	3	1	1	2	0 ETHERNET		0	1514
56	PHYSICAL_IN		20252.24	ACCESSPOINT	2	2	1	2	0 ETHERNET		0	1514
57	MAC_IN		20252.24	ACCESSPOINT	2	2	1	2	0 ETHERNET		0	1514
58	MAC_OUT		20252.24	ACCESSPOINT	2	1	1	2	0 WLAN		0	1488
59	MAC_OUT		20252.24	ACCESSPOINT	2	1	1	2	0 WLAN	CS	1488	58
60	MAC_OUT		20302.24	ACCESSPOINT	2	1	1	2	0 WLAN	IEEE802_11_EVENT_DIFS_END	1488	59
61	MAC_OUT		20322.24	ACCESSPOINT	2	1	1	2	0 WLAN	IEEE802_11_EVENT_BACKOFF	1488	60
62	MAC_OUT		20342.24	ACCESSPOINT	2	1	1	2	0 WLAN	IEEE802_11_EVENT_BACKOFF	1488	61
63	MAC_OUT		20362.24	ACCESSPOINT	2	1	1	2	0 WLAN	IEEE802_11_EVENT_BACKOFF	1488	62
64	MAC_OUT		20382.24	ACCESSPOINT	2	1	1	2	0 WLAN	IEEE802_11_EVENT_BACKOFF	1488	63
65	MAC_OUT		20402.24	ACCESSPOINT	2	1	1	2	0 WLAN	IEEE802_11_EVENT_BACKOFF	1488	64
66	MAC_OUT		20422.24	ACCESSPOINT	2	1	1	2	0 WLAN	IEEE802_11_EVENT_BACKOFF	1488	65
67	MAC_OUT		20442.24	ACCESSPOINT	2	1	1	2	0 WLAN	IEEE802_11_EVENT_BACKOFF	1488	66
68	MAC_OUT		20462.24	ACCESSPOINT	2	1	1	2	0 WLAN	IEEE802_11_EVENT_BACKOFF	1488	67
69	MAC_OUT		20482.24	ACCESSPOINT	2	1	1	2	0 WLAN	IEEE802_11_EVENT_BACKOFF	1488	68
70	MAC_OUT		20502.24	ACCESSPOINT	2	1	1	2	0 WLAN	IEEE802_11_EVENT_BACKOFF	1488	69
71	MAC_OUT		20522.24	ACCESSPOINT	2	1	1	2	0 WLAN	IEEE802_11_EVENT_BACKOFF	1488	70
72	MAC_OUT		20542.24	ACCESSPOINT	2	1	1	2	0 WLAN	IEEE802_11_EVENT_BACKOFF	1488	71
73	MAC_OUT		20562.24	ACCESSPOINT	2	1	1	2	0 WLAN	IEEE802_11_EVENT_BACKOFF	1488	72
74	MAC_OUT		20582.24	ACCESSPOINT	2	1	1	2	0 WLAN	IEEE802_11_EVENT_BACKOFF	1488	73
75	PHYSICAL_OUT		20582.24	ACCESSPOINT	2	1	1	2	0 WLAN	IEEE802_11_PHY_TXSTART_REQUEST	1528	74
76	PHYSICAL_IN		21886.25	NODE	1	1	1	2	0 WLAN		0	1528
78	MAC_IN		21886.25	NODE	1	1	1	2	0 WLAN	RECEIVE_MPDU	1528	76
79	NETWORK_IN		21886.25	NODE	1	1	1	2	0 IPV4		0	1528
80	MAC_OUT		21886.25	NODE	1	1	1	2	0 WLAN	SEND_ACK	1528	78
81	TRANSPORT_IN		21886.25	NODE	1	1	1	2	0 UDP		0	1468
83	APPLICATION_IN		21886.25	NODE	1	1	1	2	0 APPLICATION		0	1460

Figura 3.7: Subeventos CS, IEEE802.11_EVENT_DIFS_END y tiempos de eventos IEEE802.11_EVENT_BACKOFF

3.6. Discusión

En NetSim cada evento ocurre en un instante particular en el tiempo y marca un cambio de estado en el sistema. Entre eventos consecutivos se supone que no ocurre ningún cambio en el sistema. De este modo, la simulación puede saltar directamente en el tiempo de un evento al siguiente.

Esto contrasta con la simulación continua en la que la simulación sigue continuamente la dinámica del sistema a lo largo del tiempo. Debido a que las simulaciones de eventos discretos no tienen que simular todos los intervalos de tiempo, normalmente pueden ejecutarse mucho más rápido que la simulación continua correspondiente.

Comprender el seguimiento de eventos de NetSim y su flujo es muy útil, especialmente para personalizar el código existente y depurar para verificar la exactitud del código modificado. Los ID de eventos proporcionados en el seguimiento de eventos se pueden usar para ir a un evento específico durante la depuración.

3.7. Informe

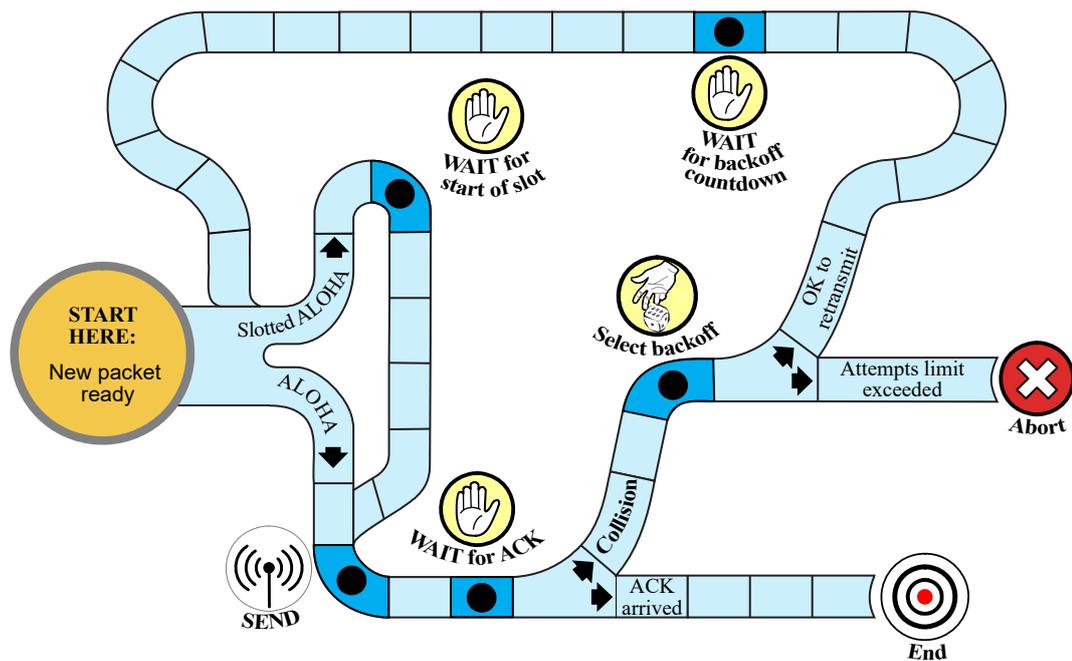
Redacta el informe con las siguientes indicaciones:

- Reproduce el experimentado mostrado en este guión.
- Realiza los comentarios, pruebas y explicaciones que consideres oportunos.
- Se valorará el contenido atendiendo a los siguientes conceptos: originalidad, organización, estética, etc.
- Además, debes indicar tu valoración personal así como los conceptos aprendidos con el desarrollo de la práctica.
- El plagio será firmemente perseguido: una vez detectado plagio, serán evaluadas a 0 tanto la copia como el original.
- Entregar las memorias en formato *pdf*.
- El fichero entregado en la tarea debe de contener vuestras siglas y número práctica. Ejemplo: **Pepito Pérez Martínez entrega la práctica 5**, entonces, el nombre de fichero debe ser: ***PPM-5.pdf***.



Práctica 4

Análisis de rendimiento en sistemas ALOHA



Generado: 03/01/2025 11:04:17

4.1. Objetivo

Comprender el procedimiento ALOHA mediante la implementación de diferentes escenarios en NetSim.

NOTA: NetSim Academic admite un máximo de 100 nodos y, por lo tanto, este experimento solo se puede realizar parcialmente con NetSim Académico. Se requeriría NetSim Standard/Pro para simular todas las configuraciones.

4.2. Teoría

ALOHA proporciona una red de datos inalámbrica. Es un protocolo de acceso múltiple (este protocolo sirve para asignar un canal de acceso múltiple). Hay dos versiones principales de ALOHA: pura y ranurada. Difieren con respecto a si el tiempo se divide en espacios discretos en los que todos los marcos deben encajar.

4.2.1. Aloha Puro

En Aloha Puro, los usuarios transmiten cada vez que tienen datos para enviar. Habrá colisiones y las tramas en colisión se retransmitirán. En la biblioteca Aloha de NetSim, el remitente espera un período de tiempo aleatorio según el algoritmo de retroceso exponencial y lo envía nuevamente. La trama se descarta cuando el número de colisiones que experimenta un paquete cruza el "Retry Limit", un parámetro configurable por el usuario en la GUI.

Sea "tiempo de trama" el tiempo necesario para transmitir la trama estándar de longitud fija. En este punto del experimento, asumimos que las tramas nuevas generadas por las estaciones viene modelado por una distribución de Poisson con una media de N tramas por tiempo de fotograma. Si $N > 1$, los nodos están generando tramas a una velocidad superior a la que el canal puede manejar y casi todas las tramas sufrirán una colisión. Para un rendimiento razonable, esperaríamos $0 < N < 1$. Además de las nuevas tramas, las estaciones también generan retransmisiones de tramas que previamente sufrieron colisiones.

La probabilidad de que no se inicie ningún otro tráfico durante todo el período vulnerable, viene dada por e^{-2G} lo que lleva a $S = G \times e^{-2G}$ donde, S es el rendimiento (*throughput*) y G es la carga ofrecida. Las unidades de S y G son tramas por tiempo de trama.

G es la media de la distribución de Poisson seguida de los intentos de transmisión por tiempo de trama, viejas y nuevas, combinadas. Por tramas antiguas se entiende aquellas que han sufrido colisiones, anteriormente.

El rendimiento máximo se produce en $G = 0,5$, con $S = \frac{1}{2e}$, que es aproximadamente 0,184. En otras palabras, lo mejor que podemos esperar es una utilización del canal del 18%. Este resultado no es muy alentador, pero como todos transmitían a voluntad, sin ningún otro tipo de restricción ni control, difícilmente podríamos haber esperado una tasa de éxito del 100%.

4.2.2. Aloha ranurado

En Aloha Ranurado, el tiempo se divide en intervalos discretos, cada intervalo corresponde a una trama. En Aloha Ranurado, se requiere que un nodo espere el comienzo del siguiente espacio para poder enviar el siguiente paquete. La probabilidad de que no se inicie ningún otro tráfico durante todo el período vulnerable, viene dado por e^{-G} , lo que lleva a $S = G \times e^{-G}$. Es fácil calcular que Aloha Ranurado alcanza su punto máximo en $G = 1$, con un rendimiento de $S = \frac{1}{e}$ ó alrededor de 0,368.

4.3. Cálculos de carga y rendimiento ofrecidos

Usando NetSim, los intentos por tiempo de paquete (G) se pueden calcular de la siguiente manera:

$$G = \frac{\text{Número de paquetes transmitidos} \times \text{Tiempo de paquete (s)}}{\text{Tiempo de simulación (s)}}$$

donde G es el tiempo de intentos por paquete. Derivamos la fórmula anterior teniendo en cuenta que (i) la métrica de salida de NetSim, el número de paquetes transmitidos, no es más que el número de intentos, y (ii) dado que los paquetes transmitidos se calculan durante todo el tiempo de simulación, el número de “tiempos de paquete” sería $\frac{\text{TiempoDeSimulacion(s)}}{\text{TiempoDeTransmisionPaquete(s)}}$, que está en el denominador. Tenga en cuenta que en NetSim los paquetes de métricas de salida transmitidos se cuentan a nivel de enlace (capa PHY). Por eso, los reintentos de la capa MAC se tienen en cuenta en esta métrica.

El rendimiento (en Mbps) por tiempo de paquete se puede obtener de la siguiente manera:

$$G = \frac{\text{Número de paquetes éxito} \times \text{Tiempo de paquete (s)}}{\text{Tiempo de simulación (s)}}$$

donde, $S = \text{Rendimiento por tiempo de paquete}$. En el caso de un paquete aloha ranurado, el tiempo (de transmisión) es igual a la longitud del slot (tiempo). El tiempo de transmisión del paquete es el tamaño del paquete de la capa PHY en bits dividido por la tasa PHY en bits/s. Considerando el tamaño del paquete de la capa PHY como 1500B y la tasa PHY de 10 Mbps, el tiempo de transmisión del paquete (o tiempo de paquete) sería $\frac{1500 \times 8}{10 \times 10^6} = 1200 \mu\text{s}$.

En el siguiente experimento, hemos tomado el tamaño del paquete como 1460 B (Data Size) más 28 B (Overheads) que equivale a 1488 B. La velocidad de datos PHY es de 10 Mbps y, por lo tanto, el tiempo del paquete es igual a 1,2ms.

4.4. Configuración de la red

Abra NetSim \mapsto Experiments \mapsto Legacy Networks \mapsto Throughput versus load for Pure and Slotted Aloha \mapsto Pure Aloha \mapsto clic en el mosaico en el panel central para cargar el ejemplo, como se muestra en la Figura 4.1.

NetSim UI muestra el archivo de configuración correspondiente al experimento como muestra en la Figura 4.2.

Aloha Puro: Entrada para muestra de 10-Nodos

1. Descargue 10 nodos (es decir, 9 nodos generan tráfico).

Los nodos 2, 3, 4, 5, 6, 7, 8, 9 y 10 generan tráfico. Las propiedades de los nodos 2, 3, 4, 5, 6, 7, 8, 9 y 10 que transmiten datos al Nodo 1 se muestran en la tabla de la Figura 4.3.

2. Propiedades del nodo inalámbrico:

NOTA: El parámetro Slot Length (s) está presente solo en Slotted Aloha \mapsto Wireless Node Properties \mapsto Interface_1 (Wireless)

3. En Adhoc Link Properties \mapsto las características del canal se establecen como **No Path Loss**.

4. Propiedades de la aplicación:

- Clic derecho en Application Flow “App1 CUSTOM” \mapsto seleccione Properties o haga clic en el icono de aplicación presente en la cinta/barra de herramientas superior. Las propiedades se establecen de acuerdo con los valores indicados en la tabla de la Figura 4.4.

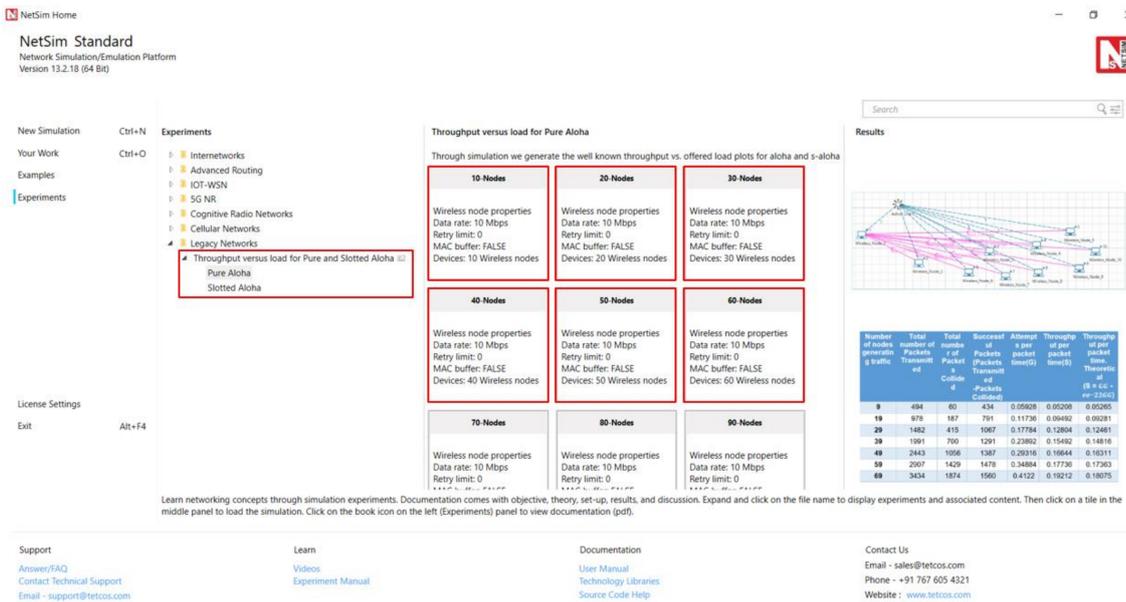


Figura 4.1: Lista de escenarios

- De manera similar, cree 8 aplicaciones más, es decir, Source_Id como 3, 4, 5, 6, 7, 8, 9, 10 y Destination_Id como 1, configure el tamaño del paquete y el tiempo entre llegadas como se muestra en la tabla anterior.

5. Los gráficos están habilitados en la GUI de NetSim.
6. Tiempo de simulación: 10 segundos

NOTA: Obtenga los valores de Número total de paquetes transmitidos y colisionados desde la ventana de resultados de NetSim.

Aloha Puro: Entrada para muestra de 20-Nodos

1. Descargue 20 nodos (es decir, 19 nodos generan tráfico).
Los nodos 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19 y 20 transmiten datos al nodo 1.

Continúe el experimento aumentando la cantidad de nodos que generan tráfico como 29, 39, 49, 59, 69, 79, 89, 99, 109, 119, 129, 139, 149, 159, 169, 179, 189 y 199 nodos.

Aloha Ranurado: Entrada para muestra de 20-Nodos

1. Descargue 20 nodos (es decir, 19 nodos generan tráfico).
Los nodos 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19 y 20 transmiten datos al nodo 1 y se establecen las propiedades de los nodos y aplicaciones como se ha mencionando anteriormente.

Continúe el experimento aumentando el número de nodos que generan tráfico como 39, 59, 79, 99, 119, 139, 159, 179, 199, 219, 239, 259, 279, 299, 319, 339, 359, 379 y 399 nodos.

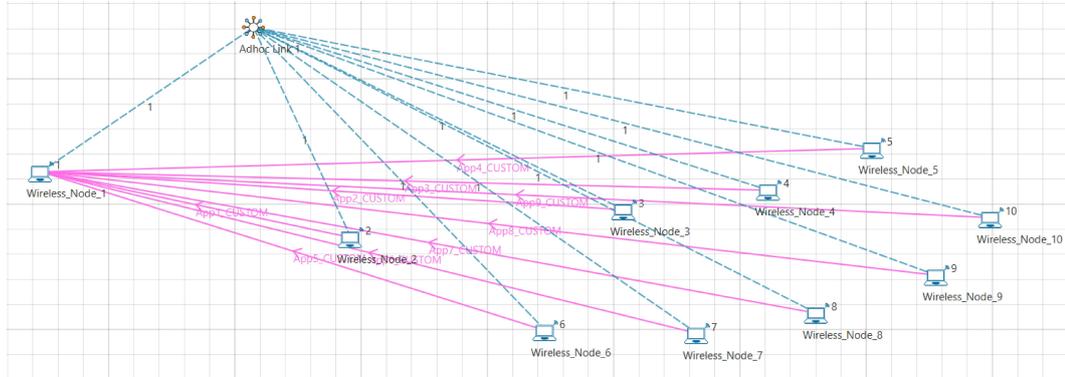


Figura 4.2: Configuración de red para el estudio de Aloha Puro

Propiedades de nodo wireless	
Interface1_Wireless (PHYSICAL_LAYER)	
Data Rate (Mbps)	10
Interface1_Wireless (DATALINK_LAYER)	
Retry_Limit	0
MAC_Buffer	FALSE
Slot Length(μs)	1200

Figura 4.3: Propiedades de nodo wireless

Propiedades Application_1		
Application Method	Unicast	
Application Type	Custom	
Source_Id	2	
Destination_Id	1	
Transport Protocol	UDP	
Packet Size	Distribution	Constant
	Value (Bytes)	1460
Inter Arrival Time	Distribution	Exponential
	Packet Inter Arrival Time (μs)	200000

Figura 4.4: Propiedades de Application_1

4.5. Salida

Tabla de comparación: los valores del número total de paquetes transmitidos y colisionados obtenidos de las estadísticas de la red después de ejecutar la simulación NetSim, se proporcionan en la tabla junto con el rendimiento por tiempo de paquete y el número de paquetes transmitidos por tiempo de paquete (ver Figura 4.5 y Figura 4.6).

Aloha Puro:

Número de nodos generando tráfico	Número de paquetes transmitidos	Número de paquetes colisionados	Éxito de paquetes (Paqts Tx - Paqts Col)	Intentos por tiempo de paquete (G)	Throughput por tiempo de paquete (S)	Throughput por tiempo de paquete teórico ($S=G*e^{-2G}$)
9	494	60	434	0.05928	0.05208	0.05265
19	978	187	791	0.11736	0.09492	0.09281
29	1482	415	1067	0.17784	0.12804	0.12461
39	1991	700	1291	0.23892	0.15492	0.14816
49	2443	1056	1387	0.29316	0.16644	0.16311
59	2907	1429	1478	0.34884	0.17736	0.17363
69	3434	1874	1560	0.4122	0.19212	0.18075
79	3964	2377	1587	0.47568	0.19044	0.18371
89	4468	2909	1559	0.53616	0.18792	0.18348
99	4998	3468	1530	0.59976	0.1836	0.18073
109	5538	4073	1465	0.66456	0.1758	0.17592
119	6023	4574	1449	0.72276	0.17388	0.1703
129	6503	5102	1401	0.78036	0.16812	0.16386
139	6992	5650	1342	0.83904	0.16104	0.15668
149	7481	6208	1273	0.89772	0.15276	0.14907
159	7998	6787	1211	0.95976	0.14532	0.14078
169	8507	7341	1166	1.02084	0.13992	0.13252
179	9008	7924	1084	1.08096	0.13008	0.12442
189	9486	8483	1003	1.13832	0.12036	0.11682
199	10025	9093	932	1.203	0.11184	0.10848

Figura 4.5: Aloha Puro

Aloha Ranurado:

Número de nodos generando tráfico	Número de paquetes transmitidos	Número de paquetes colisionados	Éxito de paquetes (Paqts Tx - Paqts Col)	Intentos por tiempo de paquete (G)	Throughput por tiempo de paquete (S)	Throughput por tiempo de paquete teórico ($S=G*e^{-G}$)
19	974	111	863	0.11688	0.10356	0.10399
39	1981	407	1574	0.23772	0.18888	0.18742
59	2893	891	2002	0.34716	0.24024	0.24534
79	3946	1504	2442	0.47352	0.29304	0.29491
99	4976	2286	2690	0.59712	0.3228	0.32865
119	5996	3144	2852	0.71952	0.34224	0.3504
139	6961	3999	2962	0.83532	0.35544	0.36231
159	7967	4974	2993	0.95652	0.35904	0.36752
179	8969	5994	2975	1.07628	0.357	0.36686
199	9983	7042	2941	1.19796	0.35292	0.36156
219	10926	8011	2915	1.31112	0.3498	0.35337
239	11928	9073	2855	1.43136	0.3426	0.34207
259	12969	10224	2745	1.55628	0.3294	0.32825
279	13916	11266	2650	1.66992	0.318	0.31438
299	14945	12430	2515	1.7934	0.3018	0.29841
319	15967	13592	2375	1.91604	0.285	0.28202
339	17011	14765	2246	2.04132	0.26952	0.26508
359	17977	15895	2082	2.15724	0.24984	0.24947
379	18983	17010	1973	2.27796	0.23676	0.23348
399	19987	18146	1841	2.39844	0.22092	0.21792

Figura 4.6: Aloha Ranurado

Así, se obtiene el siguiente gráfico característico para el ALOHA Puro (ver Figura 4.7) y el ALOHA Ranurado (ver Figura 4.8), que coincide con los resultados teóricos.

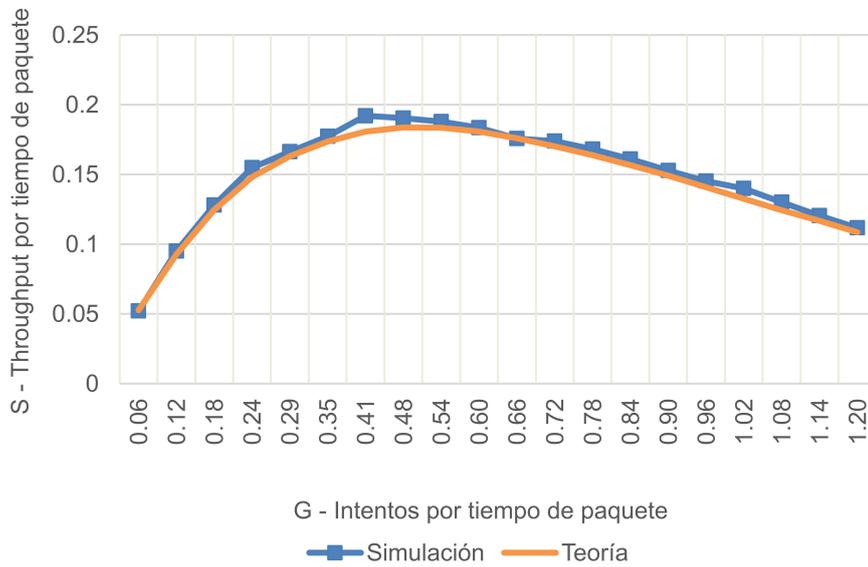


Figura 4.7: Rendimiento versus carga ofrecida para Aloha Puro

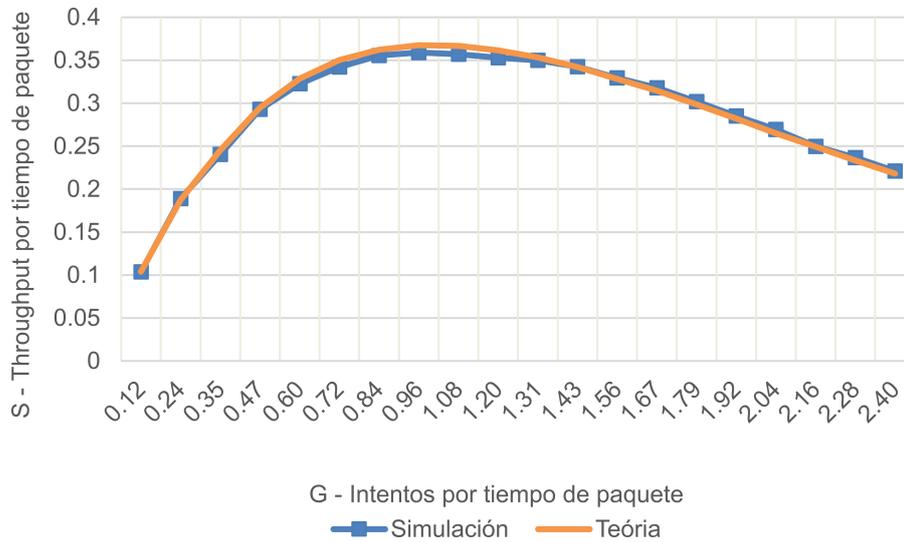


Figura 4.8: Rendimiento versus carga ofrecida para Aloha Ranurado

4.6. Informe

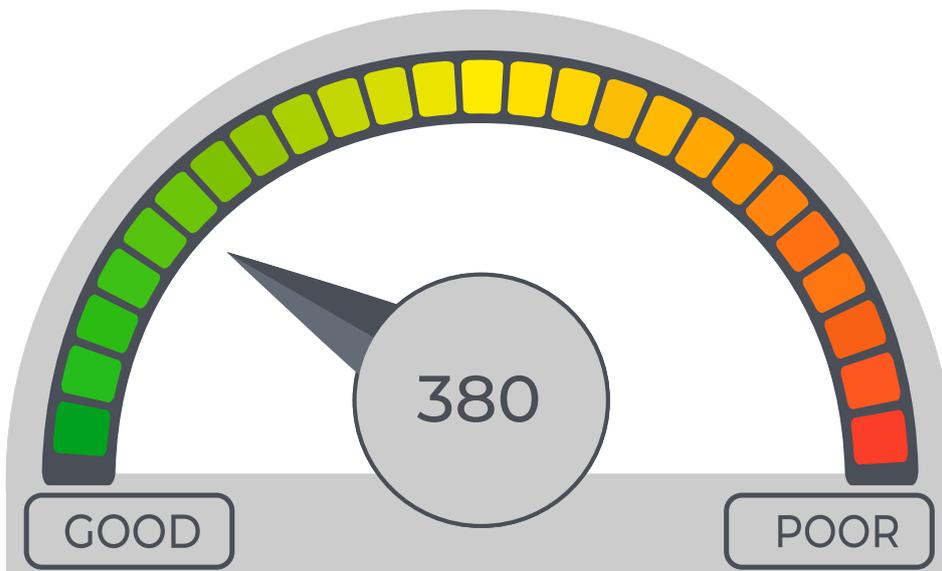
Redacta el informe con las siguientes indicaciones:

- Reproduce el experimentado mostrado en este gui3n.
- Realiza los comentarios, pruebas y explicaciones que consideres oportunos.
- Se valorar3 el contenido atendiendo a los siguientes conceptos: originalidad, organizaci3n, est3tica, etc.
- Adem3s, debes indicar tu valoraci3n personal as3 como los conceptos aprendidos con el desarrollo de la pr3ctica.
- El plagio ser3 firmemente perseguido: una vez detectado plagio, ser3n evaluadas a 0 tanto la copia como el original.
- Entregar las memorias en formato *pdf*.
- El fichero entregado en la tarea debe de contener vuestras siglas y n3mero pr3ctica. Ejemplo: **Pepito P3rez Mart3nez entrega la pr3ctica 5**, entonces, el nombre de fichero debe ser: ***PPM-5.pdf***.



Práctica 5

Medidas de rendimiento: *throughput y delay*



Generado: 03/01/2025 11:04:17

5.1. Objetivos

Experimentar las medidas de rendimiento del retardo y productividad en diferentes escenarios mediante su implementación en NetSim.

5.2. Introducción

Las dos principales medidas de rendimiento de una red son:

- **Throughput (o rendimiento):** ¿cuántos bits por segundo pasan por la red?
- **Delay (o retardo):** ¿cuánto tiempo tarda un bit de un extremo al otro?

Estos son dos conceptos ortogonales, y uno podría pensar en ellos como el ancho de una tubería y la longitud de una tubería a través de la cual fluyen datos.

5.2.1. Throughput

En términos generales, el throughput es la tasa de producción o la tasa a la que algo se produce. Cuando se utiliza en el contexto de redes de comunicación, como Ethernet o paquetes, el radio, rendimiento o rendimiento de red, es la tasa de entrega exitosa de mensajes en un canal de comunicación.

El throughput está relacionado con otras cantidades como el ancho de banda o la velocidad de datos de un enlace. Un enlace puede tener un determinado ancho de banda “nominal” o tasa de datos para enviar datos, sin embargo, es posible que no todos se utilicen todo el tiempo para enviar bits útiles. También puede tener pérdidas y retransmisiones de paquetes.

El throughput mide el número de bits útiles entregados al receptor y es diferente, pero relacionado, con las tasas de datos del enlace individual.

El throughput de una red está limitado por el enlace con el rendimiento más lento a lo largo del camino, el enlace cuello de botella. No se pueden enviar datos más rápido que la velocidad del enlace más lento. Tenga en cuenta que el enlace cuello de botella no siempre tiene que ser el enlace con la velocidad de datos nominal más lenta. A veces, un enlace de alta velocidad puede ser compartido por varios flujos, lo que hace que cada flujo reciba una pequeña parte, convirtiéndose así en un cuello de botella. En otros casos, es posible que no siempre puedas enviar a la velocidad del cuello de botella, porque el protocolo puede tener otros retrasos, como esperar ACK. Por lo tanto, si bien el rendimiento instantáneo puede ser la tasa de enlace de cuello de botella, el rendimiento promedio puede ser menor.

La forma de calcular el rendimiento promedio siempre es: ver los datos enviados durante un período y obtener la proporción. Un archivo de tamaño F tarda T unidades de tiempo en transferirse. El rendimiento promedio es F/T .

5.2.2. Delay

El retraso (Delay) de un extremo a otro en una ruta es la suma de los retrasos en todos los enlaces y nodos intermedios.

Cuando un paquete sale de un nodo, primero experimenta un retraso en la transmisión. Es decir, todos los bits de un paquete que debe publicarse en el enlace. Si un enlace puede transmitir datos a R bits/s, un paquete de tamaño B requerirá B/R segundos para publicarse.

El siguiente es el retraso de propagación. Es decir, los bits tienen que propagarse a la velocidad de las ondas en el medio de transmisión para llegar al otro extremo. Este retraso depende de la longitud del cable y

normalmente sólo es significativo para enlaces de larga distancia. Si d es la distancia que debe recorrer la onda y s es la velocidad en el medio, entonces, el retraso de propagación es d/s . La velocidad de la luz es 3×10^8 m/s en espacio libre y, por tanto, una onda de radio tarda $1 \mu\text{s}$ en recorrer una distancia de 300 metros. La velocidad de la luz en el cobre es de alrededor de 2×10^8 m/s, y tardaría unos 10 ns en viajar a largo de un cable de 2 m de longitud.

Si el retraso de propagación es menor que el retraso de transmisión, entonces el primer bit del paquete habría alcanzado el otro punto final antes de que el remitente termine de colocar todos los bits en el cable. Por eso el factor limitante es la velocidad del enlace. Por otro lado, si el retraso de propagación es mayor que el retraso en la transmisión, como es el caso de los enlaces de larga distancia, entonces el primer bit llega al otro punto final mucho después de que se haya enviado el último bit. Luego, una vez que el paquete llega al otro punto final, debe ser procesado por el conmutador o enrutador. Este retraso en el procesamiento podría implicar la búsqueda de tablas de enrutamiento, cálculos de sumas de verificación de encabezados, etc. Nuevamente, esto no suele ser un componente significativo con el hardware de alta velocidad actual.

Una vez que un punto intermedio procesa el paquete y decide a qué enlace enviarlo, el paquete puede, potencialmente, ponerse en cola hasta que el siguiente enlace quede libre. Este retraso se llama retraso en la cola. Esta es la parte más impredecible del retraso, ya que depende del tráfico enviado por otros nodos. Una gran rama de estudio llamada *Teoría de Colas*, que se dedica a modelar y comprender este retraso en diversas condiciones. El tráfico de Internet suele estar en ráfagas y, por lo tanto, se producen retrasos en las colas incluso si el tráfico agregado es menor que la capacidad de los enlaces en promedio. Es decir, supongamos que los paquetes entrantes llegan a una velocidad agregada de L bits/s y la velocidad de enlace es R bits/s, mientras $L < R$, parecería que no debería haber cola. Sin embargo, los paquetes no llegan de manera equidistante y el patrón de llegada suele ser aleatorio. En tales casos, el retraso en la cola puede ser alto incluso si $\frac{L}{R} < 1$. De hecho, el retraso en la cola aumenta, de una forma bastante pronunciada, a medida que L/R se aproxima a 1. Es aproximadamente igual a $\frac{1}{(R-L)}$. Generalmente, los diseñadores de red intentan mantener esta proporción muy por debajo de 1.

Una vez que el paquete sale de la cola y se prepara para la transmisión, el ciclo comienza nuevamente con el retraso de transmisión en el siguiente enlace. Entonces, agregamos uno de cada uno de los 4 retrasos por cada enlace atravesado. Algunos conmutadores también pueden iniciar la transmisión incluso antes de que se complete por completo la recepción. Pero la mayoría de las veces, los conmutadores actuales son de almacenamiento y reenvío. Es decir, esperan a que llegue el paquete completo y luego comienzan a reenviarlo. Una vez que una cola está llena, también puede descartar paquetes, lo que lleva a pérdidas. También pueden producirse pérdidas debido a errores de transmisión en el cable. Esto es más común en enlaces inalámbricos. Los enlaces por cable son bastante fiables.

5.3. Configuración de la simulación NetSim

Abra NetSim \mapsto clic en Experiments \mapsto Internetworks \mapsto Network Performance \mapsto Understanding Measure of Network Performance Throughput and Delay \mapsto luego clic en mosaico en el panel central para cargar el ejemplo como se muestra en la Figura 5.1.

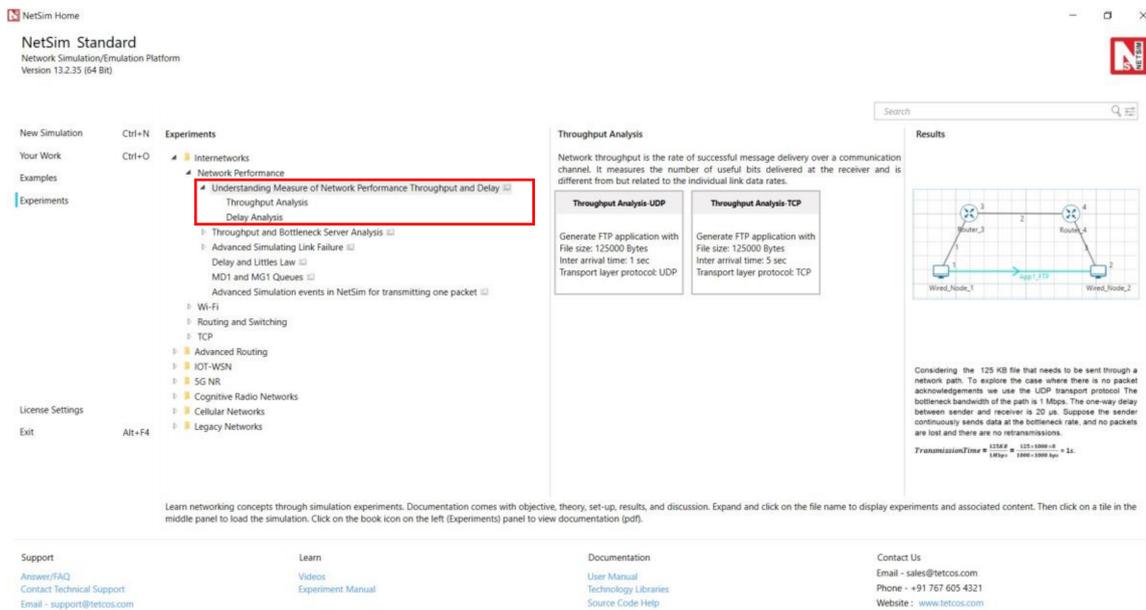


Figura 5.1: Escenarios para medidas del Rendimiento y retraso

5.4. Parte 1: Análisis de rendimiento

5.4.1. Sin acuse de recibo de paquete (UDP)

Análisis de rendimiento UDP: considere un archivo de 125 KB que debe enviarse a través de una ruta de una red. Para explorar el caso en el que no hay acuses de recibo de paquetes, utilizamos el protocolo de transporte UDP. El ancho de banda del cuello de botella de la ruta es de 1 Mbps. El retardo unidireccional entre el emisor y el receptor es de $20 \mu s$. Supongamos que el remitente envía datos continuamente a la tasa del cuello de botella, y no se pierden paquetes ni hay retransmisiones.

$$TransmissionTime = \frac{125 \text{ KB}}{1 \text{ Mbps}} = \frac{125 \times 1000 \times 8 \text{ bits}}{10^6 \text{ bps}} = 1 \text{ s}$$

Tomará 1 s enviar el archivo y el rendimiento promedio es de 1 Mbps, que es el ancho de banda del cuello de botella.

NetSim UI muestra el archivo de configuración correspondiente a este experimento como se muestra en la Figura 5.2.

Se realizó el siguiente conjunto de procedimientos para generar esta muestra.

1. Se diseña un escenario de red en la GUI de NetSim que consta de 2 enrutadores y 2 nodos cableados en la biblioteca de red "**Internetworks**".
2. Clic derecho en el enlace cableado \rightarrow Properties \rightarrow BER se establece en 0 \rightarrow retardo de propagación se establece en $20 \mu s$. Para ID de enlace 2, la velocidad del enlace se establece en 1 Mbps.
3. Clic derecho en Application Flow **App1 FTP** \rightarrow Properties o haga clic en el icono de la aplicación presente en la cinta/barra de herramientas superior.

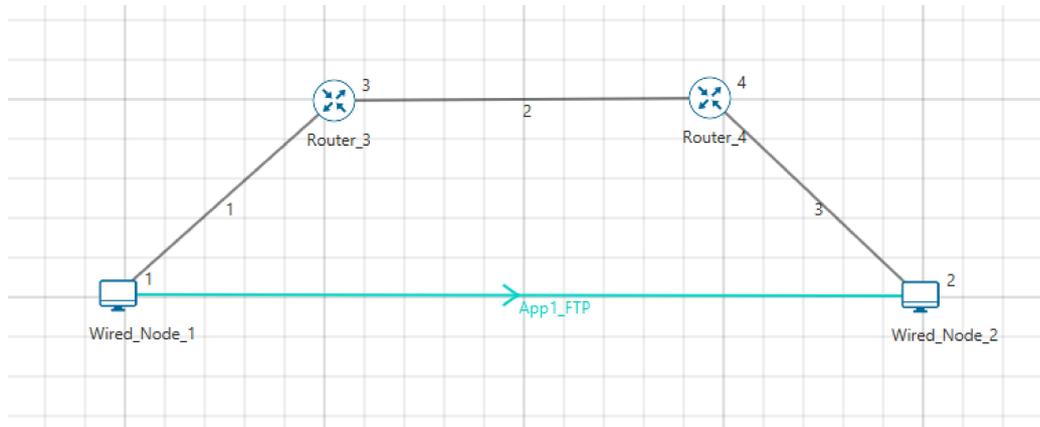


Figura 5.2: Red configurada para estudiar el análisis de rendimiento

Se genera una aplicación FTP desde `Wired_Node_1`, es decir, el origen, hasta `Wired_Node_2`, es decir, el destino, manteniendo un tamaño de archivo de 125000 bytes y un Inter Arrival Time de 1 s.

El protocolo de transporte está configurado en UDP en lugar de TCP.

- Habilite los gráficos \rightarrow Run Simulation. El tiempo de simulación se establece en 100 segundos.

5.4.2. Con acuse de recibo de paquete (TCP)

Análisis de rendimientoTCP: supongamos que el remitente necesita esperar un ACK después de enviar cada tráfico TCP de paquete de 1 KB. Supongamos que ACK también tarda 20 ms en regresar. Ahora, el remitente puede enviar 1 KB en $20 + 20 = 40$ ms. Por lo tanto, el rendimiento promedio (θ) es:

$$\theta = \frac{1 \times 8 \times 1000 \text{ bits}}{40 \text{ ms}} = 200 \text{ kbps}$$

Observe que el rendimiento promedio es una quinta parte de lo que era antes, con el nuevo requisito de ACK. Y el tiempo necesario para enviar el archivo será 5 veces mayor, es decir, 5 segundos. También puede calcular los 5 s de la siguiente manera: 1 KB tarda 40 ms, por lo que 125 KB tardan:

$$= 125 \times 40 \text{ ms} = 5 \text{ s}$$

Se realizó el siguiente conjunto de procedimientos para generar esta muestra:

- Clic derecho en el enlace cableado \rightarrow Properties \rightarrow BER se establece en 0 y Propagation Delay se establece en $40 \mu\text{s}$. Para el enlace ID 2, la velocidad del enlace se establece en 1 Mbps.
- Clic derecho en Application Flow **App1 FTP** \rightarrow Properties o haga clic en el Icono de aplicación presente en la cinta/barra de herramientas superior.

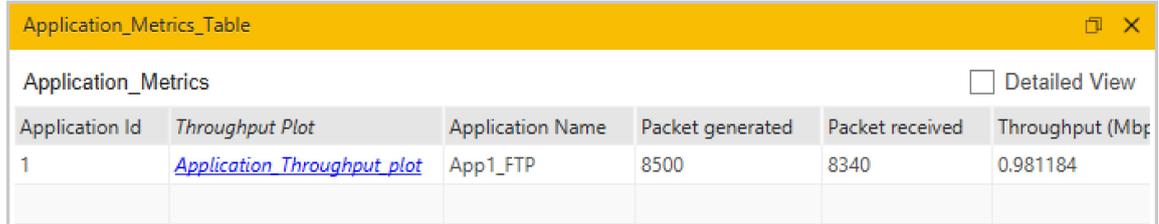
Se genera una aplicación FTP desde `Wired_Node_1`, es decir, el origen, hasta `Wired_Node_2`, es decir, el destino, manteniendo el tamaño del archivo de 125000 Bytes y el tiempo entre llegadas de 5 segundos.

El protocolo de transporte está configurado en TCP.

- Habilite los gráficos \rightarrow Run simulation. El tiempo de simulación se establece en 100 segundos.

5.4.3. Salida

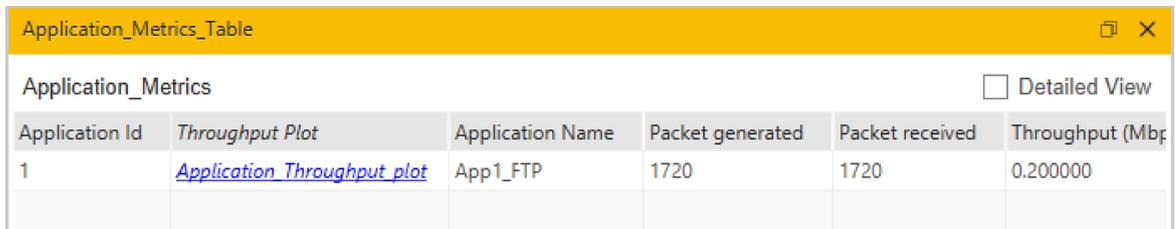
Análisis de rendimientoUDP



Application Id	Throughput Plot	Application Name	Packet generated	Packet received	Throughput (Mbps)
1	Application Throughput plot	App1_FTP	8500	8340	0.981184

Figura 5.3: Análisis de Rendimiento de Aplicación para UDP

Análisis de rendimientoTCP



Application Id	Throughput Plot	Application Name	Packet generated	Packet received	Throughput (Mbps)
1	Application Throughput plot	App1_FTP	1720	1720	0.200000

Figura 5.4: Análisis de Rendimiento de Aplicación para TCP

5.5. Parte 1: Análisis de Retardo

5.5.1. Procedimiento

Análisis de retardo UDP: Considere el siguiente problema A–S–B. Supongamos que A quiere enviar un fichero de 1 MB a B a través del dispositivo S. A dividirá el fichero de 1 MB en paquetes de 1480 bytes (el tamaño de paquete estándar para UDP).

$$\text{Number of packets} = \frac{10^6 \text{ bytes}}{1480 \text{ bytes}} = 675 \text{ paquetes de } 1480 + \text{último paquete de } 1054$$

A estos paquetes se les añade un encabezado de 54 bytes. Esto hace que el tamaño total del paquete sea 1534B ó $1534 \times 8 = 12,272$ bits. Un paquete de tamaño 12,272 bits tardaría $12,272 \mu\text{s}$ en ser transmitido a través de un enlace de 1 Mbps (megabit por segundo). A continuación, calculemos los retrasos de un extremo a otro.

Por ahora, ignoremos los retrasos en la propagación y el procesamiento, ya que son pequeños.

A envía el primer paquete de 1534 bytes en 12,27 ms y el paquete de 1054 bytes en 8,43 ms. Mientras S reenvía este paquete a B, A puede enviar el siguiente paquete a S (los conmutadores pueden enviar paquetes en un puerto mientras los reciben en otro puerto).

$$\text{Tiempo de transmisión de archivos por enlace} = 675 \times 12272 + 1 \times 1054 \times 8 = 8,29 \text{ s}$$

Por tanto, A tarda 8,29s en enviar todos los paquetes a S. Y se tarda una cantidad de tiempo similar por S para enviar el archivo a B. Por lo tanto, el tiempo total para enviar el archivo de A a B, sería:

$$T_{\text{Tiempo de transmision por enlace}} \times 2 = 8,29 \times 2 = 16,58 \mu\text{s}$$

Esto ahora se simula en NetSim. La GUI abre el archivo de configuración correspondiente a este experimento, como se muestra en la Figura 5.5.

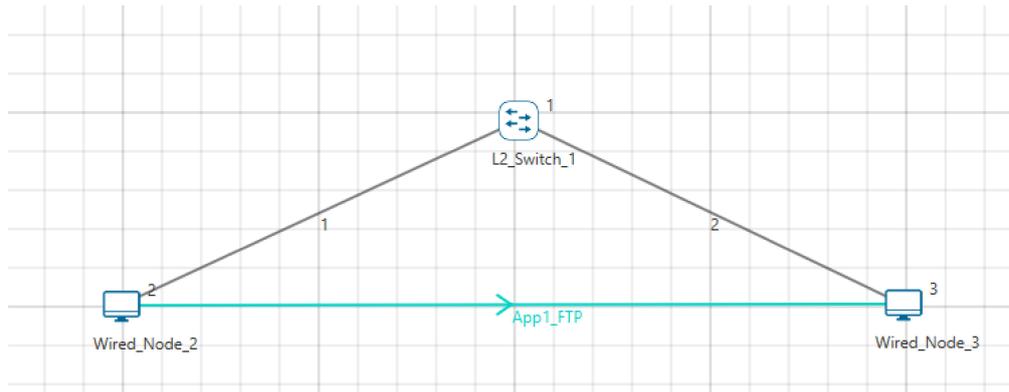


Figura 5.5: Red configurada para estudiar el análisis de retardo

Se realizó el siguiente conjunto de procedimientos para generar esta muestra:

1. Se diseña un escenario de red en la GUI de NetSim que consta de 1 conmutador L2 y 2 nodos cableados en la biblioteca de red "**Internetworks**".
2. Clic derecho en el enlace cableado \rightarrow Properties \rightarrow la velocidad del enlace se establece en 1 Mbps, BER se establece en 0 y el retardo de propagación se establece en 0 μs .
3. Click derecho en Application Flow **App1 FTP** \rightarrow Properties o haga clic en el icono de la aplicación presente en la cinta/barra de herramientas superior.

Se genera una aplicación FTP desde el Wired_Node_1, es decir, el origen, hasta Wired_Node_2, es decir, el destino, manteniendo un tamaño de archivo de 1.000.000 bytes y el tiempo entre llegadas de 100 segundos.

El protocolo de transporte está configurado en UDP en lugar de TCP.

4. Habilite el seguimiento y los trazados de paquetes \rightarrow Clic en Ejecutar simulación. El tiempo de simulación está establecido a 100 segundos.

5.5.2. Salida

Análisis de retardo UDP: en el seguimiento de paquetes podemos ver que solo se genera un archivo desde el origen hasta Destino, el archivo se divide en paquetes. Filtre el tipo de paquete como FTP para calcular.

$$\text{Retraso extremo-a-extremo} = \text{PHY_LAYER_END_TIME} - \text{PHY_LAYER_ARRIVAL_TIME}$$

Enviar un archivo de 1 MB en un enlace de 1 Mbps debería tardar 8,29s y lo mismo se ve en el seguimiento del paquete. Luego se necesitan otros 8,29s para pasar del conmutador al nodo, o 16,58s en total (consulte la Figura 5.6).

TRX_LAYER_ARRIVAL_TIME[US]	NW_LAYER_ARRIVAL_TIME[US]	MAC_LAYER_ARRIVAL_TIME[US]	PHY_LAYER_ARRIVAL_TIME[US]	PHY_LAYER_START_TIME[US]	PHY_LAYER_END_TIME[US]	End to End Delay	APP_LAYER_PA
0	0	0	0	0.96	12272.96	12273.96	12273
0	0	0	0	12273.92	24545.92	24546.92	12273
0	0	0	0	12273.96	24546.96	24546.96	12273
0	0	0	0	24546.88	36818.88	36819.88	12273
0	0	0	0	24546.92	36818.92	36819.92	12273
0	0	0	0	36819.84	49091.84	49092.84	12273
0	0	0	0	36819.88	49091.88	49092.88	12273
0	0	0	0	49092.8	61364.8	61365.8	12273
0	0	0	0	49092.84	61364.84	61365.84	12273
0	0	0	0	61365.76	73637.76	73638.76	12273
0	0	0	0	61365.8	73637.8	73638.8	12273
0	0	0	0	73638.72	85910.72	85911.72	12273
0	0	0	0	73638.76	85910.76	85911.76	12273
0	0	0	0	85911.68	98183.68	98184.68	12273
0	0	0	0	85911.72	98183.72	98184.72	12273
0	0	0	0	98184.64	110457.64	110457.64	12273
0	0	0	0	98184.68	110457.68	110457.68	12273
0	0	0	0	110457.6	122729.6	122730.6	12273
0	0	0	0	110457.64	122729.64	122730.64	12273
0	0	0	0	122730.56	135002.56	135003.56	12273
0	0	0	0	122730.6	135002.6	135003.6	12273
0	0	0	0	135003.52	147275.52	147276.52	12273
0	0	0	0	135003.56	147275.56	147276.56	12273
0	0	0	0	147276.48	159549.48	159549.48	12273
0	0	0	0	147276.52	159549.52	159549.52	12273

Figura 5.6: Retardo de extremo a extremo desde el seguimiento

5.6. Informe

Redacta el informe con las siguientes indicaciones:

- Reproduce el experimentado mostrado en este guión.
- Realiza los comentarios, pruebas y explicaciones que consideres oportunos.
- Se valorará el contenido atendiendo a los siguientes conceptos: originalidad, organización, estética, etc.
- Además, debes indicar tu valoración personal así como los conceptos aprendidos con el desarrollo de la práctica.
- El plagio será firmemente perseguido: una vez detectado plagio, serán evaluadas a 0 tanto la copia como el original.
- Entregar las memorias en formato *pdf*.
- El fichero entregado en la tarea debe de contener vuestras siglas y número práctica. Ejemplo: **Pepito Pérez Martínez entrega la práctica 5**, entonces, el nombre de fichero debe ser: **PPM-5.pdf**.



Práctica 6

Fallo de enlace



Generado: 03/01/2025 11:04:17

6.1. Objetivo

Modelado y simulación de fallos en la red así como su impacto en el rendimiento.

6.2. Teoría

Una falla en el enlace puede ocurrir debido a i) fallas en el enlace físico y ii) falla del puerto conectado. Cuando falla un enlace, los paquetes no se pueden transportar. Esto también significa que las rutas establecidas para los destinos pueden dejar de estar disponibles. En tales casos, el protocolo de enrutamiento debe recalcular un camino alternativo alrededor de la falla.

En NetSim, sólo pueden fallar los enlaces WAN (que conectan dos enrutadores) → Haga clic derecho en un enlace WAN entre dos enrutadores → ventana Propiedades del enlace se muestra en la Figura 6.1.

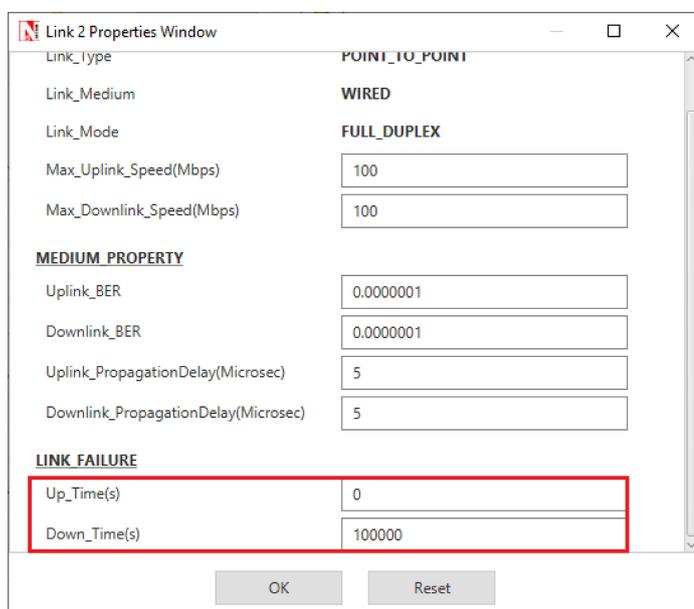


Figura 6.1: Ventana Propiedades del enlace cableado

El tiempo de actividad del enlace (Up_Time (s)) se refiere a los momentos en que el enlace está funcional y el tiempo de inactividad del enlace (Down_Time (s)) se refiere a los momentos en los que falla un enlace → Clic en Up_Time o Down_Time para comprender las opciones de configuración.

NOTA: La falla del enlace solo se puede configurar para “Interfaces WAN”.

6.3. Configuración de la red

Abra NetSim → clic en Experiments → Internetworks → Network Performance → Advanced Simulating Link Failure → clic en el mosaico en el panel central para cargar el ejemplo como se muestra en la Figura 6.2.

NetSim UI muestra el fichero de configuración correspondiente a este experimento como se muestra en la Figura 6.3.

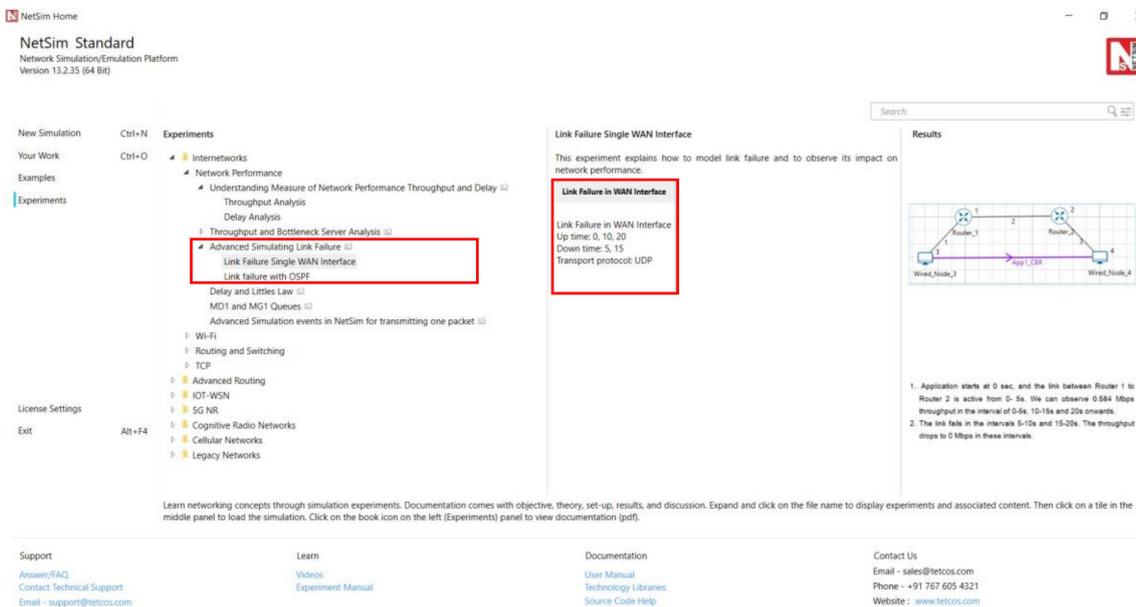


Figura 6.2: Configuración de red para estudiar la interfaz WAN única de falla de enlace

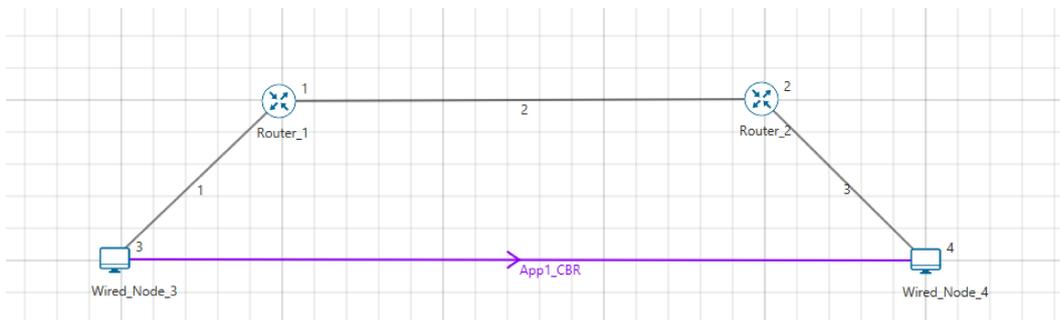


Figura 6.3: Configuración de red para el estudio de Fallo de enlace en Interface WAN

6.3.1. Procedimiento

Se realizó el siguiente conjunto de procedimientos para generar esta muestra:

1. En la biblioteca “**Internetworks**” y se diseña un escenario de red en NetSim compuesto por 2 nodos cableados y 2 enrutadores.
2. De forma predeterminada, el tiempo de actividad por falla del enlace (Up_Time) se establece en 0, 10, 20 y el tiempo de inactividad (Down_Time) se establece en 5, 15. Esto significa que el enlace está arriba 0-5s, 10-15s y 20s en adelante, y está abajo 5-10s y 15-20s.
3. Packet Trace está habilitado en la GUI de NetSim. Al final de la simulación, un archivo .csv que contiene toda la información del paquete está disponible para realizar análisis a nivel de paquete.
4. Haga clic derecho en Application Flow App1 CBR → Properties o haga clic en el icono de la aplicación presente en la cinta/barra de herramientas superior.

Se genera una aplicación CBR desde `Wired_Node_3`, es decir, desde la fuente hasta `Wired_Node_4`, es decir, Destino, manteniendo un tamaño de paquete 1460 bytes y un tiempo entre llegadas de 20000 μ s.

5. Protocolo de transporte configurado como UDP.
6. Habilite los gráficos y ejecute la simulación durante 50 segundos.

6.3.2. Salida

Vaya a la ventana de resultados de la simulación NetSim y abra el gráfico de rendimiento de la aplicación (ver Figura 6.4). Podemos observar lo siguiente:

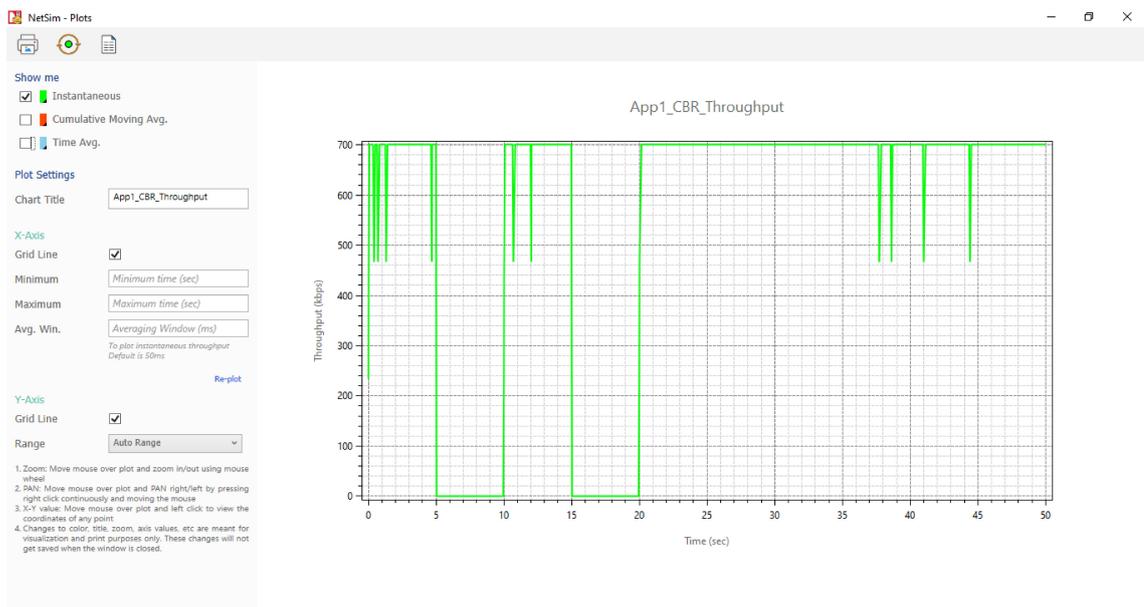


Figura 6.4: Gráfico de rendimiento de la aplicación para APP1_CBR

- La aplicación comienza en 0 segundos y el enlace entre el Router_1 y el Router_2 está activo de 0 a 5 segundos. Podemos observar un rendimiento de 0,584Mbps en el intervalo de 05 s, 1015 s y 20 s en adelante.
- El enlace falla en los intervalos de 5 a 10 segundos y de 15 a 20 segundos. El rendimiento cae a 0 Mbps en estos intervalos.

6.4. Fallo de enlace con OSPF

La interfaz UI de NetSim muestra el archivo de configuración correspondiente a este experimento como se muestra en la Figura 6.5.

6.4.1. Procedimiento

Sin error de enlace: se realizó el siguiente conjunto de procedimientos para generar este ejemplo:

1. En la biblioteca “**Internetworks**” y se diseña un escenario de red en NetSim compuesto por 2 nodos cableados y 7 enrutadores.

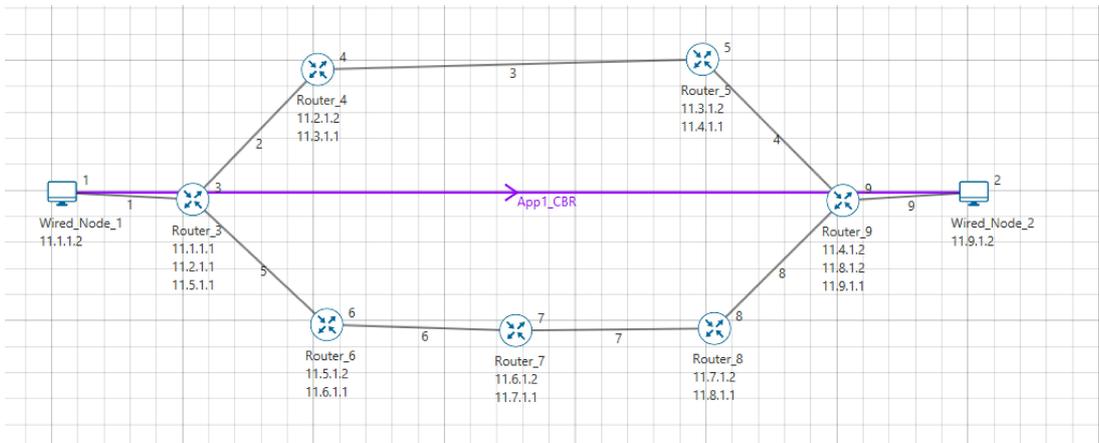


Figura 6.5: Red configurada para estudiar la falla del enlace con OSPF

- De forma predeterminada, el tiempo de actividad por falla del enlace se establece en 0 y el tiempo de inactividad se establece en 100000.
- Packet Trace está habilitado en la GUI de NetSim. Al final de la simulación, un archivo .csv que contiene toda la información del paquete está disponible para realizar análisis a nivel de paquete.
- Haga clic derecho en Application Flow App1 CBR → Propiedades o haga clic en el Icono de aplicación presente en la cinta/barra de herramientas superior.

Se genera una aplicación CBR desde Wired_Node_1, es decir, desde la fuente, hasta Wired_Node_2, es decir, Destino, manteniendo un tamaño de paquete de 1460 bytes y un tiempo entre llegadas de 20000 μ s.

Además, el parámetro “Start Time(s)” se establece en 30, mientras se configura la aplicación. Este tiempo generalmente se establece mayor que el tiempo necesario para la convergencia OSPF (es decir, el intercambio de información OSPF entre todos los enrutadores), y aumenta a medida que el tamaño de la red aumenta.

- Protocolo de transporte configurado como TCP.
- Habilite los gráficos y ejecute la simulación durante 80 segundos.

Con error de enlace: los siguientes cambios en la configuración se realizan a partir del ejemplo anterior:

- En Propiedades del enlace 3 → el tiempo de actividad por falla del enlace se establece en 0 y el tiempo de inactividad se establece en 50. Esto significa que el enlace fallaría a los 50 segundos.
- Habilite los gráficos y ejecute la simulación durante 80 segundos.

6.4.2. Salida

Vaya a la ventana de animación de paquetes de NetSim → clic en el botón Reproducir. Podemos observar lo siguiente:

- Inicialmente se intercambian paquetes de control OSPF entre todos los enrutadores.
- Una vez después del intercambio de paquetes de control, los paquetes de datos se envían desde el origen al destino.

- Los paquetes se enrutan al destino a través de $N1 > R3 > R4 > R5 > R9 > N2$, como se muestra debajo de la Figura 6.6.

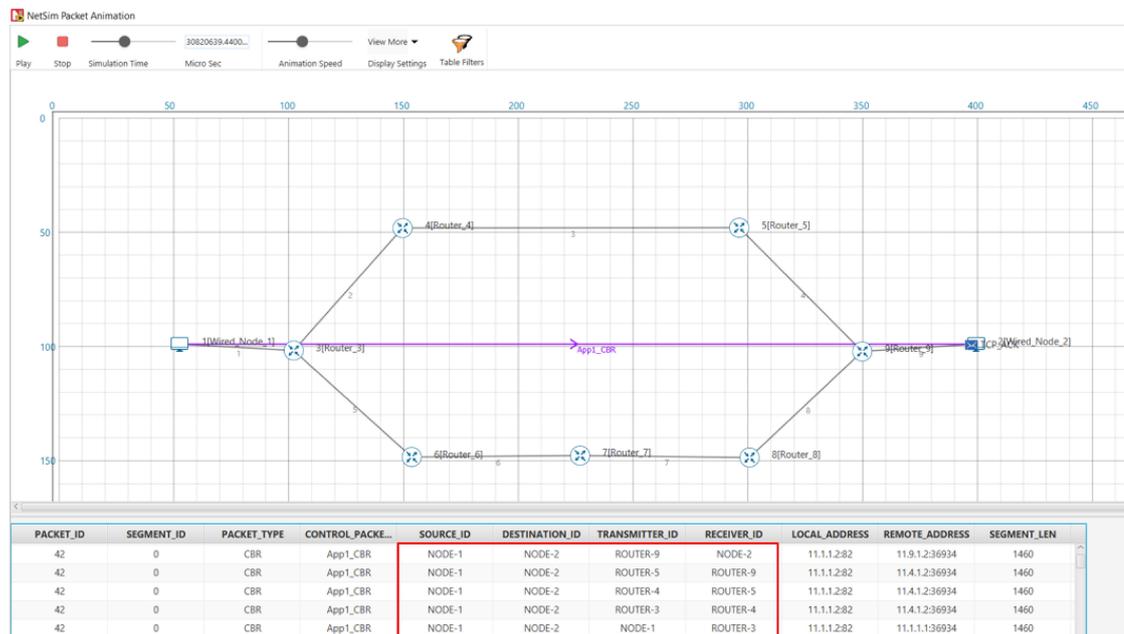


Figura 6.6: Ventana de animación sin fallo de enlace

Con fallo de enlace:

- Creamos un fallo de enlace en el Link 3, entre el Router_4 y el Router_5 a los 50s.
- Dado que los paquetes no pueden llegar al destino, el protocolo de enrutamiento vuelve a calcular un camino alternativo hacia el Destino.
- Esto se puede observar en el Packet Trace.
- Vaya al Panel de resultados \rightarrow clic en Open Packet Trce en el panel izquierdo y haga lo siguiente:
- Filtre Control Packet Type/App Name a APP1 CBR y Transmitter ID a Router_3 (ver Figura 6.7).
- Podemos observar que los paquetes han cambiado sus rutas desde $N1 > R3 > R4 > R5 > R9 > N2$ a $N1 > R3 > R6 > R7 > R8 > R9 > N2$ a los 50 s de simulación.

También podemos observarlo en la animación de paquetes antes y después del fallo de enlace, como se muestra en la Figura 6.8 y Figura 6.9.

PACKET_ID	SEGMENT_ID	PACKET_TYPE	CONTROL_PACKET_TYPE/APP_NAME	SOURCE_ID	DESTINATION_ID	TRANSMITTER_ID	RECEIVER_ID
994	0	CBR	App1_CBR	NODE-1	NODE-2	ROUTER-3	ROUTER-4
995	0	CBR	App1_CBR	NODE-1	NODE-2	ROUTER-3	ROUTER-4
996	0	CBR	App1_CBR	NODE-1	NODE-2	ROUTER-3	ROUTER-4
997	0	CBR	App1_CBR	NODE-1	NODE-2	ROUTER-3	ROUTER-4
998	0	CBR	App1_CBR	NODE-1	NODE-2	ROUTER-3	ROUTER-4
999	0	CBR	App1_CBR	NODE-1	NODE-2	ROUTER-3	ROUTER-4
1000	0	CBR	App1_CBR	NODE-1	NODE-2	ROUTER-3	ROUTER-4
1001	0	CBR	App1_CBR	NODE-1	NODE-2	ROUTER-3	ROUTER-4
1001	0	CBR	App1_CBR	NODE-1	NODE-2	ROUTER-3	ROUTER-6
1002	0	CBR	App1_CBR	NODE-1	NODE-2	ROUTER-3	ROUTER-6
1003	0	CBR	App1_CBR	NODE-1	NODE-2	ROUTER-3	ROUTER-6
1004	0	CBR	App1_CBR	NODE-1	NODE-2	ROUTER-3	ROUTER-6
1005	0	CBR	App1_CBR	NODE-1	NODE-2	ROUTER-3	ROUTER-6
1006	0	CBR	App1_CBR	NODE-1	NODE-2	ROUTER-3	ROUTER-6
1007	0	CBR	App1_CBR	NODE-1	NODE-2	ROUTER-3	ROUTER-6
1008	0	CBR	App1_CBR	NODE-1	NODE-2	ROUTER-3	ROUTER-6
1009	0	CBR	App1_CBR	NODE-1	NODE-2	ROUTER-3	ROUTER-6

Figura 6.7: Ventana de animación del paquete antes de la falla del enlace que muestra el flujo de paquetes con falla del enlace

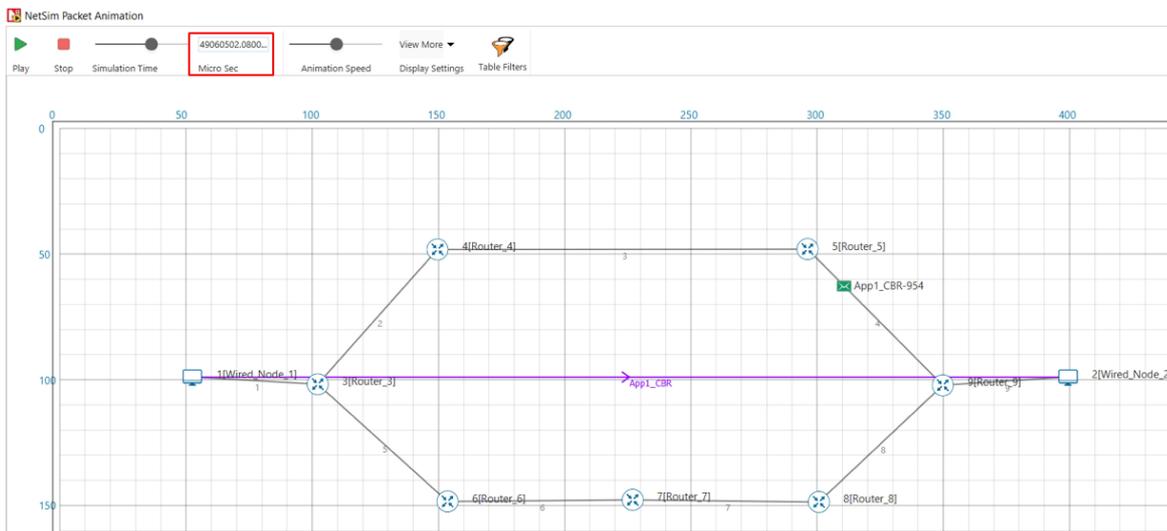


Figura 6.8: Ventana de animación de paquetes **antes** de una falla de enlace que muestra el flujo de paquetes con falla de enlace

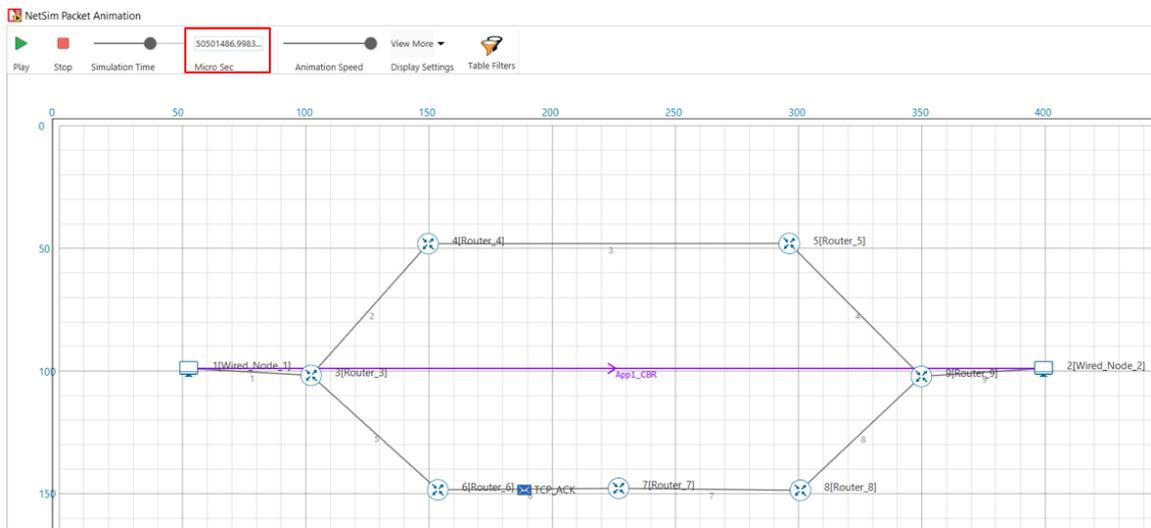


Figura 6.9: Ventana de animación de paquetes **después** de una falla de enlace que muestra el flujo de paquetes con falla de enlace

6.5. Informe

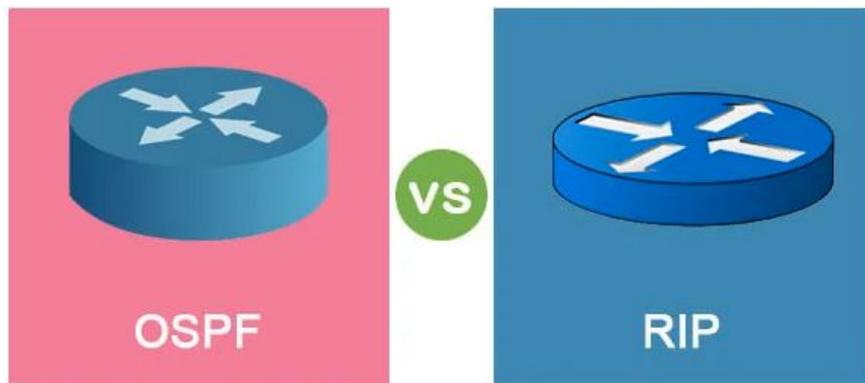
Redacta el informe con las siguientes indicaciones:

- Reproduce el experimentado mostrado en este gui3n.
- Realiza los comentarios, pruebas y explicaciones que consideres oportunos.
- Se valorar3 el contenido atendiendo a los siguientes conceptos: originalidad, organizaci3n, est3tica, etc.
- Adem3s, debes indicar tu valoraci3n personal as3 como los conceptos aprendidos con el desarrollo de la pr3ctica.
- El plagio ser3 firmemente perseguido: una vez detectado plagio, ser3n evaluadas a 0 tanto la copia como el original.
- Entregar las memorias en formato *pdf*.
- El fichero entregado en la tarea debe de contener vuestras siglas y n3mero pr3ctica. Ejemplo: **Pepito P3rez Mart3nez entrega la pr3ctica 5**, entonces, el nombre de fichero debe ser: ***PPM-5.pdf***.



Práctica 7

RIP y OSPF



Generado: 03/01/2025 11:04:17

7.1. Objetivo

Estudiar la formación de la tabla de trabajo y enrutamiento de Protocolos de enrutamiento interior, es decir, información de enrutamiento Protocolo (RIP) y Abrir primero la ruta más corta (OSPF).

7.2. Introducción

7.2.1. RIP

RIP (*Routing Internet Protocol*) está destinado a permitir que los hosts y las puertas de enlace intercambien información para rutas informáticas a través de una red basada en IP. RIP es un protocolo de vector de distancia basado en el algoritmo de BellmanFord. Este algoritmo se ha utilizado para el cálculo de enrutamiento en la red.

Los algoritmos de vector de distancia se basan en el intercambio de sólo una pequeña cantidad de información mediante mensajes RIP.

Se supone que cada entidad (enrutador o host) que participa en el protocolo de enrutamiento mantiene información sobre todos los destinos dentro del sistema. En general, información sobre todas las entidades conectadas a una red se resume en una sola entrada, que describe la ruta a todos los destinos de esa red. Este resumen es posible porque en lo que respecta a IP, el enrutamiento dentro de una red es invisible. Cada entrada en esta base de datos de enrutamiento incluye el siguiente enrutador al que se deben enviar los datagramas destinados a la entidad. Además, incluye una "métrica" que mide la distancia total a la entidad.

La distancia es un concepto algo generalizado, que puede abarcar el retardo en llegar mensajes a la entidad, el costo en dólares de enviarle mensajes, etc. Los algoritmos Vector de distancia reciben su nombre del hecho de que es posible calcular rutas óptimas cuando la única información intercambiada es la lista de estas distancias. Además, la información sólo se intercambia entre entidades adyacentes, es decir, entidades que comparten una red común.

7.2.2. OSPF

En OSPF (*Open Short Path First*), los paquetes se transmiten a través de la ruta más corta entre el origen y el destino.

OSPF permite al administrador asignar un costo por pasar por un enlace. El costo total de una ruta particular es igual a la suma de los costos de todos los enlaces que componen la ruta. Un enrutador elige la ruta con el costo más corto (el más pequeño).

En OSPF, cada enrutador tiene una base de datos de estado de enlace que es una representación tabular de la topología de la red (incluido el costo). Utilizando el algoritmo de Dijkstra, cada enrutador encuentra el camino más corto entre origen y destino.

7.2.3. Formación de la tabla de enrutamiento OSPF

1. Los enrutadores que hablan OSPF envían paquetes de saludo a todas las interfaces habilitadas para OSPF. Si dos enrutadores que comparten un enlace de datos aceptan ciertos parámetros especificados en sus respectivos paquetes *Hello*, se convertirán en vecinos.
2. Las adyacencias, que pueden considerarse como enlaces virtuales punto a punto, se forman entre algunos vecinos. OSPF define varios tipos de redes y varios tipos de enrutadores. El establecimiento de una adyacencia está determinado por los tipos de enrutadores que intercambian Hellos y el tipo de red a través de la cual se intercambian los Hellos.

3. Cada enrutador envía anuncios de estado de enlace (LSA, *Link-State Advertisements*) a todas las adyacencias. Las LSA describen todos los enlaces o interfaces del enrutador, los vecinos del enrutador y el estado de los enlaces. Estos enlaces pueden ser a redes *stub* (redes sin otro enrutador conectado), a otros enrutadores OSPF o a redes externas (redes aprendidas de otro proceso de enrutamiento). Debido a los distintos tipos de información de estado de enlace, OSPF define múltiples tipos de LSA.
4. Cada enrutador que recibe un LSA de un vecino, registra el LSA en su base de datos de estado de enlace y envía una copia del LSA a todos sus demás vecinos (inundación).
5. Mediante la
6. Al inundar los LSA en un área, todos los enrutadores crearán bases de datos de estado de enlace idénticas.
7. Cuando las bases de datos están completas, cada enrutador utiliza el algoritmo SPF (Short Path First) para calcular un grafo libre de bucles que describe la ruta más corta (de menor costo) a cada destino conocido, siendo él mismo la raíz. Este gráfico es el árbol SPF.
8. Cada enrutador crea su tabla de rutas a partir de su árbol SPF.

7.3. Configuración de la red

Abra NetSim \rightarrow clic en Experiments \rightarrow Internetworks \rightarrow Routing and Switching \rightarrow Route table formation in RIP and OSPF \rightarrow clic en el mosaico en el panel central para cargar el ejemplo como se muestra en la Figura 7.1.

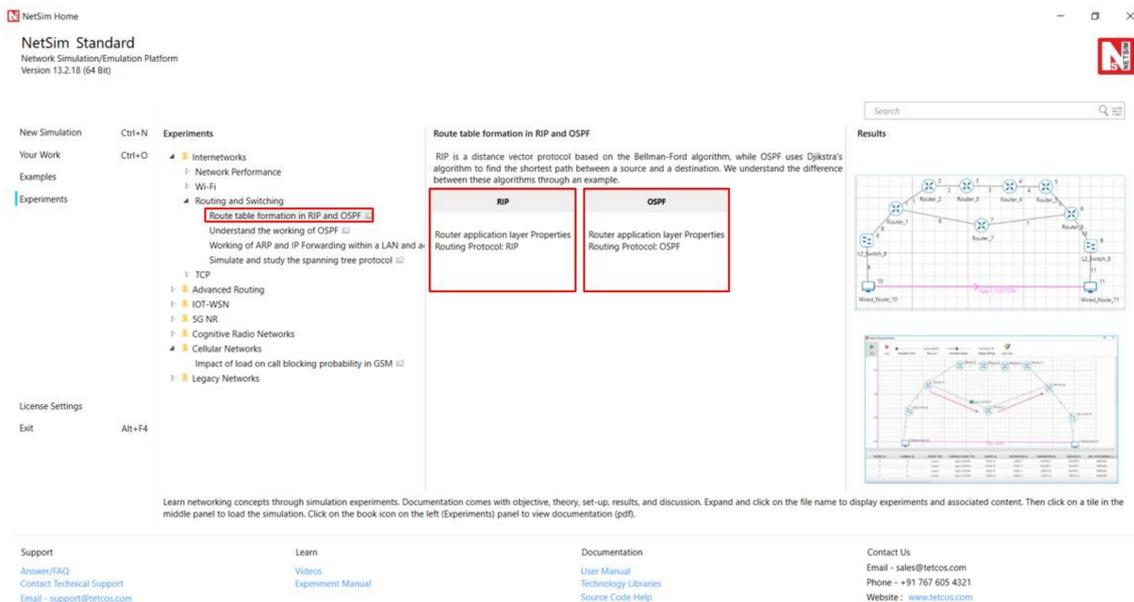


Figura 7.1: Lista de escenarios para el ejemplo de la formación de la tabla de enrutamiento en RIP y OSPF

NetSim UI muestra el fichero de configuración correspondiente a este experimento como se muestra en la Figura 7.2.

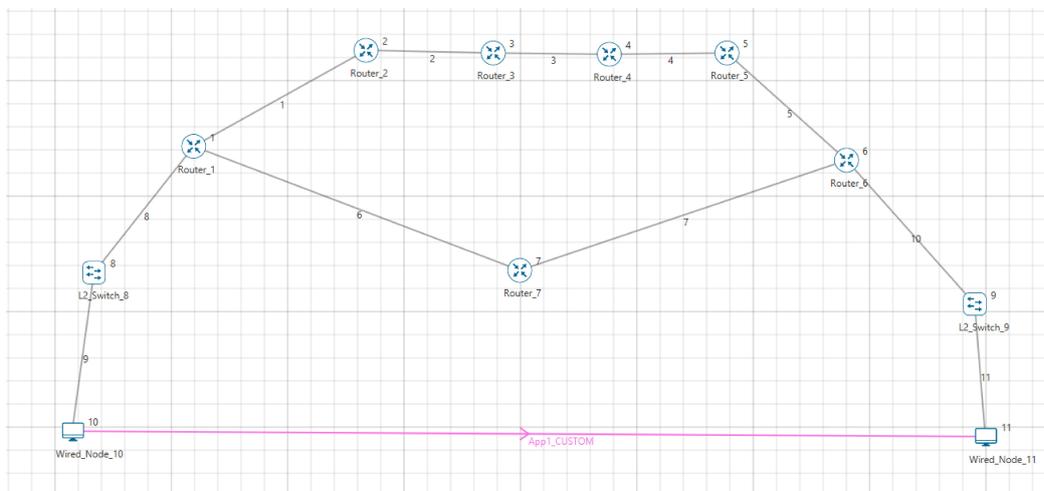


Figura 7.2: Configuración de red para el estudio de RIP/OSPF

7.4. Procedimiento

RIP:

El siguiente es el conjunto de procedimientos que se realizaron para generar esta muestra.

1. Se diseña un escenario de red en la GUI de NetSim que consta de 2 nodos cableados, 2 conmutadores L2 y 7 enrutadores.
2. Vaya a Propiedades del Router_1 → en la capa de aplicación, el protocolo de enrutamiento está configurado como RIP (ver Figura 7.3).

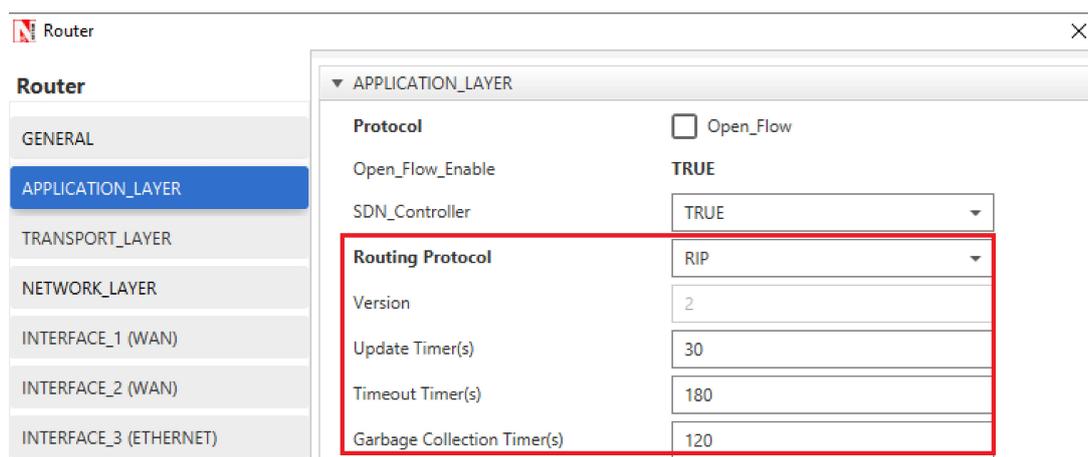


Figura 7.3: Ventana de capa de aplicación: el protocolo de enrutamiento está configurado como RIP

La ventana de configuración del enrutador que se muestra en la Figura indica el protocolo de enrutamiento configurado como RIP junto con sus parámetros asociados. El

parámetro **“Routing Protocol”** es Global, es decir, cambiar en el Router_1 afectará a todos los demás enrutadores. Entonces, en todos los enrutadores, el protocolo de enrutamiento ahora está configurado como RIP.

3. Clic derecho en App1 CUSTOM \mapsto Propiedades o haga clic en el ícono de Aplicación presente en la cinta/barra de herramientas superior. El protocolo de transporte está configurado en UDP.

Se genera una aplicación PERSONALIZADA desde Wired_ Node_10, es decir, el origen a Wired_ Node_11, es decir, el destino, manteniendo un tamaño de paquete de 1460 bytes y un tiempo entre llegadas 20000 μ s.

4. El seguimiento de paquetes está habilitado y, por lo tanto, podemos rastrear la ruta que los paquetes han elegido para llegar al destino según el protocolo de información de enrutamiento configurado.
5. Habilite los gráficos y ejecute la simulación durante 100 segundos.

OSPF:

A continuación se presenta el conjunto de procedimientos que se siguen para realizar este experimento.

1. Se diseña un escenario de red en la GUI de NetSim que consta de 2 nodos cableados, 2 conmutadores L2 y 7 enrutadores.
2. Vaya a Propiedades del enrutador 1 \mapsto en la capa de aplicación, el protocolo de enrutamiento está configurado como OSPF (ver Figura 7.4).

La ventana de configuración del enrutador que se muestra en la Figura indica el protocolo de enrutamiento configurado como RIP junto con sus parámetros asociados. El parámetro **“Routing Protocol”** es Global, es decir, cambiar en el Router_1 afectará a todos los demás enrutadores. Entonces, en todos los enrutadores, el protocolo de enrutamiento ahora está configurado como OSPF.

3. Vaya a Propiedades de Router_7 \mapsto en ambas interfaces WAN, el costo de salida se establece en 2000 (ver Figura 7.5).

El parámetro **“Costo de salida”** en la interfaz WAN \mapsto Capa de aplicación de un enrutador indica el costo de enviar un paquete de datos en esa interfaz y se expresa en la métrica del estado del enlace.

4. Clic derecho en App1 CUSTOM \mapsto Propiedades o haga clic en el ícono de la aplicación presente en la cinta/barra de herramientas superior.

Se genera una aplicación PERSONALIZADA desde el Wired_ Node_10, es decir, la fuente, al Wired_ Node_11, es decir, Destino, manteniendo un tamaño de paquete de 1460 bytes y un tiempo de llegada entre llegadas de 20000 μ s.

Además, el parámetro **“Star Time (s)”** se establece en 40, mientras se configura la aplicación. Este tiempo, generalmente, se establece en mayor que el tiempo necesario

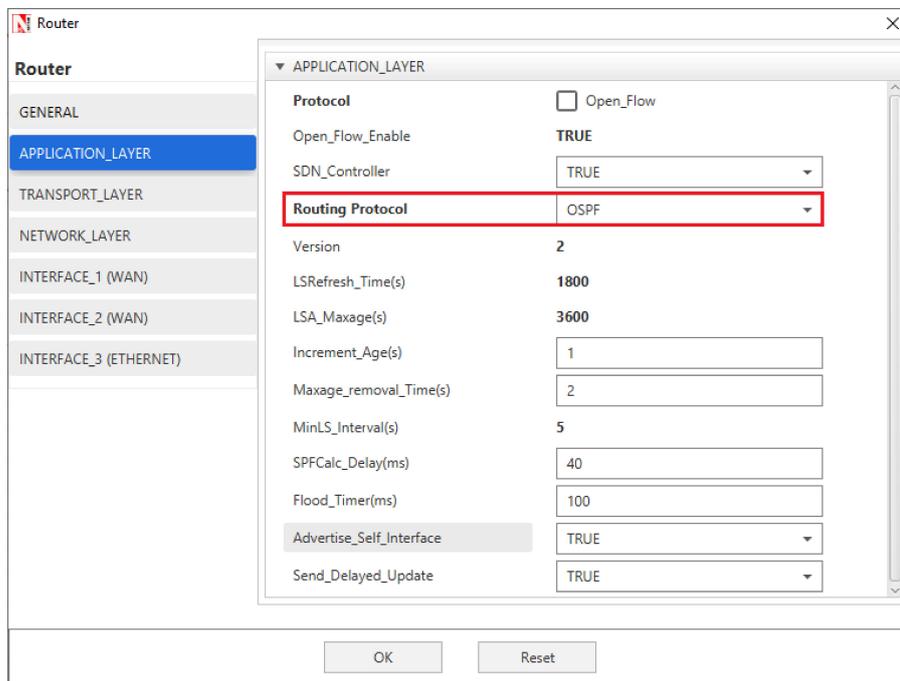


Figura 7.4: Ventana de capa de aplicación: el protocolo de enrutamiento está configurado como OSPF

para la convergencia OSPF (es decir, el intercambio de información OSPF entre todos los enrutadores), y aumenta a medida que el tamaño de la red aumenta.

5. Packet Trace está habilitado y, por lo tanto, podemos rastrear la ruta que los paquetes han elegido para llegar al destino basándose en el protocolo de enrutamiento *Open Shortest Path First*, que ha sido establecido.
6. Habilite los gráficos y ejecute la simulación durante 100 segundos.

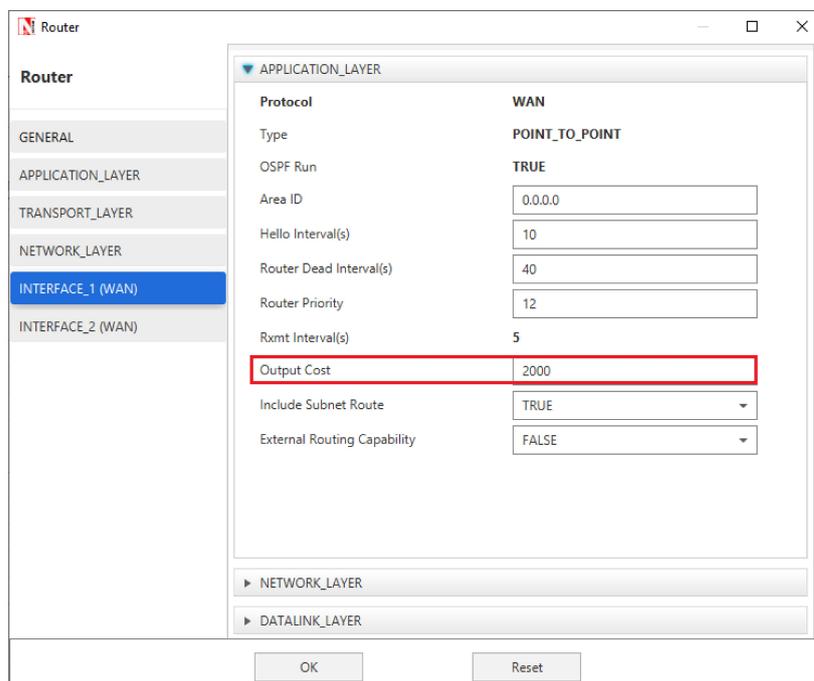


Figura 7.5: Interfaces WAN: el costo de salida se establece en 2000

7.5. 3.1.4 Salida para RIP

Vaya a la ventana NetSim Packet Animation y reproduzca la animación. La ruta que siguen los paquetes para llegar al destino se puede ver en la animación y en la siguiente tabla, que contiene varios campos de información de paquetes, como se muestra en la Figura 7.6.

Los usuarios pueden ver lo mismo en Packet Trace.

La ruta más corta desde Wired_Node_10 a Wired_Node_11 en RIP es Wired_Node_10 \rightarrow Switch_L2_8 \rightarrow Router_1 \rightarrow Router_7 \rightarrow Router_6 \rightarrow Switch_L2_9 \rightarrow Wired_Node_11. RIP elige la ruta inferior (el número de saltos es menor) para reenviar paquetes desde el origen al destino, ya que se basa en el conteo de saltos.

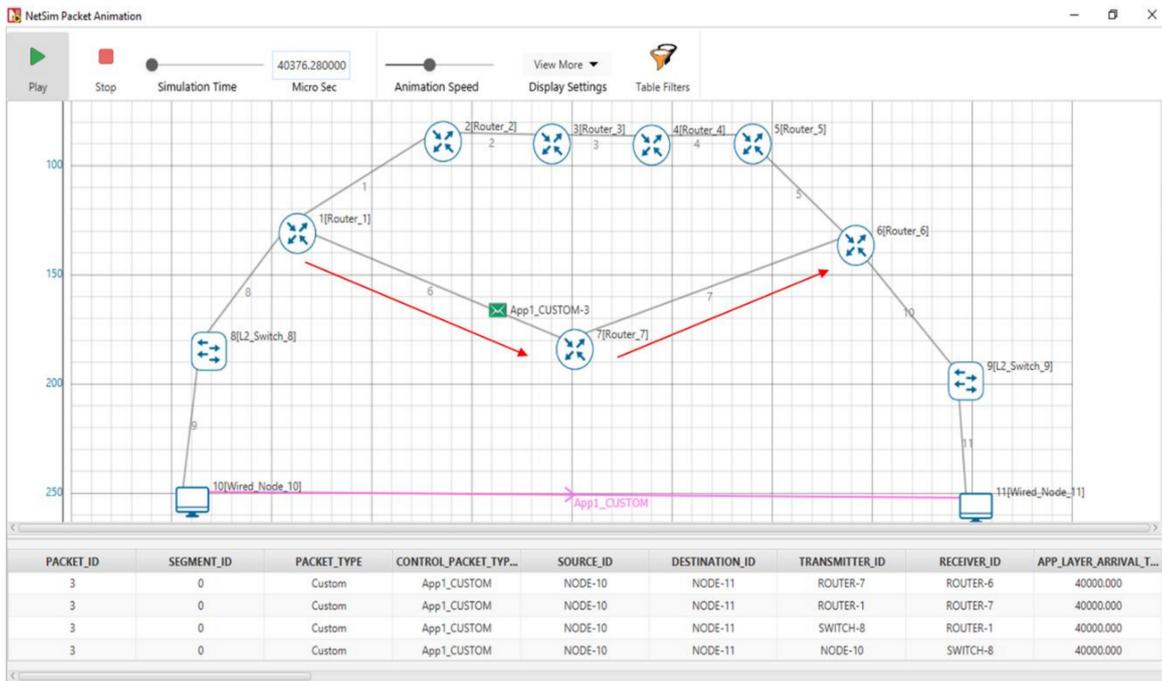


Figura 7.6: Ventana de animación para RIP

7.6. 3.1.4 Salida para OSPF

Vaya a la ventana NetSim Packet Animation y reproduzca la animación. La ruta que siguen los paquetes para llegar al destino se puede ver en la animación y en la siguiente tabla, que contiene varios campos de información de paquetes como se muestra en la Figura 7.7.

Los usuarios pueden ver lo mismo en Packet Trace.

La ruta más corta desde Wired_Node_10 a Wired_Node_11 en RIP (utilice la animación de paquetes) es Wired_Node_10 \rightarrow Switch_L2_8 \rightarrow Router_1 \rightarrow Router_2 \rightarrow Router_3 \rightarrow Router_4 \rightarrow Router_5 \rightarrow Router_6 \rightarrow Switch_L2_9 \rightarrow Wired_Node_11. OSPF elige la ruta inferior (el coste es menor, 5) para reenviar paquetes desde el origen al destino, ya que se basa en el coste.

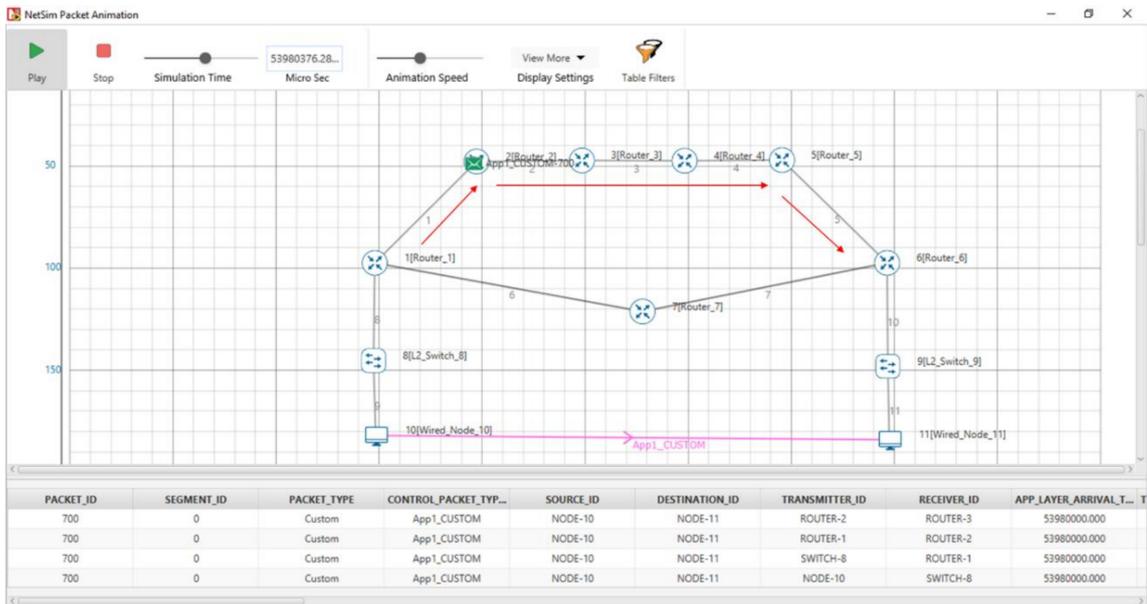


Figura 7.7: Ventana de animación para OSPF

7.7. Inferencia

7.7.1. RIP

En el enrutamiento por vector de distancia, cada enrutador comparte periódicamente su conocimiento sobre toda el red con sus vecinos. Las tres claves para entender el algoritmo:

1. **Conocimiento sobre toda la red:** el enrutador envía todo el conocimiento recopilado sobre la red a sus vecinos.
2. *Enrutamiento solo a vecinos:* cada enrutador envía periódicamente su información sobre el red sólo a aquellos enrutadores a los que tiene enlaces directos. Envía cualquier conocimiento que tenga de toda la red a través de todos sus puertos. Esta información es recibida y conservada por cada enrutador vecino y se utiliza para actualizar su propia información sobre la red.
3. **Intercambio de información a intervalos regulares:** por ejemplo, cada 30 segundos, cada enrutador envía su información sobre toda la red a sus vecinos. Este intercambio ocurre ya sea la red ha cambiado o no desde la última vez que se intercambió información

En NetSim la formación de la tabla de enrutamiento tiene 3 etapas:

1. **Tabla Inicial:** mostrará las conexiones directas realizadas por cada Router.
2. **Tabla Intermedia:** contendrá las actualizaciones de la Red en cada 30 segundos.
3. **Tabla Final:** se forma cuando no existe ninguna actualización en la Red.

Los datos deben reenviarse utilizando la tabla de enrutamiento con la distancia más corta.

7.7.2. OSPF

La operación principal del protocolo OSPF ocurre en las siguientes etapas consecutivas, y conduce a la convergencia de las redes:

1. Recopilar el LSDB (*Link State Data Base*).
2. Calcular el árbol de ruta más corta primero (SPF, Short Path First).
3. Crear las entradas de la tabla de enrutamiento.

Compilar el LSDB

LSDB es una base de datos de todos los LSA de enrutadores OSPF. El LSDB se compila mediante un intercambio continuo de LSA entre enrutadores vecinos para que cada enrutador esté sincronizado con su vecino. Cuando la red convergió, todos los enrutadores tienen las entradas apropiadas en su LSDB.

Calcular el árbol SPF utilizando el algoritmo de Dijkstra

Una vez compilado el LSDB, cada enrutador OSPF realiza un cálculo de ruta de menor costo llamado algoritmo de Dijkstra en la información del LSDB y crea un árbol de caminos más cortos para entre todos los enrutadores y redes, con ellos mismos como raíz. Este árbol se conoce como árbol SPF y contiene una ruta única y de menor costo para cada enrutador y en la red. El cálculo de la ruta de menor costo lo realiza cada enrutador, siendo él mismo la raíz del árbol.

Calcular las entradas de la tabla de enrutamiento desde el árbol SPF

Las entradas de la tabla de enrutamiento OSPF se crean a partir del árbol SPF y se produce una única entrada para cada red en el AS (Autonomous System). La métrica para la entrada de la tabla de enrutamiento es el costo calculado por OSPF, no un recuento de saltos.

Si el tiempo de inicio de la aplicación se inicia y no han cambiado, entonces:

1. Los paquetes generados antes de la convergencia de la tabla OSPF pueden descartarse en la puerta de enlace del enrutador.
2. La aplicación también puede detenerse si ICMP está habilitado en el enrutador.
3. Si TCP está habilitado, TCP puede detenerse después de alcanzar el límite de reintentos (ya que los paquetes SYN no llegaría al destino).

NOTA: La numeración del dispositivo/enlace y la configuración de la dirección IP en NetSim se basan en el orden en que los dispositivos se arrastran/sueltan, y el orden en que se conectan los enlaces. Por lo tanto, si el orden en el que un usuario ejecuta estas tareas es diferente de

lo que se muestra en las capturas de pantalla, los usuarios notarán tablas diferentes de lo que se muestra en las capturas de pantalla.

7.8. Informe

Redacta el informe con las siguientes indicaciones:

- Reproduce el experimentado mostrado en este guión.
- Realiza los comentarios, pruebas y explicaciones que consideres oportunos.
- Se valorará el contenido atendiendo a los siguientes conceptos: originalidad, organización, estética, etc.
- Además, debes indicar tu valoración personal así como los conceptos aprendidos con el desarrollo de la práctica.
- El plagio será firmemente perseguido: una vez detectado plagio, serán evaluadas a 0 tanto la copia como el original.
- Entregar las memorias en formato *pdf*.
- El fichero entregado en la tarea debe de contener vuestras siglas y número práctica. Ejemplo: **Pepito Pérez Martínez entrega la práctica 5**, entonces, el nombre de fichero debe ser: *PPM-5.pdf*.



Práctica 8

ARP y reenvío de paquetes

ARP
*Address
Resolution
Protocol*

Generado: 03/01/2025 11:04:17

8.1. Objetivo

Comprender el funcionamiento de ARP y el reenvío de IP dentro de un LAN y a través de un enrutador

8.2. Teoría

En la arquitectura de red, las diferentes capas tienen su propio esquema de direccionamiento. Esto ayuda a las diferentes capas son en gran medida independientes. La capa de aplicación utiliza nombres de host, la capa de red utiliza direcciones IP y la capa de enlace utiliza direcciones MAC. Siempre que un nodo fuente quiera enviar un datagrama IP a un nodo de destino, necesita conocer la dirección del destino. Dado que hay direcciones IP y direcciones MAC, es necesario realizar una traducción entre ellos. Esta traducción es manejada por el Protocolo de resolución de direcciones (ARP, *Address Resolution Protocol*). En redes IP, el enrutamiento IP implica la determinación de la ruta adecuada para un paquete de red desde un origen hasta su destino. Si la dirección de destino no está en la red local, los enrutadores reenvían los paquetes a la siguiente red adyacente.

(Referencia: una buena referencia para este tema es la Sección 5.4.1: Direccionamiento de capa de enlace y ARP, del libro *Computer Networking, A TopDown Approach*, sexta edición de Kurose y Ross)

8.3. Descripción Protocolo ARP

1. El módulo ARP en el host de envío toma cualquier dirección IP como entrada y devuelve la dirección MAC correspondiente.
2. Primero, el remitente construye un paquete especial llamado paquete ARP, que contiene varios campos, incluidas las direcciones IP y MAC de envío y recepción.
3. Tanto los paquetes de solicitud como de respuesta ARP tienen el mismo formato.
4. El propósito del paquete de solicitud ARP es consultar todos los demás hosts y enrutadores en la subred para determinar la dirección MAC correspondiente a la dirección IP que se está resolviendo.
5. El remitente transmite el paquete de solicitud ARP, que es recibido por todos los hosts en la subred.
6. Cada nodo verifica si su dirección IP coincide con la dirección IP de destino en el paquete ARP.
7. El que coincide envía al host que realiza la consulta un paquete ARP de respuesta con el mapeo deseado.
8. Cada host y enrutador tiene una tabla ARP en su memoria, que contiene el mapeo de direcciones IP a direcciones MAC.

9. La tabla ARP también contiene un valor de tiempo de vida (TTL, Time To Live), que indica cuándo cada La asignación se eliminará de la tabla.

8.4. Formato de trama ARP

El formato de mensaje ARP está diseñado para acomodar las direcciones de capa dos y tres de varios tamaños. Este diagrama (ver Figura 8.1) muestra la implementación más común, que utiliza 32 bits para las direcciones de capa tres (“Protocolo”) y 48 bits para las direcciones de hardware de capa dos.

Hardware Type		Protocol Type
Hardware Address Length	Protocol address length	Opcode
Sender Hardware Address		
Sender Protocol Address (1-2)		Sender Protocol Address (3-4)
Target hardware Address		
Target Protocol Address		

Figura 8.1: Formato de trama ARP

8.5. Descripción de reenvío de IP

1. Cada enrutador tiene una tabla de reenvío que asigna las direcciones de destino (o partes de las direcciones de destino) a los enlaces salientes de ese enrutador.
2. Un enrutador reenvía un paquete examinando el valor de un campo en la cabecera del paquete entrante y luego usa este valor de la cabecera para indexar en la tabla de reenvío del enrutador.
3. El valor almacenado en la entrada de la tabla de reenvío para esa cabecera indica la interface de salida del enrutador del enlace por el el se reenviará ese paquete.
4. Dependiendo del protocolo de capa de red, el valor de la cabecera podría ser la dirección destino del paquete o una indicación de la conexión a la que pertenece el paquete.
5. ARP opera cuando un host quiere enviar un datagrama a otro host en la misma subred.
6. Al enviar un datagrama fuera de la subred, el datagrama primero debe enviarse al enrutador de primer salto en el camino hacia el destino final. La dirección MAC de la interfaz del enrutador se adquiere mediante ARP.
7. El enrutador determina la interfaz en la que se reenviará el datagrama consultando su tabla de reenvío.

8. El enrutador obtiene la dirección MAC del nodo de destino mediante ARP.
9. El enrutador envía el paquete a la subred respectiva desde la interfaz que fue identificada utilizando la tabla de reenvío.

8.6. Configuración de la red

Abra NetSim \rightarrow clic en Experiments \rightarrow Internetworks \rightarrow Routing and Switching \rightarrow Working of ARP and IP Forwarding within a LAN and across a router \rightarrow luego clic en el mosaico en el panel central para cargar el como se muestra en el ejemplo, consulte la Figura 8.2.

The screenshot shows the NetSim Standard interface. On the left, the 'Experiments' panel is expanded to 'Routing and Switching', where the experiment 'Working of ARP and IP Forwarding within a LAN and across a router' is highlighted with a red box. The central panel displays the experiment's title and a brief description. Below this, a table compares configurations for LAN and WAN:

ARP across a LAN	ARP across a WAN
Custom application across LAN with Transport Protocol: UDP Packet Size: 1460 Bytes Inter arrival time: 20000 μ s Static ARP Configuration: Disable	Custom application across WAN with Transport Protocol: UDP Packet Size: 1460 Bytes Inter arrival time: 20000 μ s Static ARP Configuration: Disable

The right panel shows the 'Results' section, which includes a network diagram with nodes like Router_1, Router_2, L2_Switch_4, L2_Switch_5, and Wired_Node_1 through 3. Below the diagram is a flow diagram titled 'ARP PROTOCOL WORKING' showing the sequence: Source \rightarrow ARP \rightarrow Switch \rightarrow ARP \rightarrow Destination.

Figura 8.2: Lista de escenarios para el ejemplo de Manejo de ARP y reenvío IP en una LAN y a través de router

NetSim UI muestra el fichero de configuración correspondiente a este experimento como se muestra en la Figura 8.3.

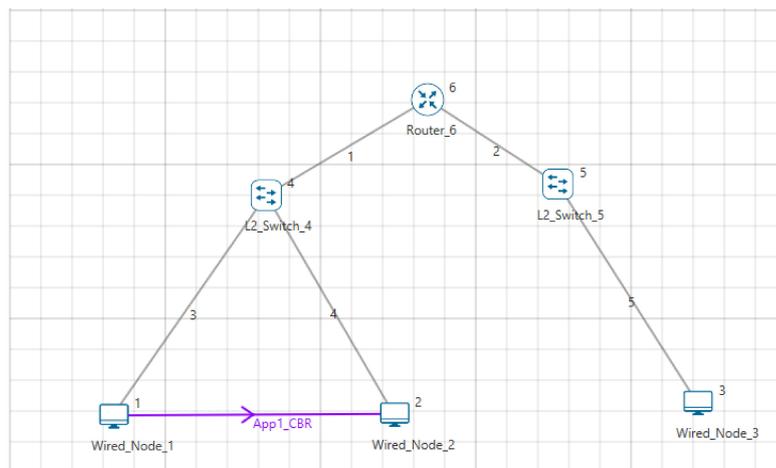


Figura 8.3: Red configurada para analizar ARP a través de una LAN

8.7. Procedimiento

ARP a través de una LAN

Se realizó el siguiente conjunto de procedimientos para generar esta muestra:

1. Se diseña un escenario de red en la GUI de NetSim que consta de 3 nodos cableados, 2 L2 Switches y 1 enrutador en la biblioteca de red “**Internetworks**”.
2. Clic derecho en Application Flow App1 CBR \rightarrow seleccione Propiedades o haga clic en el Icono de aplicación presente en la cinta/barra de herramientas superior.

Se genera una aplicación CBR desde Wired_Node_1, es decir, desde la fuente, hasta Wired_Node_2, es decir, Destino, manteniendo un tamaño de paquete de 1460 bytes y un tiempo entre llegadas de 20000 μ s.

El protocolo de transporte está configurado en UDP en lugar de TCP. Si se establece en TCP, la tabla ARP se actualizará debido a la transmisión de paquetes de control TCP, eliminando así la necesidad de que ARP resuelva direcciones.

3. Packet Trace está habilitado en la GUI de NetSim y, por lo tanto, podemos ver la solicitud ARP y paquetes de respuesta ARP intercambiados inicialmente, antes de la transmisión de los paquetes de datos.
4. Habilite los gráficos y haga clic en Ejecutar simulación \rightarrow el tiempo de simulación se establece en 10 segundos \rightarrow En la pestaña “**Static ARP Configuration**”, ARP estática desactivada (consulte la Figura 8.4) \rightarrow clic en Accept \rightarrow clic OK.

Si ARP estático está habilitado, NetSim creará automáticamente una tabla ARP para cada nodo. Para ver el funcionamiento del protocolo ARP, los usuarios deben desactivar el ARP estático. Al hacerlo, la solicitud ARP se enviará al destino para conocer la dirección MAC del destino.

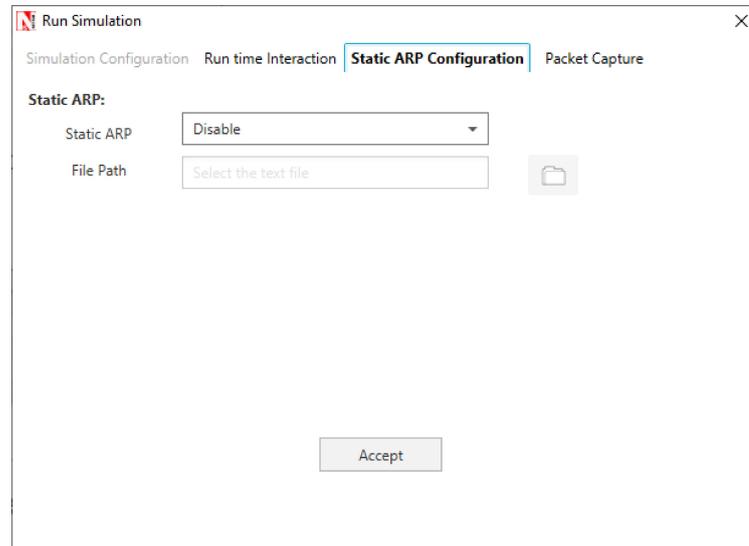


Figura 8.4: Ventana de configuración de ARP estática

8.8. Salida - ARP a través de una LAN

Una vez completada la simulación, para ver el archivo de seguimiento de paquetes ↪ clic **Open Packet Trace**", opción presente en el lado izquierdo del Panel de resultados (consulte la Figura 8.5).

PACKET_ID	SEGMENT_ID	PACKET_TYPE	CONTROL_PACKET_TYPE/APP_NAME	SOURCE_ID	DESTINATION_ID	TRANSMITTER_ID	RECEIVER_ID
0	N/A	Control_Packet	ARP_Request	NODE-1	Broadcast-0	NODE-1	SWITCH-4
0	N/A	Control_Packet	ARP_Request	NODE-1	Broadcast-0	SWITCH-4	ROUTER-6
0	N/A	Control_Packet	ARP_Request	NODE-1	Broadcast-0	SWITCH-4	NODE-2
0	N/A	Control_Packet	ARP_Reply	NODE-2	NODE-1	NODE-2	SWITCH-4
0	N/A	Control_Packet	ARP_Reply	NODE-2	NODE-1	SWITCH-4	NODE-1

Figura 8.5: Seguimiento de paquetes

El NODO 1 enviará ARP_REQUEST al SWITCH4, el SWITCH4 lo envía al ROUTER-6 y SWITCH4 también envía esto al NODO2. ARP_REPLY es enviado por el NODO2 al SWITCH4, y a su vez el SWITCH4 lo envía al NODO1.

8.9. Discusión: ARP a través de una LAN

Reenvío IP INTRA-LAN:

El NODO-1 difunde ARP_Request, que luego es difundido por SWITCH-4. NODO-2 envía el ARP_Reply al NODO-1 a través del SWITCH-4. Después de este paso, los datagramas se transmiten desde NODO-1 al NODO-2. Observe la columna DESTINATION_ID para paquetes de tipo ARP_Request, lo que indica Broadcast-0 (consulte la Figura 8.6).

ARP a través de WAN



Figura 8.6: Reenvío IP intra LAN

NetSim UI muestra el fichero de configuración correspondiente a este experimento como se muestra en la Figura 8.7.

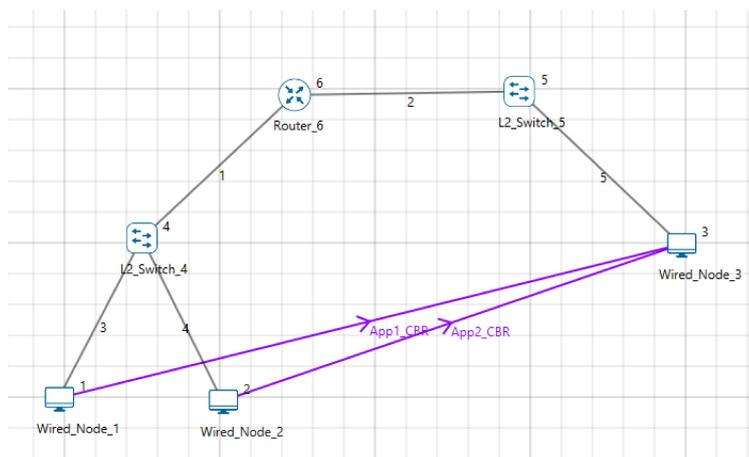


Figura 8.7: Red configurada para analizar ARP a través de una WAN

8.10. Procedimiento

Se realizó el siguiente conjunto de procedimientos para generar esta muestra.

1. Se diseña un escenario de red en la GUI de NetSim que consta de 3 nodos cableados, 2 Switches L2 y 1 Router.
2. Clic derecho en la barra de herramientas de la aplicación ⇨ seleccione Propiedades o haga clic en la Aplicación icono presente en la cinta/barra de herramientas superior.

Se crea APP 1 CBR desde Wired_Node_1 a Wired_Node_3, el tamaño del paquete se establece en 1460 bytes, tiempo de llegada entre 20000 μ s y protocolo de capa de transporte a UDP.

Se crea APP 1 CBR desde Wired_Node_2 a Wired_Node_3, el tamaño del paquete se establece en 1460 bytes, tiempo de llegada entre 20000 μ s y protocolo de capa de transporte a UDP. Además, el tiempo de inicio se establece en 1 segundo y la hora de finalización en 3 segundos.

El protocolo de transporte está configurado en UDP en lugar de TCP. Si se establece en TCP, la tabla ARP se actualizará durante la transmisión de paquetes de control TCP, eliminando así la necesidad de que ARP resuelva direcciones.

3. Packet Trace está habilitado en la GUI de NetSim y, por lo tanto, podemos ver la solicitud ARP y paquetes de respuesta ARP intercambiados inicialmente, antes de la transmisión de los paquetes de datos.
4. Haga clic en Ejecutar simulación. El tiempo de simulación se establece en 10 segundos. En el "Static ARP Configuration", ARP estático está deshabilitado.

8.11. Salida I: ARP a través de una WAN

Una vez que se completa la simulación, para ver el archivo de seguimiento de paquetes → "Open Packet Trace", en el lado izquierdo del Panel de resultados.

En el seguimiento de paquetes, filtre el campo CONTROL PACKET TYPE/APP NAME para ver la APP 1CBR, ARP_REQUEST, ARP_REPLY (ver Figura 8.8).

PACKET ID	SEGMENT ID	PACKET TYPE	CONTROL PACKET TYPE/APP NAME	SOURCE ID	DESTINATION ID	TRANSMITTER ID	RECEIVER ID
0	N/A	Control_Packet	ARP_Request	NODE-1	Broadcast-0	NODE-1	SWITCH-4
0	N/A	Control_Packet	ARP_Request	NODE-1	Broadcast-0	SWITCH-4	ROUTER-6
0	N/A	Control_Packet	ARP_Request	NODE-1	Broadcast-0	SWITCH-4	NODE-2
0	N/A	Control_Packet	ARP_Reply	ROUTER-6	NODE-1	ROUTER-6	SWITCH-4
0	N/A	Control_Packet	ARP_Reply	ROUTER-6	NODE-1	SWITCH-4	NODE-1
1	0	CBR	App1_CBR	NODE-1	NODE-3	NODE-1	SWITCH-4
1	0	CBR	App1_CBR	NODE-1	NODE-3	SWITCH-4	ROUTER-6
0	N/A	Control_Packet	ARP_Request	ROUTER-6	Broadcast-0	ROUTER-6	SWITCH-5
0	N/A	Control_Packet	ARP_Request	ROUTER-6	Broadcast-0	SWITCH-5	NODE-3
0	N/A	Control_Packet	ARP_Reply	NODE-3	ROUTER-6	NODE-3	SWITCH-5
0	N/A	Control_Packet	ARP_Reply	NODE-3	ROUTER-6	SWITCH-5	ROUTER-6
1	0	CBR	App1_CBR	NODE-1	NODE-3	ROUTER-6	SWITCH-5
1	0	CBR	App1_CBR	NODE-1	NODE-3	SWITCH-5	NODE-3
2	0	CBR	App1_CBR	NODE-1	NODE-3	NODE-1	SWITCH-4
2	0	CBR	App1_CBR	NODE-1	NODE-3	SWITCH-4	ROUTER-6
2	0	CBR	App1_CBR	NODE-1	NODE-3	ROUTER-6	SWITCH-5
2	0	CBR	App1_CBR	NODE-1	NODE-3	SWITCH-5	NODE-3
3	0	CBR	App1_CBR	NODE-1	NODE-3	NODE-1	SWITCH-4
3	0	CBR	App1_CBR	NODE-1	NODE-3	SWITCH-4	ROUTER-6
3	0	CBR	App1_CBR	NODE-1	NODE-3	ROUTER-6	SWITCH-5
3	0	CBR	App1_CBR	NODE-1	NODE-3	SWITCH-5	NODE-3
4	0	CBR	App1_CBR	NODE-1	NODE-3	NODE-1	SWITCH-4

Figura 8.8: Seguimiento de paquetes

NODE-1 enviará ARP_REQUEST a SWITCH4, el SWITCH4 lo envía a ROUTER6 y SWITCH4 también lo envía a NODE2. ROUTER6 envía ARP_REPLY a SWITCH4 y, a su vez, SWITCH4 lo envía a NODE1. Nuevamente, ROUTER6 enviará ARP_REQUEST a SWITCH5, SWITCH5 lo envía a NODE3. ARP_REPLY es enviado por NODE3 a SWITCH5 y a su vez, SWITCH5 lo envía a ROUTER6.

Se puede acceder a la tabla de reenvío de IP formada en el enrutador desde la lista IP_Forwarding presente en la ventana Resultados de la simulación, como se muestra a continuación en la Figura 8.9. Haga clic en la casilla de verificación Vista detallada para ver los campos adicionales

como se indica en la Figura.



Network Destination	Netmask/Prefix len	Gateway	Interface
11.2.0.0	255.255.0.0	on-link	11.2.1.1
11.1.0.0	255.255.0.0	on-link	11.1.1.1
224.0.0.1	255.255.255.255	on-link	11.1.1.1 11.2.1.1
224.0.0.0	240.0.0.0	on-link	11.1.1.1 11.2.1.1
255.255.255.255	255.255.255.255	on-link	11.2.1.1
255.255.255.255	255.255.255.255	on-link	11.1.1.1

Figura 8.9: Tabla de reenvío IP

El enrutador reenvía paquetes destinados a la subred 11.2.0.0 a la interfaz con la IP 11.2.1.11 basado en la primera entrada en su tabla de enrutamiento.

8.12. Discusión I – ARP a través de una WAN

Del caso anterior podemos entender que, dado que Router_6 no conocía la dirección del destino, los paquetes de la aplicación llegan sólo hasta el Router_6, y el mecanismo ARP continúa con Router_6, retransmite el ARP_REQUEST, encuentra la dirección de destino y el datagrama se transfiere a Wired_Node_3 (destino).

8.13. Salida II – ARP a través de una WAN

En el mismo seguimiento de paquete, filtre la columna CONTROL PACKET TYPE/APP NAME para visualiza APP 2 CBR, ARP_REQUEST, ARP_REPLY.

En la siguiente Figura 8.10 puede observar que ARP_REQUEST se transmite desde Wired_Node_2, la Respuesta ARP se envía desde el Router_6, al recibir el ARP_REPLY. Router_6, directamente, comienza a enviar el paquete de datos al Wired_Node_3 a diferencia del ejemplo anterior.

PACKET ID	SEGMENT ID	PACKET TYPE	CONTROL_PACKET TYPE/APP NAME	SOURCE ID	DESTINATION ID	TRANSMITTER ID	RECEIVER ID	APP LAYER ARRIVAL TIME(US)	TRX LAYER ARRIVAL TIME(US)
0	N/A	Control_Packet	ARP_Request	NODE-1	Broadcast-0	NODE-1	SWITCH-4	N/A	N/A
0	N/A	Control_Packet	ARP_Request	NODE-1	Broadcast-0	SWITCH-4	ROUTER-6	N/A	N/A
0	N/A	Control_Packet	ARP_Request	NODE-1	Broadcast-0	SWITCH-4	NODE-2	N/A	N/A
0	N/A	Control_Packet	ARP_Reply	ROUTER-6	NODE-1	SWITCH-4	NODE-1	N/A	N/A
0	N/A	Control_Packet	ARP_Request	ROUTER-6	Broadcast-0	ROUTER-6	SWITCH-5	N/A	N/A
0	N/A	Control_Packet	ARP_Request	ROUTER-6	Broadcast-0	SWITCH-5	NODE-3	N/A	N/A
0	N/A	Control_Packet	ARP_Reply	NODE-3	ROUTER-6	NODE-3	SWITCH-5	N/A	N/A
0	N/A	Control_Packet	ARP_Request	NODE-2	Broadcast-0	NODE-2	SWITCH-4	N/A	N/A
0	N/A	Control_Packet	ARP_Request	NODE-2	Broadcast-0	SWITCH-4	ROUTER-6	N/A	N/A
0	N/A	Control_Packet	ARP_Reply	ROUTER-6	NODE-2	ROUTER-6	SWITCH-4	N/A	N/A
0	N/A	Control_Packet	ARP_Reply	ROUTER-6	NODE-2	SWITCH-4	NODE-2	N/A	N/A
1	0	CBR	App2_CBR	NODE-2	NODE-3	NODE-2	SWITCH-4	1000000	1000000
1	0	CBR	App2_CBR	NODE-2	NODE-3	SWITCH-4	ROUTER-6	1000000	1000000
1	0	CBR	App2_CBR	NODE-2	NODE-3	ROUTER-6	SWITCH-5	1000000	1000000
1	0	CBR	App2_CBR	NODE-2	NODE-3	SWITCH-5	NODE-3	1000000	1000000
2	0	CBR	App2_CBR	NODE-2	NODE-3	NODE-2	SWITCH-4	1020000	1020000
2	0	CBR	App2_CBR	NODE-2	NODE-3	SWITCH-4	ROUTER-6	1020000	1020000
2	0	CBR	App2_CBR	NODE-2	NODE-3	ROUTER-6	SWITCH-5	1020000	1020000
2	0	CBR	App2_CBR	NODE-2	NODE-3	SWITCH-5	NODE-3	1020000	1020000
3	0	CBR	App2_CBR	NODE-2	NODE-3	NODE-2	SWITCH-4	1040000	1040000
3	0	CBR	App2_CBR	NODE-2	NODE-3	SWITCH-4	ROUTER-6	1040000	1040000
3	0	CBR	App2_CBR	NODE-2	NODE-3	ROUTER-6	SWITCH-5	1040000	1040000
3	0	CBR	App2_CBR	NODE-2	NODE-3	SWITCH-5	NODE-3	1040000	1040000
4	0	CBR	App2_CBR	NODE-2	NODE-3	NODE-2	SWITCH-4	1060000	1060000
4	0	CBR	App2_CBR	NODE-2	NODE-3	SWITCH-4	ROUTER-6	1060000	1060000
4	0	CBR	App2_CBR	NODE-2	NODE-3	ROUTER-6	SWITCH-5	1060000	1060000
4	0	CBR	App2_CBR	NODE-2	NODE-3	SWITCH-5	NODE-3	1060000	1060000
5	0	CBR	App2_CBR	NODE-2	NODE-3	NODE-2	SWITCH-4	1080000	1080000
5	0	CBR	App2_CBR	NODE-2	NODE-3	SWITCH-4	ROUTER-6	1080000	1080000

Figura 8.10: Seguimiento de paquetes

8.14. Discusión II – ARP a través de una WAN

Reenvío de IP a través del enrutador

NODE2 transmite ARP_Request que luego es transmitido por SWITCH4. ROUTER6 envía ARP_Reply a NODE2 que pasa por SWITCH4. Entonces NODE2 comienza a enviar datagramas a NODE3. Si el enrutador tiene la dirección MAC de NODE3 en su tabla ARP, entonces ARP termina aquí, y el enrutador comienza a reenviar los datagramas a NODE3 consultando su tabla de reenvío. El router 6 tiene esta información actualizada durante la transmisión de paquetes APP1 y, por lo tanto, no es necesario volver a enviar la solicitud ARP para identificar la dirección MAC de NODE3. En el otro caso (Salida I), el enrutador envía ARP_Request a la subred adecuada y, después de obtener la dirección MAC de NODE3, reenvía los datagramas a NODE3 utilizando su tabla de reenvío (ver Figura 8.11).

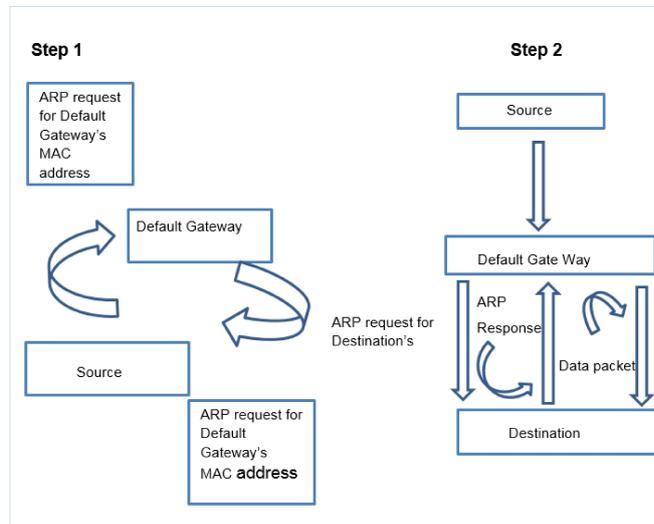


Figura 8.11: Reenvío de IP a través del enrutador

8.15. Informe

Redacta el informe con las siguientes indicaciones:

- Reproduce el experimentado mostrado en este guión.
- Realiza los comentarios, pruebas y explicaciones que consideres oportunos.
- Se valorará el contenido atendiendo a los siguientes conceptos: originalidad, organización, estética, etc.
- Además, debes indicar tu valoración personal así como los conceptos aprendidos con el desarrollo de la práctica.
- El plagio será firmemente perseguido: una vez detectado plagio, serán evaluadas a 0 tanto la copia como el original.
- Entregar las memorias en formato *pdf*.
- El fichero entregado en la tarea debe de contener vuestras siglas y número práctica. Ejemplo: **Pepito Pérez Martínez entrega la práctica 5**, entonces, el nombre de fichero debe ser: *PPM-5.pdf*.