MANUAL DE PRÁCTICAS DE LABORATORIO

Medios y Protocolos de Comunicación

Laboratorio

Programa Académico	**Ingeniero en Software**
Plan de Estudios	**2022**
Fecha de elaboración	**30/06/2025**
Versión del Documento	**1**

UES
Universidad Estatal de Sonora
La Fuerza del Saber Estimulará mi Espíritu

Dra. Martha Patricia Patiño Fierro
Rectora

Mtra. Ana Lisette Valenzuela Molina
Encargada del Despacho de la Secretaría General Académica

Mtro. José Antonio Romero Montaño
Secretario General Administrativo

Lic. Jorge Omar Herrera Gutiérrez
Encargado de Despacho de Secretario General de Planeación

Tabla de contenido

INTRODUCCIÓN

Como parte de las herramientas esenciales para la formación académica de los estudiantes de la Universidad Estatal de Sonora, se definen manuales de práctica de laboratorio como elemento en el cual se define la estructura normativa de cada práctica y/o laboratorio, además de representar una guía para la aplicación práctica del conocimiento y el desarrollo de las competencias clave en su área de estudio. Su diseño se encuentra alineado con el modelo educativo institucional, el cual privilegia el aprendizaje basado en competencias, el aprendizaje activo y la conexión con escenarios reales.

Con el propósito de fortalecer la autonomía de los estudiantes, su pensamiento crítico y sus habilidades para la resolución de problemas, las prácticas de laboratorio integran estrategias didácticas como el aprendizaje basado en proyectos, el trabajo colaborativo, la experimentación guiada y el uso de tecnologías educativas. De esta manera, se promueve un proceso de enseñanza-aprendizaje dinámico, en el que los estudiantes no solo adquieren conocimientos teóricos, sino que también desarrollan habilidades prácticas y reflexivas para su desempeño profesional.

Señalar en este apartado brevemente los siguientes elementos según corresponda:

- Propósito del manual
- Justificación de su uso en el programa académico
- Competencias a desarrollar
    - **Competencias blandas:** Habilidades transversales que se refuerzan en las prácticas, como la comunicación, el trabajo en equipo, el uso de tecnologías, etc.
    - **Competencias disciplinares:** Conocimientos específicos del área del laboratorio, incluyendo fundamentos teóricos y habilidades técnicas.
    - **Competencias profesionales:** Aplicación de los conocimientos adquiridos en escenarios reales o simulados, en concordancia con el perfil de egreso del programa.

IDENTIFICACIÓN

Nombre de la Asignatura		Medios y Protocolos de Comunicación	
Clave	061CP031	Créditos	
Asignaturas Antecedentes	061CP043	Plan de Estudios	Ingeniero en Software

Área de Competencia	Competencia del curso
Desarrollar software y servicios de soporte técnico y redes, con la finalidad de solucionar problemas y agilizar procesos en la toma de decisiones en empresas públicas y privadas, bajo estándares de calidad nacional e internacional, a través del análisis de problemas, comunicación, liderazgo e innovación.	Aplicar los medios y protocolos de comunicación en la implementación de una red de datos para enlazar las diferentes áreas de la organización, según la arquitectura TCP/IP y utilizando normas de calidad de organismos internacionales; bajo los principios de ética, trabajo en equipo y una acertada toma de decisiones.

Carga Horaria de la asignatura

Horas Supervisadas			Horas Independientes	Total de Horas
Aula	Laboratorio	Plataforma		
2	1	1	1	5

Consignación del Documento

Unidad Académica	Unidad Académica Hermosillo
Fecha de elaboración	27/06/2025
Responsables del diseño	Jalil Gerardo Espinoza Zepeda jalil.espinoza@ues.mx https://orcid.org/0009-0007-3064-077X Julian Flores Figueroa julian.flores@ues.mx https://orcid.org/0000-0002-4155-8153 Gabriel Garcia Corrales gabriel.garcia@ues.mx
Validación	
Recepción	Coordinación de Procesos Educativos

MATRIZ DE CORRESPONDENCIA

Señalar la relación de cada práctica con las competencias del perfil de egreso del Ingeniero en Software.

PRÁCTICA	PERFIL DE EGRESO
Práctica 1: Introducción al modelo OSI y arquitectura TCP/IP mediante simulación	• Desarrollar soporte y asistencia técnica para la prevención y corrección de problemas en los sistemas de cómputo, • Implementar redes de cómputo enlazando las diferentes áreas de la organización para compartir recursos, bajo los estándares de control de calidad nacional e internacional.
Práctica 2: Implementación y análisis del protocolo IP y utilerías básicas	• Desarrollar soporte y asistencia técnica para la prevención y corrección de problemas en los sistemas de cómputo, • Implementar redes de cómputo enlazando las diferentes áreas de la organización para compartir recursos, bajo los estándares de control de calidad nacional e internacional.
Práctica 3: Fragmentación y reensamblado de paquetes IP	• Desarrollar soporte y asistencia técnica para la prevención y corrección de problemas en los sistemas de cómputo, • Implementar redes de cómputo enlazando las diferentes áreas de la organización para compartir recursos, bajo los estándares de control de calidad nacional e internacional.
Práctica 4: Estructura y configuración del direccionamiento IPv4 e IPv6	• Desarrollar soporte y asistencia técnica para la prevención y corrección de problemas en los sistemas de cómputo, • Implementar redes de cómputo enlazando las diferentes áreas de la organización para compartir recursos, bajo los estándares de control de calidad nacional e internacional.
Práctica 5: Subnetting tradicional y método VLSM	• Desarrollar soporte y asistencia técnica para la prevención y corrección de problemas en los sistemas de cómputo, • Implementar redes de cómputo enlazando las diferentes áreas de la organización para compartir recursos, bajo los estándares

	de control de calidad nacional e internacional.
Práctica 6: Configuración y análisis del encaminamiento CIDR	• Desarrollar soporte y asistencia técnica para la prevención y corrección de problemas en los sistemas de cómputo, • Implementar redes de cómputo enlazando las diferentes áreas de la organización para compartir recursos, bajo los estándares de control de calidad nacional e internacional.
Práctica 7: Análisis y simulación de los protocolos TCP y UDP	• Desarrollar soporte y asistencia técnica para la prevención y corrección de problemas en los sistemas de cómputo, • Implementar redes de cómputo enlazando las diferentes áreas de la organización para compartir recursos, bajo los estándares de control de calidad nacional e internacional.
Práctica 8: Configuración y análisis de redes de conmutación de paquetes	• Desarrollar soporte y asistencia técnica para la prevención y corrección de problemas en los sistemas de cómputo, • Implementar redes de cómputo enlazando las diferentes áreas de la organización para compartir recursos, bajo los estándares de control de calidad nacional e internacional.
Práctica 9: Implementación práctica de protocolos de enrutamiento avanzados (IGP, RIP, OSPF, EGP y BGP)	• Desarrollar soporte y asistencia técnica para la prevención y corrección de problemas en los sistemas de cómputo, • Implementar redes de cómputo enlazando las diferentes áreas de la organización para compartir recursos, bajo los estándares de control de calidad nacional e internacional.

NORMAS DE SEGURIDAD Y BUENAS PRÁCTICAS

Reglamento general del laboratorio

Asistencia y puntualidad

- Se debe ingresar al laboratorio puntualmente según el horario asignado.
- La asistencia será registrada por el docente o responsable técnico.

Comportamiento responsable y respetuoso

- Mantener el orden, respeto y silencio dentro del laboratorio.
- No se permite consumir alimentos ni bebidas.
- Los dispositivos móviles deben estar en modo silencioso o vibrador y su uso solo se permitirá con fines académicos.

Cumplimiento académico

- Cada alumno debe seguir las instrucciones del docente y cumplir con las actividades asignadas dentro del tiempo establecido.
- La práctica debe realizarse de manera individual o en equipo, según se indique.

Salud y ergonomía

- Usar el mobiliario de forma adecuada (sillas, mesas y postura al trabajar frente al equipo).
- Evitar bloqueos de salidas de emergencia o pasillos.

Reglamento de uniforme

Ropa formal adecuada: sin gorras, sandalias, pantalones rotos, pantalones cortos.

Uso adecuado del equipo y materiales

Encendido y apagado correcto del equipo

- Encender y apagar los equipos únicamente bajo indicación del docente.
- Apagar los equipos antes de salir del laboratorio.

Cuidado del equipo de cómputo

- No modificar configuraciones predeterminadas del sistema operativo, software de red ni BIOS.
- No instalar programas sin autorización expresa del docente.
- Evitar conectar o desconectar cables de red o energía sin supervisión.

Manejo responsable de software y simuladores

- Utilizar únicamente el software permitido por la institución, como Cisco Packet Tracer u otros indicados.
- Guardar la información en medios externos personales. El laboratorio no se responsabiliza por archivos no respaldados.

Reportes y fallas

- Reportar inmediatamente cualquier falla de hardware o software al docente o responsable técnico.
- No intentar reparar por cuenta propia ningún dispositivo.

Cuidado del entorno físico

- Mantener el área de trabajo limpia y libre de objetos ajenos a la práctica.
- Al finalizar la sesión, dejar el equipo y mobiliario en el estado y posición original.

Procedimientos en caso de emergencia

Evacuación: Al activarse una alarma de evacuación, seguir las rutas de salida establecidas en orden y sin correr.

Atención a instrucciones: Atender exclusivamente las indicaciones del docente, brigadistas o personal de Protección Civil.

Concentración en puntos de reunión: Reunirse con el grupo en el punto designado y esperar la revisión de lista.

No regresar sin autorización: No volver al laboratorio hasta que la autoridad correspondiente lo autorice.

RELACIÓN DE PRÁCTICAS DE LABORATORIO POR ELEMENTO DE COMPETENCIA

Elemento de Competencia al que pertenece la práctica	**Elementos de competencia 1**
	Describir los mecanismos y protocolos de la capa de internet según la arquitectura TCP/IP para implementarlos en una red de datos dentro de las organizaciones, bajo los principios de ética, trabajo en equipo y una acertada toma de decisiones.

PRÁCTICA	NOMBRE	COMPETENCIA
Práctica No. 1	Introducción al Modelo OSI y Arquitectura TCP/IP mediante simulación	Identificar las capas del modelo OSI y la arquitectura TCP/IP para comprender la estructura de comunicación en redes de datos, mediante la simulación en Cisco Packet Tracer, en un entorno académico controlado, fomentando el trabajo colaborativo y la toma de decisiones informadas.
Práctica No. 2	PRÁCTICA 2: Implementación y análisis del protocolo IP y utilerías básicas	Aplicar el direccionamiento IP y las utilerías básicas como ping, tracert e ipconfig, para verificar la conectividad y funcionalidad en una red TCP/IP, mediante ejercicios prácticos simulados en Cisco Packet Tracer, en escenarios típicos de implementación de redes locales, fomentando la ética profesional y la capacidad analítica para la solución de problemas.
Práctica No. 3	PRÁCTICA 3: Fragmentación y reensamblado de paquetes IP	Analizar el proceso de fragmentación y reensamblado de paquetes IP para asegurar la transmisión eficiente de datos en redes TCP/IP, mediante prácticas guiadas en Cisco Packet Tracer, en situaciones que requieran optimizar el rendimiento de la red frente a limitaciones técnicas, fomentando la precisión técnica y la toma de decisiones bajo criterios éticos.

Elemento de Competencia al que pertenece la práctica	**Elementos de competencia 2**
	Comprender el direccionamiento IP de las capas de red e internet según la arquitectura TCP/IP para implementarlos en una red de datos dentro de las organizaciones, bajo los principios de ética, trabajo en equipo y una acertada toma de decisiones.

PRÁCTICA	NOMBRE	COMPETENCIA
Práctica No. 4	PRÁCTICA 4: Estructura y configuración del direccionamiento IPv4 e IPv6	Identificar la estructura y tipos de direccionamiento IP versión 4 y 6 para aplicar correctamente configuraciones en una red de área local, mediante el uso de Cisco Packet Tracer, en entornos simulados representativos de una organización, fomentando la toma de decisiones éticas y fundamentadas.
Práctica No. 5	PRÁCTICA 5: Subnetting con Máscara de Subred de Longitud Fija (FLSM)	Aplicar técnicas de segmentación de red utilizando subnetting con Máscara de Subred de Longitud Fija (FLSM) para optimizar el uso de direcciones IP en redes organizacionales, mediante simulaciones en Cisco Packet Tracer, promoviendo el pensamiento lógico y la responsabilidad técnica.
Práctica No. 6	PRÁCTICA 6: Subnetting con Máscara de Subred de Longitud Variable (VLSM)	Aplicar técnicas de segmentación de red utilizando subnetting con Máscara de Subred de Longitud Variable (VLSM) para optimizar el uso de direcciones IP en redes organizacionales, utilizando simulaciones en Cisco Packet Tracer, promoviendo el pensamiento crítico y la responsabilidad técnica.

Elemento de Competencia al que pertenece la práctica	**Elementos de competencia 3**
	Implementar una red de datos dentro de una organización, aplicando las normas, mecanismos y protocolos de las capas de transporte e internet que regulan el funcionamiento de una red TPC/IP bajo una acertada toma de decisiones.

PRÁCTICA	NOMBRE	COMPETENCIA
Práctica No. 7	Análisis y simulación de los protocolos TCP y UDP	Comparar el funcionamiento de los protocolos TCP y UDP para seleccionar el más adecuado según las necesidades del servicio en red, mediante la simulación de tráfico en Cisco Packet Tracer, en entornos prácticos de transmisión de datos, promoviendo la toma de decisiones informadas y la ética profesional.
Práctica No. 8	Configuración y análisis de redes de conmutación de paquetes	Implementar una red de conmutación de paquetes para analizar el comportamiento de los algoritmos de encaminamiento, mediante simulaciones en Cisco Packet Tracer, en un entorno de red organizacional simulado, fomentando la toma de decisiones técnicas responsables y el pensamiento crítico.
Práctica No. 9	Implementación práctica de protocolos de enrutamiento avanzados BGP	Configurar y analizar el protocolo de enrutamiento avanzado BGP para garantizar la conectividad entre redes de diferentes sistemas autónomos, utilizando simulaciones en Cisco Packet Tracer, fomentando el pensamiento estratégico, la responsabilidad técnica y la toma de decisiones fundamentadas en redes organizacionales.

UES

Universidad Estatal de Sonora

La Fuerza del Saber Estimulará mi Espíritu

PRÁCTICAS

NOMBRE DE LA PRÁCTICA	PRÁCTICA 1: Introducción al Modelo OSI y Arquitectura TCP/IP mediante simulación
COMPETENCIA DE LA PRÁCTICA	Identificar las capas del modelo OSI y la arquitectura TCP/IP para comprender la estructura de comunicación en redes de datos, mediante la simulación en Cisco Packet Tracer, en un entorno académico controlado, fomentando el trabajo colaborativo y la toma de decisiones informadas.

FUNDAMENTO TÉORICO

El Modelo OSI (Open Systems Interconnection) es un estándar teórico que establece siete capas para describir las comunicaciones en redes: física, enlace de datos, red, transporte, sesión, presentación y aplicación. La Arquitectura TCP/IP, por otro lado, consta de cuatro capas (red, internet, transporte y aplicación), siendo la base de comunicación más utilizada en redes actuales. Comprender ambos modelos permite analizar y diseñar eficientemente las redes informáticas.

MATERIALES, EQUIPAMIENTO Y/O REACTIVOS

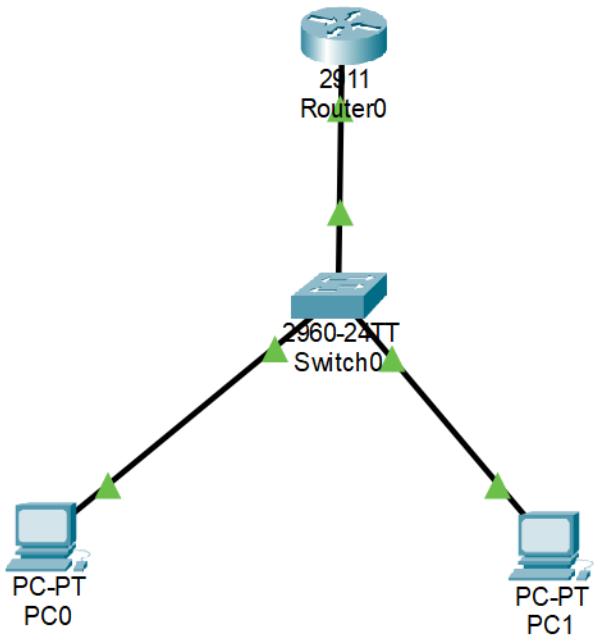
- Software Cisco Packet Tracer (última versión disponible).
- Ordenador con Windows (10, 11), macOS (10.15 o posterior) o Ubuntu (sistema operativo 22.04 LTS), CPU amd64 (x86-64), 4 GB de RAM libre y 1,4 GB de espacio libre en disco.

PROCEDIMIENTO O METODOLOGÍA

1. Abre Cisco Packet Tracer y crea una nueva topología:
    - Dos computadoras (PC0 y PC1)
    - Un Switch (Switch0)
    - Un Router (Router0)
2. Conecta PC0 y PC1 al Switch0, luego conecta el Switch0 al Router0.
3. Configura la interfaz del Router0:
    - Interfaz GigabitEthernet0/0: 192.168.1.1 / Máscara: 255.255.255.0
4. Configura las computadoras con las siguientes direcciones IP estáticas:

Dispositivo	Dirección IP	Máscara Subred	Gateway
PC0	192.168.1.10	255.255.255.0	192.168.1.1
PC1	192.168.1.11	255.255.255.0	192.168.1.1

5. Diseño gráfico de la configuración de los equipos utilizados.



6. Activa el modo de simulación en Cisco Packet Tracer.

7. Realiza pruebas enviando paquetes de un equipo a otro utilizando la función de simulación.

8. Observa detalladamente el proceso de comunicación e identifica las capas del Modelo OSI y la arquitectura TCP/IP involucradas.

9. Registra observaciones sobre la actividad y función específica de cada capa visualizada durante la simulación.

RESULTADOS ESPERADOS

- Diseño de la arquitectura de la red solicitada.
- Registro claro de las capas del modelo OSI y TCP/IP que intervienen en la comunicación simulada.
- Capturas de pantalla mostrando claramente el proceso de envío y recepción de datos entre dispositivos.

ANÁLISIS DE RESULTADOS

- ¿Cuáles son las principales diferencias observadas entre el modelo OSI y la arquitectura TCP/IP en la simulación?
- ¿Qué capas del modelo OSI y TCP/IP fueron visibles explícitamente en Cisco Packet Tracer?
- ¿Qué rol específico desempeñó cada capa durante la transferencia de datos en la práctica?

CONCLUSIONES Y REFLEXIONES

- Conclusión: La práctica permite comprender de manera aplicada cómo los modelos OSI y TCP/IP estructuran la comunicación en redes de datos. Mediante la simulación en Cisco Packet Tracer, fue posible observar cómo un paquete se genera, encapsula, transmite, desencapsula y entrega correctamente entre dos dispositivos a través de una red compuesta por router, switch y computadoras. Se logra identificar las funciones específicas de cada capa involucrada en el proceso de transmisión, validando así el rol de cada dispositivo y protocolo dentro de la arquitectura de red.
- Reflexión: Comprender los modelos OSI y TCP/IP no solo facilita la resolución de problemas técnicos en redes, sino que también fortalece el pensamiento estructurado y lógico al analizar sistemas complejos. Esta práctica fomenta el desarrollo de habilidades clave como la toma de decisiones informadas, la ética en el manejo de información y el trabajo colaborativo. Al visualizar la teoría en acción, se mejora significativamente la comprensión del funcionamiento interno de las redes de comunicación, lo cual es esencial para cualquier profesional en el campo de redes y ciberseguridad.

ACTIVIDADES COMPLEMENTARIAS

- Realiza una simulación adicional incorporando un servidor DHCP y observa cómo afecta a la configuración IP de los dispositivos.

EVALUACIÓN Y EVIDENCIAS DE APRENDIZAJE

Criterios de evaluación	• Claridad y precisión en el registro de resultados. • Correcta identificación y descripción de las capas involucradas. • Participación activa y trabajo colaborativo durante la simulación.

Rúbricas o listas de cotejo para valorar desempeño	• Correcta configuración de la red simulada (30%). • Análisis reflexivo y conclusiones pertinentes (30%). • Rúbrica: Reporte de práctica de laboratorio (40%).

Formatos de reporte de prácticas	• Documento institucional editable de “reporte de prácticas” que contiene:
	  ○ Portada,
	  ○ Introducción
	  ○ Fundamentos teóricos
	  ○ Objetivo de la práctica, hipótesis
	  ○ Expectativa o planteamiento experimental
	  ○ Materiales, equipamiento y/o reactivos
	  ○ Procedimiento o metodología
	  ○ Procesamiento de datos
	  ○ Resultados
	  ○ Análisis y discusión.
	  ○ Conclusiones
	  ○ Bibliografía
	  ○ Anexos

NOMBRE DE LA PRÁCTICA	PRÁCTICA 2: Implementación y análisis del protocolo IP y utilerías básicas
COMPETENCIA DE LA PRÁCTICA	Aplicar el direccionamiento IP y las utilerías básicas como ping, tracert e ipconfig, para verificar la conectividad y funcionalidad en una red TCP/IP, mediante ejercicios prácticos simulados en Cisco Packet Tracer, en escenarios típicos de implementación de redes locales, fomentando la ética profesional y la capacidad analítica para la solución de problemas.

FUNDAMENTO TÉORICO

El Protocolo de Internet (IP) es el responsable de dirigir y enrutar los paquetes de datos entre dispositivos en una red. Junto con las utilerías ping, tracert e ipconfig, se pueden realizar diagnósticos sobre la conectividad, rutas de acceso y configuraciones de red. Estas herramientas permiten verificar el correcto funcionamiento de una red IP, identificar errores de configuración o de comunicación y evaluar el rendimiento de los enlaces.

MATERIALES, EQUIPAMIENTO Y/O REACTIVOS

- Software Cisco Packet Tracer (última versión disponible).
- Ordenador con Windows (10, 11), macOS (10.15 o posterior) o Ubuntu (sistema operativo 22.04 LTS), CPU amd64 (x86-64), 4 GB de RAM libre y 1,4 GB de espacio libre en disco.

PROCEDIMIENTO O METODOLOGÍA

1. Abre la práctica 1 realizada en Cisco Packet Tracer. Donde se tiene un Router y dos PC.
2. Desde cada PC:
    a. Ejecuta el comando ping hacia las otras dos PC y hacia el router.
    b. Usa tracert para comprobar la ruta hacia una de las otras PCs.
    c. Ejecuta ipconfig para visualizar y verificar la configuración IP.
3. Introduce errores intencionales (por ejemplo, cambiar una IP o gateway) y observa el efecto en los resultados de las utilerías.
4. Registra cada observación y corrige los errores identificados.

RESULTADOS ESPERADOS

- Éxito en la comunicación entre dispositivos usando ping
- Visualización de rutas con tracert
- Lectura clara de configuración IP con ipconfig
- Diagnóstico correcto de fallas simples y sus soluciones

ANÁLISIS DE RESULTADOS

- ¿Qué ocurre cuando hay una IP mal configurada?
- ¿Cómo ayuda tracert a identificar problemas de enrutamiento?
- ¿Qué información útil brinda ipconfig para diagnosticar errores?

CONCLUSIONES Y REFLEXIONES

- Conclusión: La práctica permitió aplicar el protocolo IP en un entorno simulado, comprendiendo su funcionamiento y el rol de herramientas esenciales como ping, tracert e ipconfig. Se evidenció la importancia de una configuración correcta para asegurar la conectividad entre dispositivos. Además, el ejercicio fortaleció las habilidades de diagnóstico al identificar y corregir errores de red comunes.
- Reflexión: El dominio del direccionamiento IP y las utilerías de diagnóstico es una competencia básica en redes. Esta práctica proporciona una base sólida para resolver problemas reales, fomenta la autonomía técnica y refuerza el pensamiento lógico al enfrentar fallas de comunicación. Los estudiantes desarrollan no solo habilidades técnicas, sino también actitudes proactivas frente a la resolución de problemas.

ACTIVIDADES COMPLEMENTARIAS

- Agrega un servidor DHCP para asignar IPs dinamicamente a la red y observa los cambios con ipconfig /renew (en modo simulación).

EVALUACIÓN Y EVIDENCIAS DE APRENDIZAJE

Criterios de evaluación	• Comprobación correcta del funcionamiento de la red • Interpretación adecuada de los comandos ejecutados • Solución eficiente de errores intencionados

Rúbricas o listas de cotejo para valorar desempeño	• Correcta configuración IP (10%) • Ejecución y análisis de utilerías (30%) • Diagnóstico y solución de errores (20%) • Rúbrica: Reporte de práctica de laboratorio (40%).

Formatos de reporte de prácticas	• Documento institucional editable de “reporte de prácticas” que contiene:
	  ○ Portada,
	  ○ Introducción
	  ○ Fundamentos teóricos
	  ○ Objetivo de la práctica, hipótesis
	  ○ Expectativa o planteamiento experimental
	  ○ Materiales, equipamiento y/o reactivos
	  ○ Procedimiento o metodología
	  ○ Procesamiento de datos
	  ○ Resultados
	  ○ Análisis y discusión.
	  ○ Conclusiones
	  ○ Bibliografía
	  ○ Anexos

NOMBRE DE LA PRÁCTICA	PRÁCTICA 3: Fragmentación y reensamblado de paquetes IP
COMPETENCIA DE LA PRÁCTICA	Analizar el proceso de fragmentación y reensamblado de paquetes IP para asegurar la transmisión eficiente de datos en redes TCP/IP, mediante prácticas guiadas en Cisco Packet Tracer, en situaciones que requieran optimizar el rendimiento de la red frente a limitaciones técnicas, fomentando la precisión técnica y la toma de decisiones bajo criterios éticos.

FUNDAMENTO TÉORICO

Cuando un paquete IP excede el tamaño máximo permitido por una red (MTU: Unidad Máxima de Transferencia), debe fragmentarse en partes más pequeñas para poder ser transmitido. Cada fragmento contiene un encabezado IP con información que permite al receptor reensamblar los datos correctamente. Esta operación es gestionada por routers y dispositivos de red según los campos del encabezado IP como identificación, offset y flags. Comprender este proceso es fundamental para diagnosticar problemas de rendimiento y asegurar una comunicación efectiva en redes complejas.

MATERIALES, EQUIPAMIENTO Y/O REACTIVOS

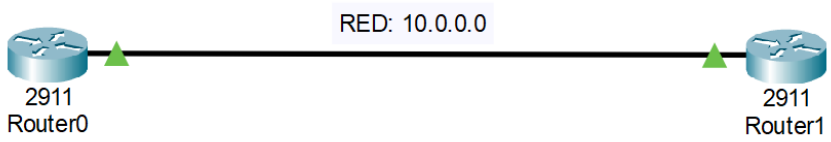
- Software Cisco Packet Tracer (última versión disponible).
- Ordenador con Windows (10, 11), macOS (10.15 o posterior) o Ubuntu (sistema operativo 22.04 LTS), CPU amd64 (x86-64), 4 GB de RAM libre y 1,4 GB de espacio libre en disco.

PROCEDIMIENTO O METODOLOGÍA

1. Diseña en Cisco Packet Tracer una topología de red entre dos dos Router utilizando el ID de red 10.0.0.0.
2. Configura los router en su interface GigabitEthernet 0/0 con las siguientes direcciones IP estáticas:

Interface GigabitEthernet 0/0		
Dispositivo	**Dirección IP**	**Máscara Subred**
Router0	10.0.0.1	255.0.0.0
Router1	10.0.0.2	255.0.0.0

3. El diseño de la red se muestra como se muestra en la siguiente imagen.



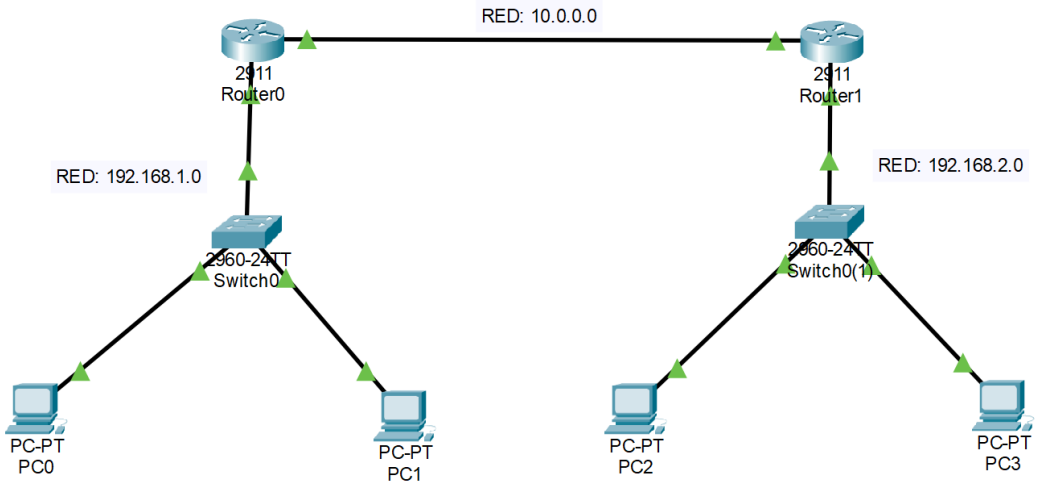
4. Crear una red local en cada Router. Cada red esta constituido por un Switch y dos computadoras. Router0 (PC0 y PC1) y Router1 (PC2 y PC3).

5. Configura las computadoras de ambas redes con las siguientes direcciones IP estáticas:

Route0			
Dispositivo	**Dirección IP**	**Máscara Subred**	**Gateway**
PC0	192.168.1.10	255.255.255.0	192.168.1.1
PC1	192.168.1.11	255.255.255.0	192.168.1.1
Router0	G0/0: 192.168.1.1	255.255.255.0	

Route1			
Dispositivo	**Dirección IP**	**Máscara Subred**	**Gateway**
PC2	192.168.2.10	255.255.255.0	192.168.2.1
PC3	192.168.2.11	255.255.255.0	192.168.2.1
Router1	G0/0: 192.168.2.1	255.255.255.0	

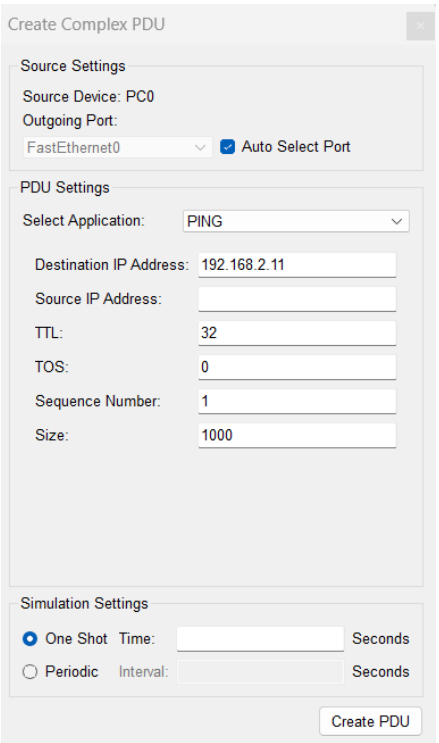
6. La topología de red se vería de la siguiente manera:



7. Cambia la MTU en las interfaces del Router0 y Router1 a un valor bajo (ej. 200 bytes). Sigue las siguientes configuraciones:

```
Router#enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface GigabitEthernet 0/0
Router(config-if)#ip mtu 200
Router(config-if)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console
copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Router#
```

8. Genera tráfico entre las Redes utilizando “Complex PDU” ( ). Por ejemplo, con paquete de la PC0 a la PC3, con tamaño de paquete de 1000 Byte.



9. Observa cómo los routers fragmenta el paquete. Usa el modo de simulación para identificar la división y reensamblado de los fragmentos.
10. Documenta los valores de fragmentación, incluyendo offset, identificación y número de fragmentos.

RESULTADOS ESPERADOS

- Visualización de fragmentación de paquetes en la simulación.
- Identificación de los campos del encabezado IP modificados.
- Confirmación de la entrega correcta del mensaje tras el reensamblado.

ANÁLISIS DE RESULTADOS

- ¿Cuántos fragmentos se generaron a partir del paquete original?
- ¿Qué valores se modificaron en el encabezado IP?
- ¿Cuál es la relación entre el valor MTU y el tamaño del fragmento?

CONCLUSIONES Y REFLEXIONES

- Conclusión: Se comprende de forma aplicada cómo funciona la fragmentación y reensamblado de paquetes IP al superar la MTU, identificando los campos relevantes del encabezado IP y su modificación durante la transmisión. Además, reforzaron habilidades para diagnosticar problemas de rendimiento y aprendieron a optimizar el tráfico de datos en la red, consolidando conocimientos necesarios para el Ingeniero en Software.
- Reflexión: Esta actividad impulsa la capacidad de relacionar teoría con práctica, fomentando el análisis crítico sobre la importancia del protocolo IP en la transmisión confiable de datos y la optimización de redes. Contribuyó a desarrollar competencias de pensamiento lógico, resolución de problemas y toma de decisiones fundamentadas, esenciales para implementar redes bajo estándares de calidad y seguridad en entornos organizacionales.

ACTIVIDADES COMPLEMENTARIAS

- Cambia el valor de MTU y observa cómo varía la cantidad de fragmentos generados.

EVALUACIÓN Y EVIDENCIAS DE APRENDIZAJE

Criterios de evaluación	• Precisión en la observación y análisis de los fragmentos IP • Correcta configuración de los parámetros de red y MTU • Capacidad para interpretar valores técnicos del encabezado IP
Rúbricas o listas de cotejo para valorar desempeño	• Configuración de red funcional (20%) • Análisis detallado de la fragmentación (30%) • Explicación clara y fundamentada del proceso (10%) • Rúbrica: Reporte de práctica de laboratorio (40%)

Formatos de reporte de prácticas	• Documento institucional editable de “reporte de prácticas” que contiene: o Portada, o Introducción o Fundamentos teóricos o Objetivo de la práctica, hipótesis o Expectativa o planteamiento experimental o Materiales, equipamiento y/o reactivos o Procedimiento o metodología o Procesamiento de datos o Resultados o Análisis y discusión. o Conclusiones o Bibliografía o Anexos

NOMBRE DE LA PRÁCTICA	PRÁCTICA 4: Estructura y configuración del direccionamiento IPv4 e IPv6
COMPETENCIA DE LA PRÁCTICA	Identificar la estructura y tipos de direccionamiento IP versión 4 y 6 para aplicar correctamente configuraciones en una red de área local, mediante el uso de Cisco Packet Tracer, en entornos simulados representativos de una organización, fomentando la toma de decisiones éticas y fundamentadas.

FUNDAMENTO TÉORICO

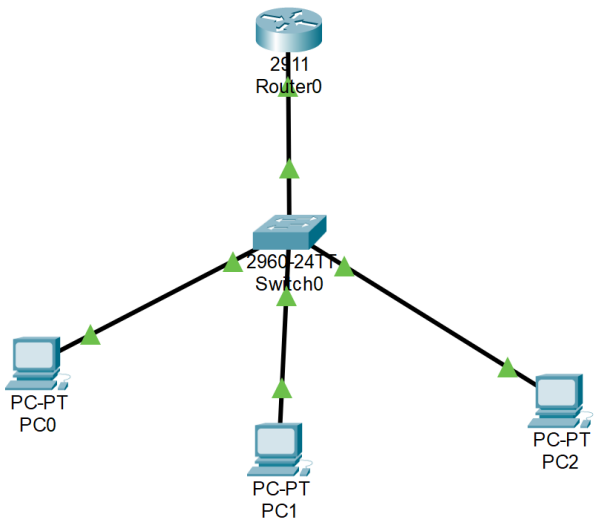
El direccionamiento IP es un componente fundamental en las redes de datos. IPv4 utiliza direcciones de 32 bits, mientras que IPv6 emplea 128 bits para ofrecer mayor capacidad. Entender la estructura, los tipos de direcciones (públicas, privadas, estáticas, dinámicas) y su asignación en una red permite diseñar topologías eficientes. IPv6 introduce nuevas formas de representación y ventajas sobre IPv4, como mayor espacio de direccionamiento y simplificación del encabezado.

MATERIALES, EQUIPAMIENTO Y/O REACTIVOS

- Software Cisco Packet Tracer (última versión disponible).
- Ordenador con Windows (10, 11), macOS (10.15 o posterior) o Ubuntu (sistema operativo 22.04 LTS), CPU amd64 (x86-64), 4 GB de RAM libre y 1,4 GB de espacio libre en disco.

PROCEDIMIENTO O METODOLOGÍA

1. Diseña una red en Cisco Packet Tracer con tres dispositivos finales (PC0, PC1, PC2), un switch (Switch0) y un router (Router0). La topología quedaría como se muestra en la imagen:



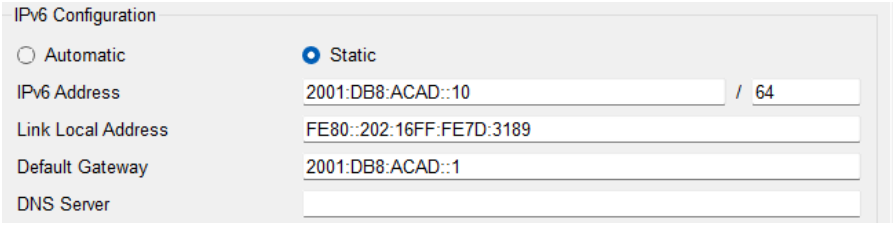
2. Asigna a PC0, PC1 y Router0 con las direcciones IPv4:

Dispositivo	Dirección IPv4	Máscara Subred	Gateway
PC0	192.168.1.10	255.255.255.0	192.168.1.1
PC1	192.168.1.11	255.255.255.0	192.168.1.1
Router0	G0/0: 192.168.1.1	255.255.255.0	

3. Asigna a PC2 y Router0 una dirección IPv6:

Dispositivo	Dirección IPv6	Gateway
PC2	2001:DB8:ACAD::10/64	2001:DB8:ACAD::1
Router0	G0/0: 2001:DB8:ACAD::1/64	

La configuración en PC2 quedaría de la siguiente manera:

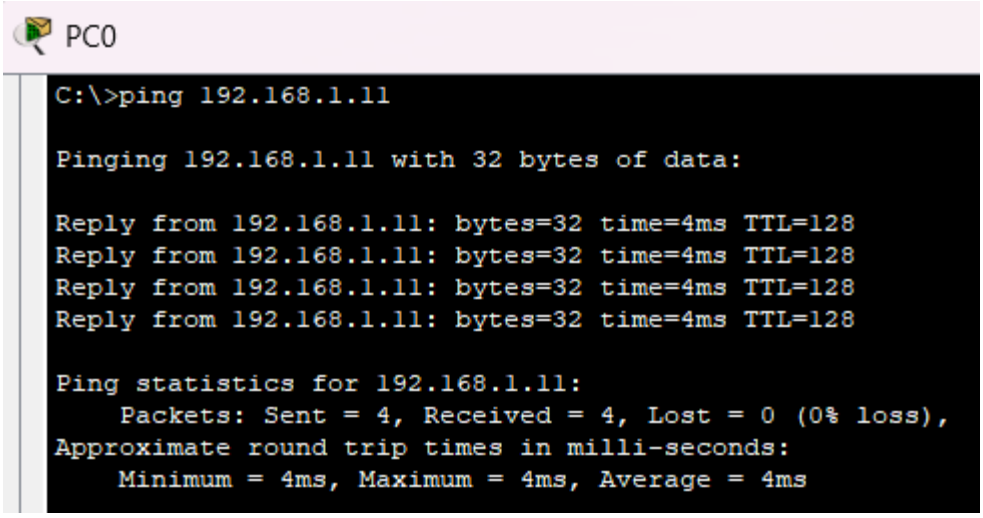


La configuración con dirección IPv6 de la interface GigabitEthernet0/0 del Router0, quedaría de la siguiente manera:

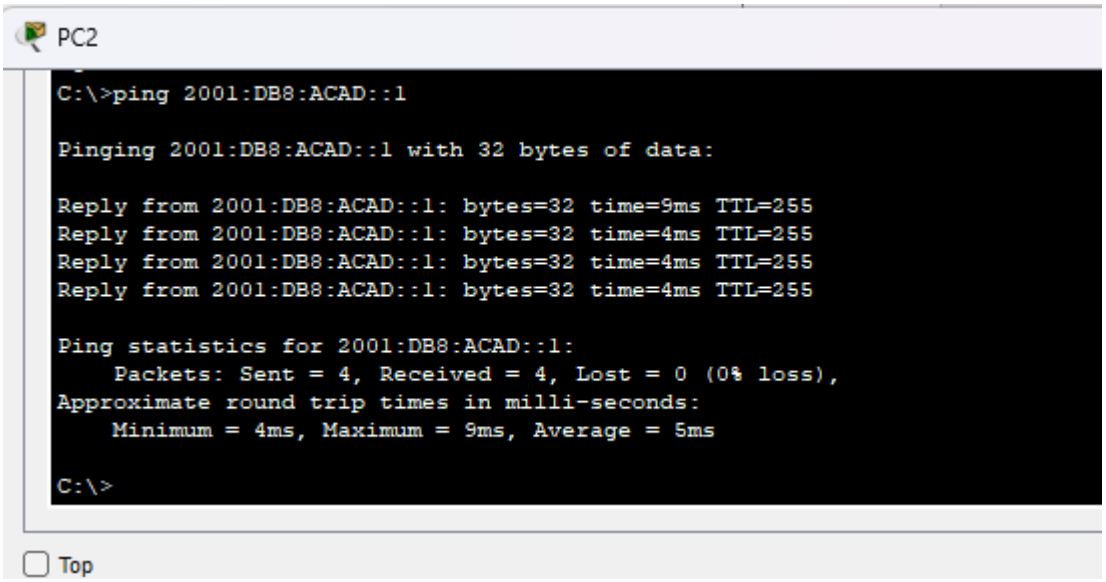
```
Router#show ipv6 interface brief
GigabitEthernet0/0         [up/up]
    FE80::1
    2001:DB8:ACAD::1
```

Nota: Utilizamos el comando "**show ipv6 interface brief"** para observar la configuración actual de las tarjetas de red.

4. Verifica la conectividad entre PC0 y PC1 con ping. (ping 192.168.1.11).



5. Verifica la conectividad entre PC2 y el Router0, usando ping para IPv6 (ping 2001:DB8:ACAD:1::1).



6. Documenta las configuraciones realizadas y realiza capturas de pantalla de la conectividad exitosa.

RESULTADOS ESPERADOS

- Comunicación exitosa entre PC0 y PC1 mediante IPv4.
- Comunicación exitosa entre PC2 y el router mediante IPv6.
- Comprensión de la estructura de ambas versiones del direccionamiento IP.

ANÁLISIS DE RESULTADOS

- ¿Qué diferencias notaste entre las configuraciones IPv4 e IPv6?
- ¿Qué ventajas ofrece IPv6 en términos de escalabilidad y seguridad?
- ¿Cómo verificaste la configuración y conectividad en cada caso?

CONCLUSIONES Y REFLEXIONES

- La práctica permitie a los estudiantes identificar y configurar correctamente direcciones IPv4 e IPv6 en redes locales simuladas, comprendiendo las diferencias de estructura y aplicación entre ambos protocolos. Se logró reforzar el dominio de conceptos de direccionamiento fundamentales para la implementación de redes, fortaleciendo habilidades técnicas que contribuyen al perfil del Ingeniero en Software en la planificación y despliegue de infraestructuras de red eficientes y escalables.
- Esta práctica fomenta la comprensión de la transición tecnológica de IPv4 a IPv6, sensibilizando a los estudiantes sobre la importancia de adaptarse a estándares internacionales y a las necesidades actuales de conectividad. Permite desarrollar competencias de análisis y resolución de problemas en escenarios de direccionamiento real, fortaleciendo la responsabilidad y el pensamiento crítico para la toma de decisiones éticas y fundamentadas en proyectos de redes dentro de las organizaciones.

ACTIVIDADES COMPLEMENTARIAS

- Agrega un servidor DHCPv6 y configura PC2 para obtener su dirección IPv6 automáticamente.

EVALUACIÓN Y EVIDENCIAS DE APRENDIZAJE	
Criterios de evaluación	• Precisión en la asignación de direcciones IP y configuración de gateway • Verificación funcional de conectividad en ambos protocolos • Documentación clara y detallada del procedimiento y resultados
Rúbricas o listas de cotejo para valorar desempeño	• Configuración funcional de IPv4 (30%) • Configuración funcional de IPv6 (30%) • Rúbrica: Reporte de práctica de laboratorio (40%).
Formatos de reporte de prácticas	• Documento institucional editable de “reporte de prácticas” que contiene: o Portada, o Introducción o Fundamentos teóricos o Objetivo de la práctica, hipótesis o Expectativa o planteamiento experimental o Materiales, equipamiento y/o reactivos o Procedimiento o metodología o Procesamiento de datos o Resultados o Análisis y discusión. o Conclusiones o Bibliografía o Anexos

NOMBRE DE LA PRÁCTICA	PRÁCTICA 5: Subnetting con Máscara de Subred de Longitud Fija (FLSM)
COMPETENCIA DE LA PRÁCTICA	Aplicar técnicas de segmentación de red utilizando subnetting con Máscara de Subred de Longitud Fija (FLSM) para optimizar el uso de direcciones IP en redes organizacionales, mediante simulaciones en Cisco Packet Tracer, promoviendo el pensamiento lógico y la responsabilidad técnica.

FUNDAMENTO TÉORICO

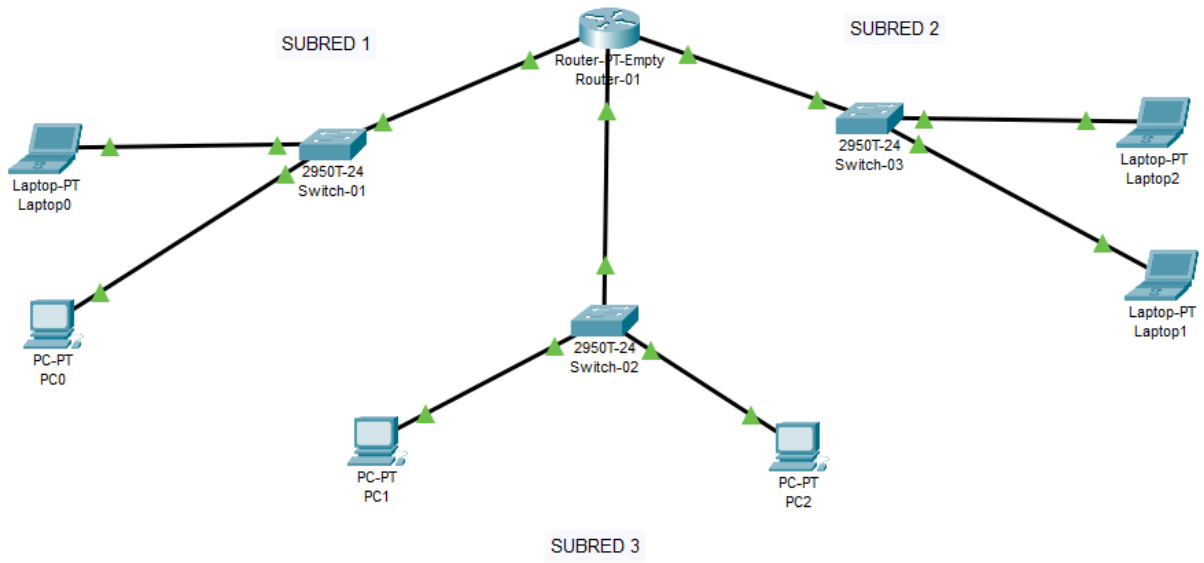
El FLSM (Fixed Length Subnet Mask) permite dividir una red en subredes iguales utilizando la misma máscara de subred, facilitando la organización y gestión de las direcciones IP y simplificando el cálculo de subredes en redes de tamaño uniforme.

MATERIALES, EQUIPAMIENTO Y/O REACTIVOS

- Software Cisco Packet Tracer (última versión disponible).
- Ordenador con Windows (10, 11), macOS (10.15 o posterior) o Ubuntu (sistema operativo 22.04 LTS), CPU amd64 (x86-64), 4 GB de RAM libre y 1,4 GB de espacio libre en disco.

PROCEDIMIENTO O METODOLOGÍA

1. Diseñar en Cisco Packet Tracer una topología de red con un router, tres switch y mínimo dos PCs o Laptops por cada subred. La topología quedaría similar a como se observa en la imagen siguiente:



2. Para el diseño de la topología de red, se desea tener como máximo 50 equipos (PCs y Laptops) en cada subred. En base a las subredes y equipos que se necesitan indicar los bits prestados para crear mínimo tres subredes y tener máximo 50 host en cada subred. utiliza la técnica FLSM (Fixed Length Subnet Mask) y como red base la “192.168.1.0/24”.

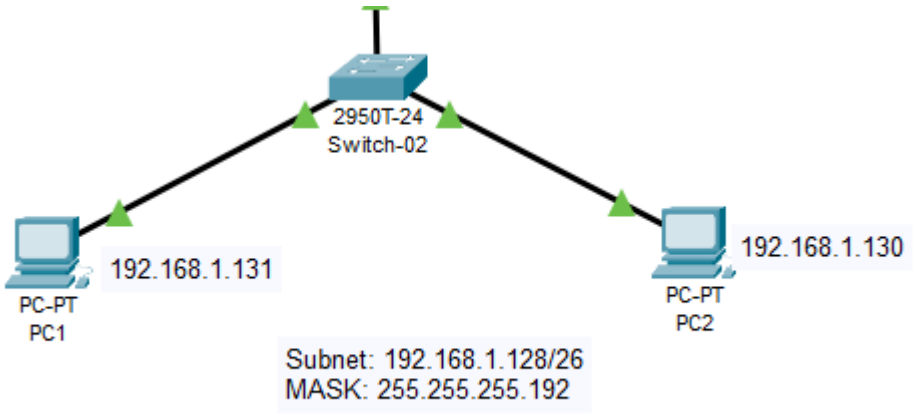
3. Realiza una tabla donde se indique el número de direcciones IP que se tienen para host por cada subred, identificador IP de subred, máscara de subred, primera IP de host, ultima IP de host e IP de broadcast por cada subred.

No.	No. host	Id de red	Máscara de subred	Primera IP	Ultima IP	Broadcast

4. En Packet Tracert Configurar cada interface del router con la primera dirección IP de cada subred.

5. Configurar las PCs y Laptops con las direcciones IP correspondientes, máscaras de subred y gateway.

6. En Packet Tracert agregar notas que contenga las direcciones IPs de los identificadores de subredes y numero de bits para definir la máscara de subred. Ejemplo:



7. Probar la conectividad entre dispositivos con el comando ping.

8. Documentar capturas de pantalla de las configuraciones y resultados.

RESULTADOS ESPERADOS

- Aplicación correcta del subnetting utilizando FLSM.
- Verificación de conectividad entre dispositivos.
- Comprensión del cálculo y asignación de subredes con FLSM.

ANÁLISIS DE RESULTADOS

- ¿Cómo se calculan las subredes utilizando FLSM?
- ¿Qué ventajas tiene utilizar subnetting FLSM?
- ¿Qué problemas se presentaron durante la práctica y cómo se resolvieron?

CONCLUSIONES Y REFLEXIONES

- Conclusión: La práctica permite a los estudiantes comprender y aplicar el subnetting con FLSM de manera efectiva, logrando distribuir de forma ordenada las direcciones IP en redes organizacionales. Se reforzaron competencias de cálculo, planeación y configuración de redes, esenciales para el perfil del Ingeniero en Software.
- Esta práctica fomenta el análisis lógico y el orden en la segmentación de redes, contribuyendo al desarrollo de habilidades técnicas y de resolución de problemas en infraestructura de redes. Permite que los estudiantes comprendan la importancia de la planificación adecuada de direcciones IP para el funcionamiento eficiente de las redes organizacionales.

ACTIVIDADES COMPLEMENTARIAS

- Realizar ejercicios de cálculo de subredes con FLSM en diferentes escenarios.
- Simular una red con diferentes segmentos utilizando FLSM y verificar el uso de las direcciones IP.

EVALUACIÓN Y EVIDENCIAS DE APRENDIZAJE	
Criterios de evaluación	• Aplicación correcta de cálculos de FLSM • Configuración funcional de subredes en la simulación • Análisis reflexivo sobre el proceso y resultados
Rúbricas o listas de cotejo para valorar desempeño	• Aplicación correcta de cálculos de FLSM (30%). • Configuración funcional de subredes en la simulación (30%). • Rúbrica: Reporte de práctica de laboratorio (40%).

Formatos de reporte de prácticas	• Documento institucional editable de “reporte de prácticas” que contiene:
	  ○ Portada,
	  ○ Introducción
	  ○ Fundamentos teóricos
	  ○ Objetivo de la práctica, hipótesis
	  ○ Expectativa o planteamiento experimental
	  ○ Materiales, equipamiento y/o reactivos
	  ○ Procedimiento o metodología
	  ○ Procesamiento de datos
	  ○ Resultados
	  ○ Análisis y discusión.
	  ○ Conclusiones
	  ○ Bibliografía
	  ○ Anexos

NOMBRE DE LA PRÁCTICA	PRÁCTICA 6: Subnetting con Máscara de Subred de Longitud Variable (VLSM)
COMPETENCIA DE LA PRÁCTICA	Aplicar técnicas de segmentación de red utilizando subnetting con Máscara de Subred de Longitud Variable (VLSM) para optimizar el uso de direcciones IP en redes organizacionales, utilizando simulaciones en Cisco Packet Tracer, promoviendo el pensamiento crítico y la responsabilidad técnica.

FUNDAMENTO TÉORICO

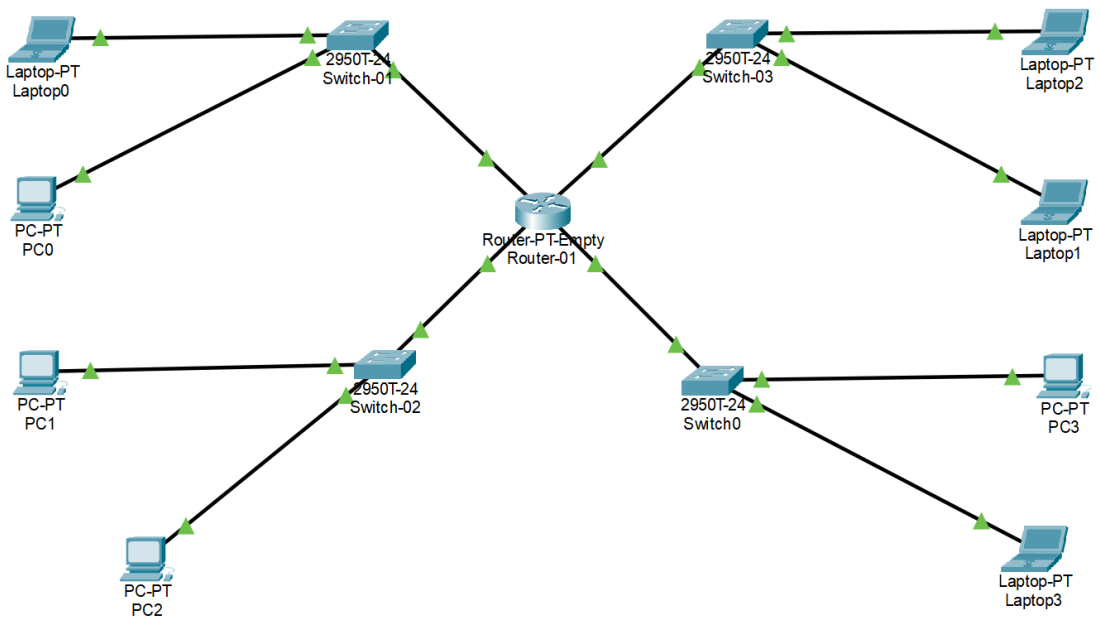
VLSM (Variable Length Subnet Mask) permite utilizar máscaras de subred de diferentes tamaños dentro de una misma red principal, asignando la cantidad exacta de direcciones IP necesarias por subred y optimizando el uso del espacio de direccionamiento, facilitando la planificación eficiente de redes escalables.

MATERIALES, EQUIPAMIENTO Y/O REACTIVOS

- Software Cisco Packet Tracer (última versión disponible).
- Ordenador con Windows (10, 11), macOS (10.15 o posterior) o Ubuntu (sistema operativo 22.04 LTS), CPU amd64 (x86-64), 4 GB de RAM libre y 1,4 GB de espacio libre en disco.

PROCEDIMIENTO O METODOLOGÍA

1. Diseñar en Cisco Packet Tracer una topología de red con un router, cuatro switch y mínimo dos PCs o Laptops por cada subred. La topología quedaría similar a como se observa en la imagen siguiente:



2. Utilizando la técnica de VLSM (Máscara de Subred de Longitud Variable), calcular número de host, Id de red, máscara de subred, prefijo de la máscara de red, primera IP, ultima IP y la dirección IP de broadcast por cada subred necesaria.

   Para la realización del cálculo se proporciona la siguiente red IP 192.168.1.0/24, la cual se quiere que se divida en subredes, una para cada red de la topología creada en cisco packet tracert. Los requerimientos de nodos por cada red son los siguientes:

   Red 1 → 60 nodos

   Red 2 → 120 nodos

   Red 3 → 10 nodos

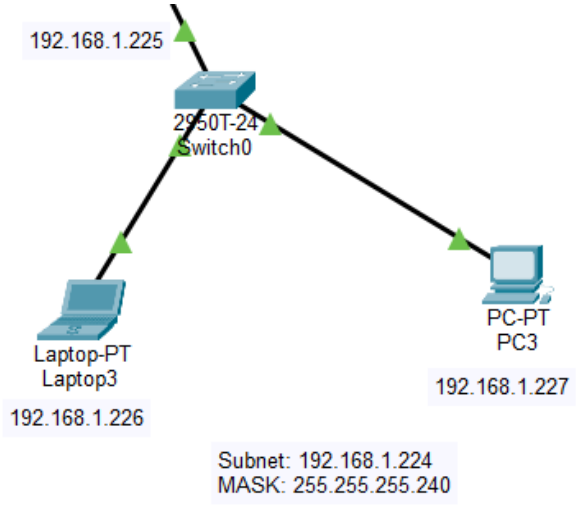
   Red 4 → 24 nodos

   Los resultados del cálculo colocarlos en la siguiente tabla en orden del número de nodos de mayor a menor.

No.	No. host	Id de red	Prefijo	Máscara de subred	Primera IP	Ultima IP	Broadcast

3. En Packet Tracert Configurar cada interface del router con la primera dirección IP de cada subred, anteriormente calculado.
4. Configurar cada PC con su dirección IP, máscara y gateway según la subred asignada.
5. Verificar la conectividad entre los dispositivos de las diferentes subredes mediante ping.

6. En Packet Tracert agregar notas que contenga las direcciones IPs de los identificadores de subredes y numero de bits para definir la máscara de subred. Ejemplo:



7. Documentar capturas de pantalla de las configuraciones y resultados.

RESULTADOS ESPERADOS

- Aplicación correcta del VLSM en la segmentación de redes.
- Conectividad funcional entre las PCs en la simulación.
- Comprensión del uso y cálculo de VLSM para optimizar el direccionamiento IP.

ANÁLISIS DE RESULTADOS

- ¿Cómo se calculó la máscara de subred para cada segmento utilizando VLSM?
- ¿Qué ventajas observaste de VLSM frente a FLSM?
- ¿Qué dificultades surgieron durante la práctica y cómo se solucionaron?

CONCLUSIONES Y REFLEXIONES
Conclusión: La práctica permitie que los estudiantes apliquen correctamente VLSM en redes simuladas, logrando optimizar el espacio de direccionamiento y adaptándose a las necesidades de cada subred. Se fortalece las competencias técnicas relevantes para el diseño y planeación de redes organizacionales. Reflexión: Esta práctica fomenta la toma de decisiones técnicas basadas en un análisis responsable, permitiendo a los estudiantes valorar la importancia de planificar de forma eficiente las direcciones IP en redes de datos y comprender el valor del uso de VLSM en proyectos de infraestructura de red escalables.

ACTIVIDADES COMPLEMENTARIAS
• Realizar ejercicios de VLSM en diferentes escenarios de redes. • Simular en Cisco Packet Tracer una red organizacional aplicando VLSM y verificar el aprovechamiento de las direcciones IP.

EVALUACIÓN Y EVIDENCIAS DE APRENDIZAJE	
Criterios de evaluación	• Cálculo correcto de las subredes con VLSM • Configuración adecuada en la simulación de Packet Tracer • Análisis reflexivo de la práctica • Reporte de práctica de laboratorio
Rúbricas o listas de cotejo para valorar desempeño	• Cálculo correcto de las subredes con VLSM (30%). • Configuración adecuada en la simulación de Packet Tracer (30%). • Rúbrica: Reporte de práctica de laboratorio (40%).

Formatos de reporte de prácticas	• Documento institucional editable de “reporte de prácticas” que contiene: o Portada, o Introducción o Fundamentos teóricos o Objetivo de la práctica, hipótesis o Expectativa o planteamiento experimental o Materiales, equipamiento y/o reactivos o Procedimiento o metodología o Procesamiento de datos o Resultados o Análisis y discusión. o Conclusiones o Bibliografía o Anexos

NOMBRE DE LA PRÁCTICA	PRÁCTICA 7: Análisis y simulación de los protocolos TCP y UDP
COMPETENCIA DE LA PRÁCTICA	Comparar el funcionamiento de los protocolos TCP y UDP para seleccionar el más adecuado según las necesidades del servicio en red, mediante la simulación de tráfico en Cisco Packet Tracer, en entornos prácticos de transmisión de datos, promoviendo la toma de decisiones informadas y la ética profesional.

FUNDAMENTO TÉORICO

TCP (Transmission Control Protocol) es un protocolo orientado a la conexión que garantiza la entrega ordenada y confiable de los datos, mientras que UDP (User Datagram Protocol) es un protocolo no orientado a la conexión que permite una transmisión más rápida, pero sin garantía de entrega. Comprender ambos protocolos es esencial para decidir cuál emplear según el tipo de servicio y las necesidades de red.

MATERIALES, EQUIPAMIENTO Y/O REACTIVOS

- Software Cisco Packet Tracer (última versión disponible).
- Ordenador con Windows (10, 11), macOS (10.15 o posterior) o Ubuntu (sistema operativo 22.04 LTS), CPU amd64 (x86-64), 4 GB de RAM libre y 1,4 GB de espacio libre en disco.

PROCEDIMIENTO O METODOLOGÍA

1. Abrir Cisco Packet Tracer y crear una topología de red: incluir un router, un switch, al menos cuatro equipos de cómputo (PCs, Laptop) un servidor DHCP, un servidor DNS y un servidor web conectados al switch.
2. Datos de la red:
    - ID de red: 192.168.100.0
    - Máscara de Subred: 255.255.255.0
    - Gateway: 192.168.100.1
    - IP DNS: 192.168.100.2
    - IP DHCP: 192.168.100.254
3. Configurar el router:
    - Asignar la IP 192.168.100.1/24 a la interfaz del router, el cual es nuestro Gateway de red.

4. Configurar el servidor DHCP: A

    - Asignar la IP estática 192.168.100.254/24.
    - Crear un pool en el servicio de DHCP con el rango de direcciones (192.168.100.10 - 192.168.100.100), máscara 255.255.255.0, gateway 192.168.100.1 y DNS 192.168.100.2.

5. Configurar el servidor DNS.

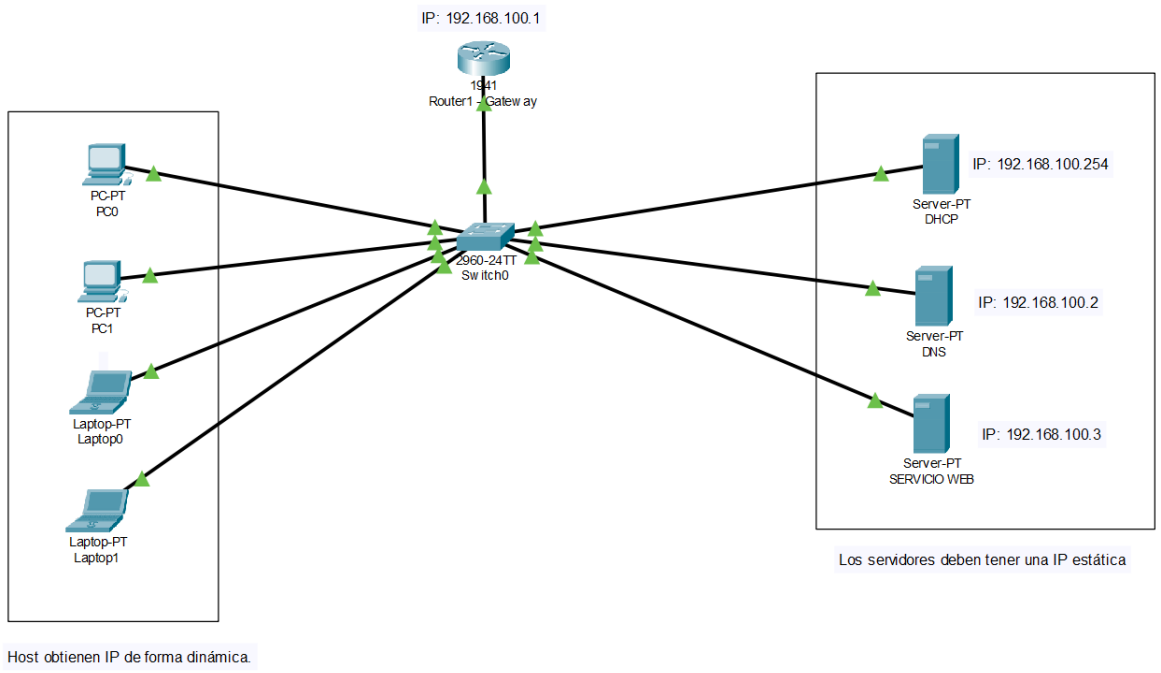
    - Asignar la IP estática 192.168.100.2/24.
    - Crear registros para “www.ues.mx” apuntando a la IP del servidor web. Ejemplo:

6. Configurar el servidor web:

    - Asignar IP estática dentro del rango (por ejemplo, 192.168.100.3/24).
    - Activar servicio HTTP y subir una página de prueba con texto de identificación de la práctica.

7. Configurar las PCs:
    - Configurar para obtener IP mediante DHCP y verificar la correcta asignación de IP, máscara, gateway y DNS.

8. El diseño de la topología de red quedaría de la siguiente manera:

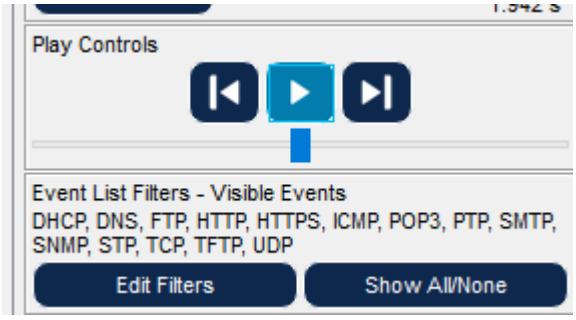


Los cables utilizados para las conexiones: straight-Through.

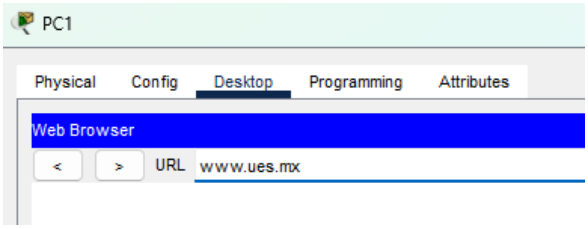
9. Verificar conectividad:
    - Realizar ping desde las PCs al router, al servidor web y al servidor DNS.

10. Probar acceso a servicios:
    - Navegar en las PCs a www.ues.mx para probar tráfico HTTP (TCP)

11. Activar modo de simulación en cisco packet tracert para probar los protocolos TCP y UDP y realiza los siguientes procedimientos:
    - Desactiva en una de las PCs el servicio DHCP para quitar la IP asignada y estando en modo simulación volvemos activar el servicio. Para que la PC y el servidor se comuniquen debemos tener visibles los eventos DHCP, DNS, TCP y UDP y a continuación dar clic en PLAY del modo simulación.



    - Navegar en las PCs a www.ues.mx para probar tráfico HTTP (TCP). Para que la PC y el servidor se comuniquen debemos tener visibles los eventos DHCP, DNS, HTTP, TCP y UDP y a continuación dar clic en PLAY del modo simulación.



    - Desde una PC, utilizar el comando nslookup www.ues.mx para verificar el funcionamiento del protocolo UDP. Dar clic en play para que la simulación comience.

12. Registrar capturas de pantalla de configuraciones, pruebas de conectividad, tráfico simulado y acceso a los servicios como evidencia de la práctica.

RESULTADOS ESPERADOS

- Identificación clara de las diferencias entre TCP y UDP.
- Comprensión del comportamiento de cada protocolo en función de las necesidades del servicio.
- Análisis de las ventajas y desventajas de ambos protocolos en redes simuladas.

ANÁLISIS DE RESULTADOS

- Identificación clara de las diferencias entre TCP y UDP.
- Comprensión del comportamiento de cada protocolo en función de las necesidades del servicio.
- Análisis de las ventajas y desventajas de ambos protocolos en redes simuladas.

CONCLUSIONES Y REFLEXIONES

Conclusión: La práctica permite a los estudiantes comprender y comparar de manera aplicada los protocolos TCP y UDP, analizando sus diferencias en confiabilidad, velocidad de transmisión y control de flujo. Los estudiantes reforzaron habilidades para elegir de manera fundamentada el protocolo adecuado según el tipo de servicio y las necesidades de la red, fortaleciendo su capacidad técnica como Ingenieros en Software.

Reflexión: Esta práctica contribuye a la formación de un criterio técnico en la toma de decisiones para la implementación de redes y aplicaciones, sensibilizando a los estudiantes sobre la importancia de comprender el funcionamiento de los protocolos de transporte en el diseño de soluciones eficientes. Promueve la responsabilidad y la ética profesional al tomar decisiones que impactan en el rendimiento y la calidad de servicio en redes de comunicación.

ACTIVIDADES COMPLEMENTARIAS

- Realizar pruebas de conectividad con ping y tracert para verificar el comportamiento de los paquetes en rutas diferentes dentro de la red configurada.
- Investigar y documentar ejemplos de aplicaciones que utilizan protocolos TCP y UDP, indicando cuál es más conveniente según el tipo de servicio.
- Configurar un servicio adicional de correo electrónico (SMTP/POP3) o Servicio FTP en Packet Tracer y observar el tráfico TCP generado.

EVALUACIÓN Y EVIDENCIAS DE APRENDIZAJE	
Criterios de evaluación	• Configuración funcional de la red • Verificación y pruebas de conectividad • Pruebas y análisis de protocolos TCP y UDP • Reporte de práctica de laboratorio
Rúbricas o listas de cotejo para valorar desempeño	• Configuración funcional de la red (20%) • Verificación y pruebas de conectividad (20%) • Pruebas y análisis de protocolos TCP y UDP (20%) • Rúbrica: Reporte de práctica de laboratorio (40%).

Formatos de reporte de prácticas	• Documento institucional editable de “reporte de prácticas” que contiene:
	  ○ Portada,
	  ○ Introducción
	  ○ Fundamentos teóricos
	  ○ Objetivo de la práctica, hipótesis
	  ○ Expectativa o planteamiento experimental
	  ○ Materiales, equipamiento y/o reactivos
	  ○ Procedimiento o metodología
	  ○ Procesamiento de datos
	  ○ Resultados
	  ○ Análisis y discusión.
	  ○ Conclusiones
	  ○ Bibliografía
	  ○ Anexos

NOMBRE DE LA PRÁCTICA	PRÁCTICA 8: Configuración y análisis de redes de conmutación de paquetes
COMPETENCIA DE LA PRÁCTICA	Implementar una red de conmutación de paquetes para analizar el comportamiento de los algoritmos de encaminamiento, mediante simulaciones en Cisco Packet Tracer, en un entorno de red organizacional simulado, fomentando la toma de decisiones técnicas responsables y el pensamiento crítico.

FUNDAMENTO TÉORICO

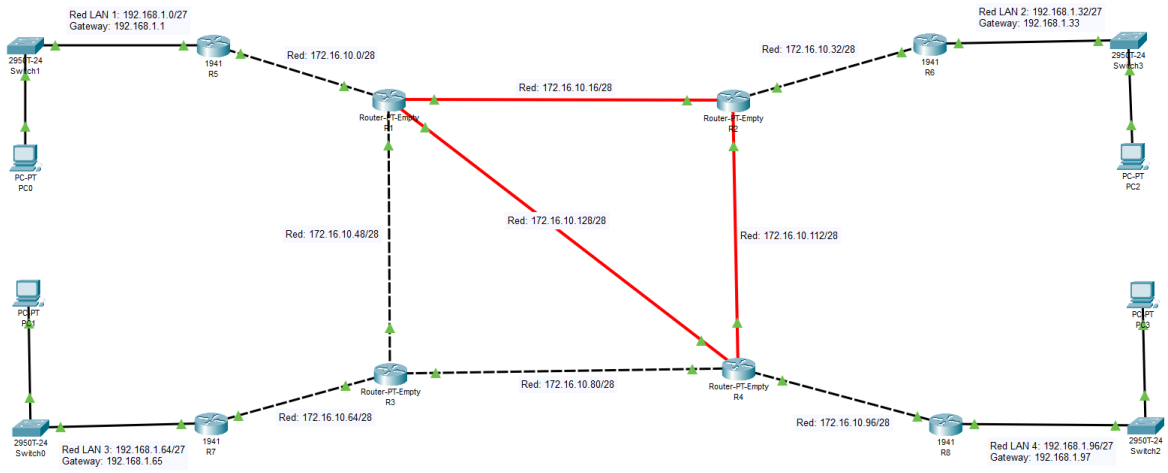
La conmutación de paquetes es una técnica de transmisión de datos en redes que permite dividir la información en pequeños paquetes que se envían de forma independiente, utilizando los recursos de red de manera eficiente. Los algoritmos de encaminamiento permiten determinar las rutas óptimas que siguen estos paquetes dentro de la red, garantizando su llegada al destino con eficiencia y evitando la congestión.

MATERIALES, EQUIPAMIENTO Y/O REACTIVOS

- Software Cisco Packet Tracer (última versión disponible).
- Ordenador con Windows (10, 11), macOS (10.15 o posterior) o Ubuntu (sistema operativo 22.04 LTS), CPU amd64 (x86-64), 4 GB de RAM libre y 1,4 GB de espacio libre en disco.
- Calculadora de subredes (ejemplo: ManageEngine).

PROCEDIMIENTO O METODOLOGÍA

1. Crear una topología en Cisco Packet Tracer con ocho routers interconectados, cada uno con un switch y una PC, simulando distintas áreas de una organización. El diseño de la topología de red es como se muestra en la siguiente imagen:



Los cables utilizados son: straight-through, cross-over y serial DTE

2. Configurar direccionamiento IP en cada red LAN, siendo estas subredes del bloque de direcciones 192.168.1.0/24 con la máscara de subred 255.255.255.0/24. A partir de la dirección de red y mascara de red vamos a crear subredes.

   - La máscara de subred a utilizar para cada subred es 255.255.255.224/27 y la Notación CIDR es 192.168.1.0/27. Se entiende que se piden tres bits prestados a la proporción de los hosts para tener 8 número de subredes y 32 números de host por subred. En la siguiente tabla se muestra la información completa de las direcciones IPs que se pueden utilizar:

Subred ID	Dirección de subred	Rango de IPs para host	Broadcast
1	192.168.1.0	192.168.1.1 - 192.168.1.30	192.168.1.31
2	192.168.1.32	192.168.1.33 - 192.168.1.62	192.168.1.63
3	192.168.1.64	192.168.1.65 - 192.168.1.94	192.168.1.95
4	192.168.1.96	192.168.1.97 - 192.168.1.126	192.168.1.127
5	192.168.1.128	192.168.1.129 - 192.168.1.158	192.168.1.159
6	192.168.1.160	192.168.1.161 - 192.168.1.190	192.168.1.191
7	192.168.1.192	192.168.1.193 - 192.168.1.222	192.168.1.223
8	192.168.1.224	192.168.1.225 - 192.168.1.254	192.168.1.255

3. Configurar direccionamiento IP entre las interconexiones en cada interfaz de los routers. La IP proporcionada para configuración de la conexión entre router es: 172.16.10.0/24 y la máscara de subred 255.255.255.0.

- La máscara de subred a utilizar para cada conexión es 255.255.255.240/28 y la Notación CIDR es 172.16.10.0/28. Se entiende que se piden tres bits prestados a la proporción de los hosts para tener 16 número de subredes y 16 números de host por subred. En la siguiente tabla se muestra la IPs de las primeras 10 subredes de 16 que se pueden utilizar en las interfaces que interconectan los routers:

Subred ID	Dirección de subred	Rango de IPs para host	Broadcast
1	172.16.10.0	172.16.10.1 - 172.16.10.14	172.16.10.15
2	172.16.10.16	172.16.10.17 - 172.16.10.30	172.16.10.31
3	172.16.10.32	172.16.10.33 - 172.16.10.46	172.16.10.47
4	172.16.10.48	172.16.10.49 - 172.16.10.62	172.16.10.63
5	172.16.10.64	172.16.10.65 - 172.16.10.78	172.16.10.79
6	172.16.10.80	172.16.10.81 - 172.16.10.94	172.16.10.95
7	172.16.10.96	172.16.10.97 - 172.16.10.110	172.16.10.111
8	172.16.10.112	172.16.10.113 - 172.16.10.126	172.16.10.127
9	172.16.10.128	172.16.10.129 - 172.16.10.142	172.16.10.143
10	172.16.10.144	172.16.10.145 - 172.16.10.158	172.16.10.159

4. Utilizando la terminal de configuración de cada router configura los protocolos de enrutamiento dinámico (RIPv2 o OSPF) para observar el comportamiento de los algoritmos de encaminamiento en la red. Ejemplo con RIPv2:

    a) Habilitar RIP v2 en el Router 5 (R5):

    Router(config)# router rip
    Router(config-router)# version 2
    Router(config-router)# no auto-summary
    Router(config-router)# network 192.168.1.0
    Router(config-router)# network 172.16.10.0

    Realizar las mismas configuraciones en cada router de la topología de red.

    b) Verificar la configuración:

    Router# show ip route
    Router# show ip protocols

5. Generar tráfico de datos entre las PCs utilizando ping y tracert para ver la ruta de los paquetes.
6. Activar el modo de simulación para observar la fragmentación, el encaminamiento de los paquetes y el comportamiento de la red bajo tráfico simulado.
7. Visualizar y analizar las rutas utilizadas por los paquetes y el funcionamiento de los algoritmos de enrutamiento.
8. Documentar capturas de pantalla de las configuraciones, pruebas de conectividad y simulaciones realizadas.

RESULTADOS ESPERADOS

- Crear una topología en Cisco Packet Tracer con al menos ocho routers interconectados, cada uno con un switch y una PC, simulando distintas áreas de una organización.
- Configurar direccionamiento IP en cada red y en cada interfaz de los routers.

- Configurar protocolos de enrutamiento dinámico (RIP o OSPF) para observar el comportamiento de los algoritmos de encaminamiento en la red.
- Generar tráfico de datos entre las PCs utilizando ping y transferencia de archivos para simular carga de red.
- Activar el modo de simulación para observar la fragmentación, el encaminamiento de los paquetes y el comportamiento de la red bajo tráfico simulado.
- Visualizar y analizar las rutas utilizadas por los paquetes y el funcionamiento de los algoritmos de enrutamiento.
- Documentar capturas de pantalla de las configuraciones, pruebas de conectividad y simulaciones realizadas.

ANÁLISIS DE RESULTADOS

- Crear una topología en Cisco Packet Tracer con al menos tres routers interconectados, cada uno con un switch y dos PCs, simulando distintas áreas de una organización.
- Configurar direccionamiento IP en cada red y en cada interfaz de los routers.
- Configurar el protocolo de enrutamiento dinámico (RIP o OSPF) para observar el comportamiento de los algoritmos de encaminamiento en la red.
- Generar tráfico de datos entre las PCs utilizando ping y transferencia de archivos para simular carga de red.
- Activar el modo de simulación para observar la fragmentación, el encaminamiento de los paquetes y el comportamiento de la red bajo tráfico simulado.
- Visualizar y analizar las rutas utilizadas por los paquetes y el funcionamiento de los algoritmos de enrutamiento.
- Documentar capturas de pantalla de las configuraciones, pruebas de conectividad y simulaciones realizadas.

CONCLUSIONES Y REFLEXIONES

Conclusión: La práctica permite a los estudiantes comprender la importancia de la conmutación de

paquetes y los algoritmos de encaminamiento en redes, facilitando el análisis de rutas y el aprovechamiento de los recursos de red para el envío eficiente de datos. Se reforzaron competencias de configuración, planeación y análisis en entornos de simulación de redes.
Reflexión: Esta práctica fomenta la toma de decisiones fundamentadas y el pensamiento crítico en los estudiantes, permitiéndoles identificar el funcionamiento interno de una red de conmutación de paquetes, así como la importancia de la configuración y elección de protocolos de enrutamiento para mantener el rendimiento y la eficiencia en redes de datos organizacionales.

ACTIVIDADES COMPLEMENTARIAS

- Investigar y comparar las características de RIP y OSPF en redes de conmutación de paquetes.
- Configurar una red adicional utilizando EIGRP y comparar su funcionamiento con OSPF y RIP.

EVALUACIÓN Y EVIDENCIAS DE APRENDIZAJE

Criterios de evaluación	• Configuración correcta de la topología de red y protocolos de enrutamiento. • Análisis y visualización del tráfico de red en simulación. • Reporte de práctica de laboratorio.
Rúbricas o listas de cotejo para valorar desempeño	• Configuración correcta de la topología de red y protocolos de enrutamiento (40%). • Análisis y visualización del tráfico de red en simulación (20%). • Rúbrica: Reporte de práctica de laboratorio (40%).

Formatos de reporte de prácticas	• Documento institucional editable de “reporte de prácticas” que contiene: o Portada, o Introducción o Fundamentos teóricos o Objetivo de la práctica, hipótesis o Expectativa o planteamiento experimental o Materiales, equipamiento y/o reactivos o Procedimiento o metodología o Procesamiento de datos o Resultados o Análisis y discusión. o Conclusiones o Bibliografía o Anexos

NOMBRE DE LA PRÁCTICA	PRÁCTICA 9: Implementación práctica de protocolos de enrutamiento avanzados BGP
COMPETENCIA DE LA PRÁCTICA	Configurar y analizar el protocolo de enrutamiento avanzado BGP para garantizar la conectividad entre redes de diferentes sistemas autónomos, utilizando simulaciones en Cisco Packet Tracer, fomentando el pensamiento estratégico, la responsabilidad técnica y la toma de decisiones fundamentadas en redes organizacionales.

FUNDAMENTO TÉORICO

BGP (Border Gateway Protocol) es un protocolo de enrutamiento de vector de trayectoria utilizado para intercambiar información de enrutamiento entre sistemas autónomos en Internet, asegurando la selección de rutas óptimas, la escalabilidad y la estabilidad en redes de gran escala. Permite establecer políticas de enrutamiento basadas en atributos y mantiene la tabla de enrutamiento actualizada en redes interconectadas.

MATERIALES, EQUIPAMIENTO Y/O REACTIVOS

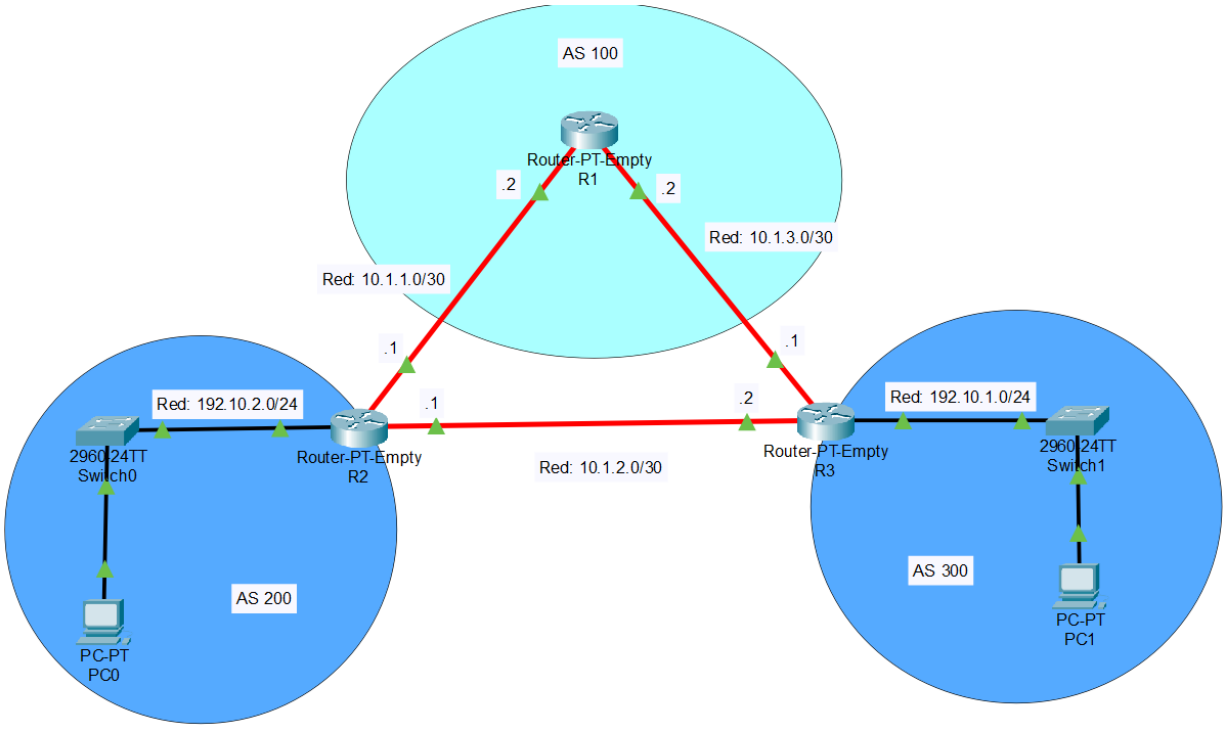
- Software Cisco Packet Tracer (última versión disponible).
- Ordenador con Windows (10, 11), macOS (10.15 o posterior) o Ubuntu (sistema operativo 22.04 LTS), CPU amd64 (x86-64), 4 GB de RAM libre y 1,4 GB de espacio libre en disco.
- Calculadora de subredes (ejemplo: ManageEngine).

PROCEDIMIENTO O METODOLOGÍA

1. Crear una topología en Cisco Packet Tracer con al menos tres routers (R1, R2, R3) simulando diferentes sistemas autónomos (AS), interconectados entre sí. La configuración a utilizar es la siguiente:

Conexión entre los dispositivos	Configuración	Máscara de red
R1 a R2	Gi0/0 10.1.1.2 - Gi0/0 10.1.1.1	255.255.255.252
R1 a R3	Gi1/0 10.1.3.2 – Gi0/0 10.1.3.1	255.255.255.252
R2 a R3	Gi1/0 10.1.2.1 – Gi1/0 10.1.2.2	255.255.255.252
R2 a PC0	Gi2/0 192.10.2.1 - Fa0 192.168.2.10	255.255.255.250
R3 a PC1	Gi2/0 192.10.1.1 - Fa0 192.168.1.10	255.255.255.250

2. La topología de la red quedaría de la siguiente manera:



Los cables utilizados son: straight-through y multi mode fiber.

1. Después de asegúrate de que las interfaces de los routers tengan direcciones IP configuradas, continuamos con la asignación de un número de sistema autónomo (AS) distinto a cada router (R1: AS 100, R2: AS 200, R3: AS 300):

   En cada router, ingresa al modo de configuración global y utiliza el comando **router bgp <número_de_as>** para definir el AS del router (router bgp 100, router bgp 200, router bgp 300). Ejemplo en terminal del router R1:

```
Router(config-if)#router bgp 100
```

2. Configuración de vecinos:

   Dentro del modo de configuración BGP, usa el comando **neighbor <dirección_ip> remote-as <número_de_as_remoto>** para establecer conexiones de peering con otros routers. Especifica la dirección IP del vecino y su número de AS remoto. Ejemplo en terminal de Cisco Packet Tracert:

```
Router(config)#router bgp 100
Router(config-router)#neighbor 10.1.1.1 remote-as 200
```

3. Anuncio de redes:

   Utiliza el comando **network <dirección_ip> mask <máscara_de_red>** para anunciar las redes directamente conectadas al router a través de BGP. Ejemplo en terminal de Cisco Packet Tracert del R1 AS 100:

```
Router(config-if)#router bgp 100
Router(config-router)#network 10.1.1.0 mask 255.255.255.252
```

4. Verificar el establecimiento de las sesiones BGP con el comando **show ip bgp summary**.
5. Utiliza el comando ping para probar la conectividad entre las redes anunciadas por diferentes routers.
6. Verifica la configuración de los vecinos con show ip bgp summary y show ip bgp neighbors.
7. Activar el modo de simulación para observar el proceso de intercambio de rutas y la transmisión de paquetes a través de BGP.
8. Documentar capturas de pantalla de las configuraciones, tablas de enrutamiento BGP y pruebas de conectividad como evidencia.

RESULTADOS ESPERADOS

- Configuración funcional de BGP entre diferentes sistemas autónomos.
- Establecimiento exitoso de sesiones de peer BGP.
- Verificación de la conectividad entre redes a través del protocolo BGP.

ANÁLISIS DE RESULTADOS

- ¿Cómo se establece la relación de peer BGP entre sistemas autónomos?
- ¿Qué ventajas ofrece BGP frente a protocolos de enrutamiento internos como OSPF o RIP?
- ¿Qué dificultades se encontraron durante la configuración y cómo se solucionaron?

CONCLUSIONES Y REFLEXIONES

Conclusión: La práctica permite a los estudiantes configurar y analizar el protocolo BGP en un entorno simulado, comprendiendo su funcionamiento para garantizar la conectividad entre redes de distintos sistemas autónomos, desarrollando habilidades técnicas necesarias para el Ingeniero en Software.

Reflexión: Esta práctica fomenta la toma de decisiones técnicas fundamentadas, permitiendo a los estudiantes identificar el papel del protocolo BGP en redes de gran escala y comprender su importancia en la conectividad y la estabilidad de Internet y redes empresariales, promoviendo la responsabilidad técnica en proyectos de infraestructura de red.

ACTIVIDADES COMPLEMENTARIAS

- Configurar filtros de rutas en BGP utilizando prefix-lists o route-maps y observar su funcionamiento.
- Investigar el uso de atributos de BGP como Weight, Local Preference y AS Path en la toma de decisiones de enrutamiento.
- Realizar un escenario con múltiples sistemas autónomos para analizar el comportamiento del protocolo BGP en entornos más complejos.

EVALUACIÓN Y EVIDENCIAS DE APRENDIZAJE

Criterios de evaluación	• Configuración correcta de BGP entre los sistemas autónomos. • Verificación de sesiones BGP y análisis de tablas de enrutamiento. • Reporte de práctica de laboratorio.
Rúbricas o listas de cotejo para valorar desempeño	• Configuración correcta de BGP entre los sistemas autónomos (30%). • Verificación de sesiones BGP y análisis de tablas de enrutamiento (30%). • Rúbrica: Reporte de práctica de laboratorio (40%).

Formatos de reporte de prácticas	• Documento institucional editable de “reporte de prácticas” que contiene: o Portada, o Introducción o Fundamentos teóricos o Objetivo de la práctica, hipótesis o Expectativa o planteamiento experimental o Materiales, equipamiento y/o reactivos o Procedimiento o metodología o Procesamiento de datos o Resultados o Análisis y discusión. o Conclusiones o Bibliografía o Anexos

FUENTES DE INFORMACIÓN

Cisco. (s.f.). Cisco Packet Tracer. Cisco Networking Academy. https://www.netacad.com/courses/packet-tracer

Kurose, J. F., & Ross, K. W. (2017). Redes de computadoras: Un enfoque descendente (7a ed.). Pearson Educación. https://www.academia.edu/40738627

Molina Robles, F. J. (2015). *Implantación de los elementos de la red local:* (ed.). RA-MA Editorial. https://elibro.net/es/lc/ues/titulos/62445

Sánchez Rubio, M., Barchino Plata, R., & Martínez Herráiz, J. J. (2020). Redes de computadores. Editorial Universidad de Alcalá. https://elibro.net/es/ereader/ues/131606

Bermúdez Luque, J. J. (Il.). (2023). *Montaje de infraestructuras de redes locales de datos. ELES0209:* (2 ed.). IC Editorial. https://elibro.net/es/lc/ues/titulos/248001

Universidad Estatal de Sonora. (2022). Secuencia didáctica del curso Medios y Protocolos de Comunicación. https://ues.sonora.edu.mx/index.php?option=com_sppagebuilder&view=page&id=81

NORMAS TÉCNICAS APLICABLES

- Justificar las configuraciones de direcciones IP y pruebas de utilerías utilizadas en prácticas.
- Sustentar el diseño de topologías con base en modelos de referencia OSI y TCP/IP.
- Asegurar el alineamiento con estándares internacionales de infraestructura de redes de datos.
  - ISO/IEC 7498-1:1994

    Base del modelo de referencia OSI, utilizado para la comprensión y segmentación de capas en redes.
  - ISO/IEC 8802-3:2017 (IEEE 802.3)

    Norma que define los aspectos de Ethernet, usada en las prácticas de conmutación de paquetes y configuración de redes.
  - RFC 791

    Norma técnica que define el protocolo IP, fundamental para direccionamiento y enrutamiento en redes TCP/IP.
  - RFC 792

    Base para las utilerías de diagnóstico de red utilizadas en prácticas (ping, tracert).
  - RFC 1058

    Define el protocolo RIP v1, base para prácticas de enrutamiento dinámico.
  - RFC 2453
  - Define las especificaciones de RIP v2, utilizado en la práctica de enrutamiento dinámico con subnetting y VLSM.
  - RFC 2328

    Define el protocolo OSPF, utilizado como referencia en prácticas de protocolos de enrutamiento avanzados.
  - RFC 4271

    Border Gateway Protocol 4 (BGP-4)

    Norma que define el protocolo BGP, aplicado en prácticas de enrutamiento de sistemas autónomos.
  - ISO/IEC 11801-1:2017

    Referente para infraestructura física de redes de datos, aplicable al diseño de topologías en prácticas.
  - IEEE 802.11
  - Wireless LAN (Wi-Fi) standards


UES
Universidad Estatal de Sonora
La Fuerza del Saber Estimulará mi Espíritu