

PRÁCTICA 1 - INTRODUCCIÓN

1. ¿Qué es una red? ¿Cuál es el principal objetivo para construir una red?

Una Red de Computadoras es un grupo de computadoras/dispositivos interconectados. El objetivo es compartir recursos como dispositivos, información y servicios.

2. ¿Qué es Internet? Describa los principales componentes que permiten su funcionamiento.

Es una red de redes de computadoras, descentralizada, pública, que ejecutan el conjunto abierto de protocolos (suite) TCP/IP. Integra diferentes protocolos de un nivel más bajo: INTERNETWORKING.

Los principales componentes son:

Capa de Acceso (Edge): Acceso Residenciales, Acceso de Organizaciones.

Capa de núcleo (Core): dividida en diferentes niveles:

Proveedores Regionales (Regional ISPs).

Proveedores Nacionales.

Proveedores Internacionales.

Proveedores Internacionales en el Tier 1.

3. ¿Qué son las RFCs?

Las RFC (Request For Comments) son documentos que establecen la definición de los protocolos.

4. ¿Qué es un protocolo?

Conjunto de conductas y normas a conocer, respetar y cumplir para comunicarse no solo en el medio oficial ya establecido, sino también en el medio social, laboral, etc.

Un protocolo define el formato, el orden de los mensajes intercambiados y las acciones que se llevan a cabo en la transmisión y/o recepción de un mensaje u otro evento.

5. ¿Por qué dos máquinas con distintos sistemas operativos pueden formar parte de una misma red?

Las máquinas con distintos sistemas operativos pueden formar parte de la misma red porque siguen protocolos de red estándar, como TCP/IP, que aseguran la interoperabilidad.

6. ¿Cuáles son las 2 categorías en las que pueden clasificarse a los sistemas finales o End Systems? Dé un ejemplo del rol de cada uno en alguna aplicación distribuida que corra sobre Internet.

Los end-systems pueden clasificarse en clientes y servidores.

Yo, utilizando el navegador, soy cliente al buscar y solicitar recursos en la red. Mientras que el servidor que aloja al sitio web google es servidor ya que procesa mis solicitudes.

7. ¿Cuál es la diferencia entre una red conmutada de paquetes de una red conmutada de circuitos?

En una red conmutada de paquetes, los datos se dividen en paquetes y cada uno viaja de forma independiente a través de la red, tomando rutas diferentes si es necesario. Esto permite un uso eficiente del ancho de banda y una mayor flexibilidad, pero puede causar variabilidad en el tiempo de entrega (latencia).

En cambio, en una red conmutada de circuitos, se establece una conexión fija y dedicada entre dos puntos durante toda la comunicación. Esto garantiza un ancho de banda constante y un retraso mínimo, pero puede ser menos eficiente en el uso de recursos si la conexión está ociosa.

8. Analice qué tipo de red es una red de telefonía y qué tipo de red es Internet.

Una red de telefonía, tradicionalmente usan conmutación de circuitos. En una llamada telefónica, se establece un circuito dedicado entre el emisor y el receptor durante toda la conversación, garantizando una calidad constante y baja latencia.

Internet, por su parte, utiliza conmutación de paquetes. Los datos se dividen en paquetes que viajan de forma independiente a través de la red, permitiendo un uso más eficiente del ancho de banda y adaptándose a la variabilidad en el tráfico de la red.

9. Describa brevemente las distintas alternativas que conoce para acceder a Internet en su hogar.

Se puede acceder mediante cable de red (Ethernet) o por conexión Wi-Fi (inalámbrica).

10. ¿Qué ventajas tiene una implementación basada en capas o niveles?

Las ventajas que ofrecen son la modularidad, interoperabilidad, flexibilidad, seguridad y gestión, y simplificación.

11. ¿Cómo se llama la PDU de cada una de las siguientes capas: Aplicación, Transporte, Red y Enlace?

Datos, segmento, paquete y trama, respectivamente.

12. ¿Qué es la encapsulación? Si una capa realiza la encapsulación de datos, ¿qué capa del nodo receptor realizará el proceso inverso?

La encapsulación en una capa de red es el proceso mediante el cual los datos son empaquetados con la información de control necesaria para que puedan ser transmitidos correctamente a través de una red.

Cada capa en el nodo receptor realiza la decapsulación de la PDU de la capa inferior para recuperar los datos originales, procesándolos en la secuencia inversa a la encapsulación que se llevó a cabo en el nodo emisor.

13. Describa cuáles son las funciones de cada una de las capas del stack TCP/IP o protocolo de Internet.

. Capa de Aplicación: Proporciona servicios de red directamente a las aplicaciones de usuario. Maneja la comunicación entre aplicaciones y protocolos como HTTP (para la web), SMTP (para correo electrónico), FTP (para transferencia de archivos), y DNS (para resolución de nombres de dominio).

. Capa de Transporte: Asegura la entrega correcta y en orden de los datos entre aplicaciones en diferentes sistemas. Controla el flujo de datos y maneja la retransmisión de paquetes perdidos. Ofrece servicios de transporte confiables o no confiables.

. Capa de Red: Se encarga del direccionamiento y enrutamiento de paquetes de datos desde el origen hasta el destino a través de la red. Determina la ruta más adecuada para los paquetes y maneja el enrutamiento entre redes diferentes.

. Capa de Enlace de Datos: Maneja la comunicación entre dispositivos en la misma red local o enlace, asegurando que los datos se transmitan de manera eficiente y libre de errores en el enlace físico. Controla el acceso al medio y detecta y corrige errores a nivel de enlace.

14. Compare el modelo OSI con la implementación TCP/IP.

Similitudes: Ambos se dividen en capas. Ambos tienen capas de aplicación, aunque incluyen servicios distintos. Ambos tienen capas de transporte similares. Ambos tienen capa de red similar pero con distinto nombre. Se supone que la tecnología es de conmutación de paquetes.

Diferencias: TCP/IP combina las funciones de la capa de presentación y de sesión en la capa de aplicación. TCP/IP combina la capas de enlace de datos y la capa física del modelo OSI en una sola capa. TCP/IP más simple porque tiene menos capas. Los protocolos TCP/IP son los estándares en torno a los cuales se desarrolló Internet, de modo que la credibilidad del modelo TCP/IP se debe en gran parte a sus protocolos. El modelo OSI es un modelo “más” de referencia, teórico, aunque hay implementaciones.

PRACTICA 2 - HTTP

1. ¿Cuál es la función de la capa de aplicación?

Provee servicios de comunicación a los usuarios y a las aplicaciones, incluye las aplicaciones mismas. Define el formato y la semántica de los mensajes. Y también define cómo debe ser el código y qué mensajes se deben intercambiar.

2. Si dos procesos deben comunicarse:

a. ¿Cómo podrían hacerlo si están en diferentes máquinas?

Deben respetar los protocolos definidos, así como también la semántica y formato de los mensajes.

b. Y si están en la misma máquina, ¿qué alternativas existen?

Lo harán mediante mecanismos locales, como por ejemplo envío de señales o memoria compartida, entre otros.

3. Explique brevemente cómo es el modelo Cliente/Servidor. Dé un ejemplo de un sistema Cliente/Servidor en la “vida cotidiana” y un ejemplo de un sistema informático que siga el modelo Cliente/Servidor. ¿Conoce algún otro modelo de comunicación?

Es un modelo de carga compartida donde la idea inicial es que el cliente pone el procesamiento de interfaz. Luego el servidor pone el resto del procesamiento. El servidor corre el servicio esperando de forma pasiva la conexión. Los clientes se conectan al servidor y se comunican a través de este.

Un ejemplo de la vida cotidiana podría ser una estación de servicio.

Google Chrome podría ser un ejemplo de un sistema informático que siga el modelo Cliente/Servidor.

Si, existen también: Modelo Mainframe Centralizado, Modelo Peer-to-Peer, Modelo Peer-to-Peer Híbrido, Nit Torrent y Skype.

4. Describa la funcionalidad de la entidad genérica "Agente de usuario" o "User agent".

La entidad genérica "**Agente de Usuario**" se refiere a un componente o entidad que actúa en nombre del usuario para interactuar con otros sistemas o servicios.

5. ¿Qué son y en qué se diferencian HTML y HTTP?

. **HTML** es un lenguaje de marcado (o etiquetado) utilizado para estructurar y presentar contenido en la web. Es el componente que define cómo se organiza y muestra el contenido en un navegador web.

. Por otro lado, **HTTP** es un protocolo de comunicación utilizado para la transferencia de datos entre un cliente (como un navegador web) y un servidor web. HTTP define cómo se envían y reciben los mensajes en la web.

6. HTTP tiene definido un formato de mensaje para los requerimientos y las respuestas.

(Ayuda: apartado "Formato de mensaje HTTP", Kurose).

a. ¿Qué información de la capa de aplicación nos indica si un mensaje es de requerimiento o de respuesta para HTTP? ¿Cómo está compuesta dicha información? ¿Para qué sirven las cabeceras?

Si tiene método, URL y versión es un mensaje de requerimiento; mientras que si indica la versión HTTP, el código de estado y la frase de razón, corresponde a una respuesta.

Una cabecera de petición está compuesta por su nombre (no sensible a las mayúsculas) seguido de dos puntos ':', y a continuación su valor.

Las cabeceras HTTP permiten al cliente y al servidor enviar información adicional junto a una petición o respuesta.

b. ¿Cuál es su formato? (Ayuda:

<https://developer.mozilla.org/es/docs/Web/HTTP/Headers>)

Una cabecera de petición está compuesta por su nombre (no sensible a las mayúsculas) seguido de dos puntos ':', y a continuación su valor (sin saltos de línea). Los espacios en blanco a la izquierda del valor son ignorados. Se pueden agregar cabeceras propietarias personalizadas usando el prefijo 'X-', pero esta convención se encuentra desfasada desde Julio de 2012.

c. Suponga que desea enviar un requerimiento con la versión de HTTP 1.1 desde curl/7.74.0 a un sitio de ejemplo como www.misitio.com para obtener el recurso /index.html. En base a lo indicado, ¿qué información debería enviarse mediante encabezados? Indique cómo quedaría el requerimiento.

GET www.misitio.com/index.html HTTP 1.1

User-Agent: curl/7.74.0

7. Utilizando la VM, abra una terminal e investigue sobre el comando curl. Analice para qué sirven los siguientes parámetros (-I, -H, -X, -s).

curl es una herramienta para transferir datos desde o hacia un servidor, utilizando uno de los protocolos admitidos (DICT, FILE, FTP, FTPS, GOPHER, HTTP, HTTPS, IMAP, IMAPS, LDAP, LDAPS, MQTT, POP3, POP3S, RTMP, RTMPS, RTSP, SCP, SFTP, SMB, SMBS, SMTP, SMTPS, TELNET y TFTP). El comando está diseñado para trabajar sin interacción del usuario.

-I, --head

(HTTP FTP FILE) Obtiene solo los encabezados. Los servidores HTTP cuentan con el comando HEAD que utiliza para obtener nada más que el encabezado de un documento. Cuando se usa en un archivo FTP o FILE, curl muestra solo el tamaño del archivo y la hora de la última modificación.

-H, --header

Sirve para incluir un header adicional en la solicitud HTTP. Se puede especificar cualquier número de encabezados adicionales. Hay que tener en cuenta que si se agrega un encabezado personalizado que tiene el mismo nombre que uno de los internos que usaría curl, se usará el encabezado establecido externamente en lugar del interno.

-X, --request

Especifica un método de solicitud personalizado que se utilizará al comunicarse con el servidor HTTP. CURL por defecto utiliza GET.

-s, --silent

Modo silencioso de CURL. No mostrará la barra de progreso ni los mensajes de error. Silencia Curl. Seguirá generando los datos que solicita, potencialmente incluso al terminal/salida estándar, a menos que los redirija. Es útil si deseas que la salida de curl sea más limpia y solo quieras ver la respuesta del servidor

8. Ejecute el comando curl sin ningún parámetro adicional y acceda a www.redes.unlp.edu.ar. Luego responda:

- a. ¿Cuántos requerimientos realizó y qué recibió? Pruebe redirigiendo la salida (>) del comando curl a un archivo con extensión html y abrirlo con un navegador.
Realicé un solo requerimiento GET y recibí un archivo HTML que tiene un tamaño de 4898.
- b. ¿Cómo funcionan los atributos href de los tags link e img en html?
El atributo href en la etiqueta se utiliza para enlazar recursos externos y el atributo src en la etiqueta se utiliza para especificar la ubicación de la imagen que se mostrará en la página web. En ambos casos, el navegador realiza solicitudes HTTP/HTTPS para descargar los recursos externos especificados en las URLs de los atributos href o src. Luego, dependiendo del tipo de recurso, realiza acciones adicionales como aplicar estilos en el caso de las hojas de estilo o mostrar imágenes en el caso de las etiquetas .

- c. *Para visualizar la página completa con imágenes como en un navegador, ¿alcanza con realizar un único requerimiento?*

No, no alcanza con un único requerimiento. Cada recurso, como un archivo CSS, un archivo JavaScript o una imagen, se solicita por separado al servidor.

- d. *¿Cuántos requerimientos serían necesarios para obtener una página que tiene dos CSS, dos Javascript y tres imágenes? Diferencie cómo funcionaría un navegador respecto al comando curl ejecutado previamente.*

Se necesitarán: 1 requerimiento para el archivo base HTML, 1 requerimiento para el favicon, 2 requerimientos para CSS, 2 requerimientos para Javascript, 3 requerimientos para las tres imágenes.

curl solo realizará un solo requerimiento (el archivo base HTML), requiere solicitudes manuales.

9. Ejecute a continuación los siguientes comandos: `curl -v -s www.redes.unlp.edu.ar > /dev/null curl -I -v -s www.redes.unlp.edu.ar`

- a. *¿Qué diferencias nota entre cada uno?*

La diferencia es que de esta manera lista por separado todas las secciones mostrando sus datos.

- b. *¿Qué ocurre si en el primer comando se quita la redirección a /dev/null? ¿Por qué no es necesaria en el segundo comando?*

Nada, continua igual.

Porque /dev/null que redirige la salida estándar (la respuesta enviada por el servidor) a /dev/null (que la descarta), entonces a lo que vemos nosotros continúa todo de la misma manera.

- c. *¿Cuántas cabeceras viajaron en el requerimiento? ¿Y en la respuesta?*

Viajaron 2 en cada una.

10. *¿Qué indica la cabecera Date?*

La cabecera "Date" es una de las cabeceras definidas en la RFC. Esta cabecera indica la fecha y hora en que se generó la solicitud o respuesta HTTP.

11. *En HTTP/1.0, ¿cómo sabe el cliente que ya recibió todo el objeto solicitado de manera completa? ¿Y en HTTP/1.1?*

. En HTTP/1.0 el cliente se da cuenta de que ha recibido todo el objeto solicitado cuando el servidor cierra la conexión después de enviar la respuesta.

. En HTTP/1.1: Se introducen mejoras para manejar este problema. El encabezado "ContentLength" indica al cliente la longitud en bytes del objeto en la respuesta, permitiéndole saber cuántos datos esperar. El encabezado "Transfer-Encoding" con valor "chunked" divide la respuesta en trozos, y el cliente detecta el final de la respuesta cuando recibe un trozo de tamaño 0.

12. *Investigue los distintos tipos de códigos de retorno de un servidor web y su significado. Considere que los mismos se clasifican en categorías (2XX, 3XX, 4XX, 5XX).*

. 1XX: Códigos informativos.

. 2XX: Códigos de éxito.

- . 3XX: Códigos de Redirección.
- . 4XX: Códigos de Error del Cliente.
- . 5XX: Códigos de Error del Servidor.

13. Utilizando curl, realice un requerimiento con el método HEAD al sitio www.redes.unlp.edu.ar e indique:

a. ¿Qué información brinda la primera línea de la respuesta?

La primera línea nos brinda la versión de HTTP (HTTP 1.1) y el código de respuesta (200 OK).

b. ¿Cuántos encabezados muestra la respuesta?

Muestra un solo encabezado.

c. ¿Qué servidor web está sirviendo la página?

Apache 2.4.56 (Unix).

14. Utilizando curl, acceda al sitio www.redes.unlp.edu.ar/restringido/index.php y siga las instrucciones y las pistas que vaya recibiendo hasta obtener la respuesta final. Será de utilidad para resolver este ejercicio poder analizar tanto el contenido de cada página como los encabezados.

redes@debian:~\$ curl -H "Authorization: Basic cmVkZXM6UlID"

www.redes.unlp.edu.ar/restringido/the-end.php

¡Felicitaciones, llegaste al final del ejercicio!

Fecha: 2024-09-02 15:00:40

Verificación: a096d59ee539474a8b56fc1f7c5ed9a1252a39c7cf62bb7f8e49d7c83cda3723

15. Utilizando la VM, realice las siguientes pruebas:

a. Ejecute el comando 'curl www.redes.unlp.edu.ar/extras/prueba-http-1-0.txt' y copie la salida completa (incluyendo los dos saltos de línea del final).

GET /http/HTTP-1.1/ HTTP/1.0

User-Agent: curl/7.38.0

Host: www.redes.unlp.edu.ar

Accept: */*

b. Desde la consola ejecute el comando telnet www.redes.unlp.edu.ar 80 y luego pegue el contenido que tiene almacenado en el portapapeles. ¿Qué ocurre luego de hacerlo?

Despliega un menú con opciones:

Usage: telnet [-4] [-6] [-8] [-E] [-L] [-a] [-d] [-e char] [-l user]
[-n tracefile] [-b addr] [-r] [host-name [port]]

bash: User-Agent:: command not found

bash: Host:: command not found

bash: Accept:: command not found

- c. Repita el proceso anterior, pero copiando la salida del recurso /extras/prueba-http-1-1.txt. Verifique que debería poder pegar varias veces el mismo contenido sin tener que ejecutar el comando telnet nuevamente.
Despliega el mismo menú que el ejemplo anterior.

16. En base a lo obtenido en el ejercicio anterior, responda:

- a. ¿Qué está haciendo al ejecutar el comando telnet?

El comando `telnet` se utiliza para conectarse a otros sistemas a través de la red utilizando el protocolo Telnet. Este protocolo permite establecer una sesión de comunicación remota con otro dispositivo, lo que te permite acceder a la línea de comandos de ese dispositivo como si estuvieras trabajando en él localmente.

- b. ¿Qué método HTTP utilizó? ¿Qué recurso solicitó?

Utiliza el método GET, y solicita la URL ingresada.

- c. ¿Qué diferencias notó entre los dos casos? ¿Puede explicar por qué?

La diferencia que hay es que la conexión no se cierra una vez que el servidor envía la respuesta en el punto c. Esto se debe a que en contraste con HTTP 1.0, donde cada solicitud y respuesta requería abrir y cerrar una nueva conexión, en HTTP 1.1, una sola conexión puede ser reutilizada para varias transacciones.

- d. ¿Cuál de los dos casos le parece más eficiente? Piense en el ejercicio donde analizó la cantidad de requerimientos necesarios para obtener una página con estilos, javascripts e imágenes. El caso elegido, ¿puede traer asociado algún problema?

Es más eficiente el caso de HTTP 1.1 ya que reduce la sobrecarga asociada con la apertura y el cierre de conexiones, lo que conduce a una carga más rápida de páginas web y una mejor utilización de los recursos de red. Hay un problema asociado con la conexión persistente, especialmente cuando se trata de recursos grandes o de larga duración. Si un recurso se mantiene en la conexión durante un período prolongado, podría bloquear la conexión y retrasar la obtención de otros recursos. Esto se conoce como el problema de "holgura de cabeza" (head-of-line blocking). Para abordar este problema, los navegadores modernos utilizan técnicas como la multiplexación y el pipelining para permitir la transferencia de múltiples recursos a la vez.

17. En el siguiente ejercicio veremos la diferencia entre los métodos POST y GET. Para ello, será necesario utilizar la VM y la herramienta Wireshark. Antes de iniciar considere:

- Capture los paquetes utilizando la interfaz con IP 172.28.0.1. (Menú “Capture ->Options”. Luego seleccione la interfaz correspondiente y presione Start).
- Para que el analizador de red sólo nos muestre los mensajes del protocolo http introduciremos la cadena ‘http’ (sin las comillas) en la ventana de especificación de filtros de visualización (display-filter). Si no hicéramos esto veríamos todo el tráfico que es capaz de capturar nuestra placa de red. De los paquetes que son capturados, aquel que esté seleccionado será mostrado en forma detallada en la sección que está justo debajo. Como sólo estamos interesados en http ocultaremos toda la información que no es relevante para esta práctica (Información de trama, Ethernet, IP y TCP). Desplegar la

información correspondiente al protocolo HTTP bajo la leyenda “Hypertext Transfer Protocol”.

- Para borrar la caché del navegador, deberá ir al menú “Herramientas->Borrar historial reciente”. Alternativamente puede utilizar Ctrl+F5 en el navegador para forzar la petición HTTP evitando el uso de caché del navegador.
 - En caso de querer ver de forma simplificada el contenido de una comunicación http, utilice el botón derecho sobre un paquete HTTP perteneciente al flujo capturado y seleccione la opción Follow TCP Stream.
- a. Abra un navegador e ingrese a la URL: www.redes.unlp.edu.ar e ingrese al link en la sección “Capa de Aplicación” llamado “Métodos HTTP”. En la página mostrada se visualizan dos nuevos links llamados: Método GET y Método POST. Ambos muestran un formulario como el siguiente:

El formulario es un cuadro rectangular con los siguientes campos:

- Campo de texto para Nombre.
- Campo de texto para Apellido.
- Campo de texto para Email.
- Campo de radio para Sexo: "Masculino" (seleccionado) y "Femenino".
- Campo de texto para Contraseña.
- Campo de checkbox para "Recibir confirmaciones por email".
- Botón azul "Enviar" en el pie de formulario.

- b. Analice el código HTML
- c. Utilizando el analizador de paquetes Wireshark capture los paquetes enviados y recibidos al presionar el botón Enviar.
- d. ¿Qué diferencias detectó en los mensajes enviados por el cliente?
La diferencia que se detecta es que si se trata de un GET, se envía la información como parámetro de la URL, mientras que si se trata de un POST, esta se envía en el cuerpo de la solicitud.
- e. ¿Observó alguna diferencia en el browser si se utiliza un mensaje u otro?
Si, en el caso del GET, se pueden ver en la URL los parámetros enviados, en el caso del POST no, se mantiene la misma URL que se tenía antes de apretar el botón ENVIAR.

18. Investigue cuál es el principal uso que se le da a las cabeceras Set-Cookie y Cookie en HTTP y qué relación tienen con el funcionamiento del protocolo HTTP.

19. ¿Cuál es la diferencia entre un protocolo binario y uno basado en texto? ¿De qué tipo de protocolo se trata HTTP/1.0, HTTP/1.1 y HTTP/2?

Un protocolo binario transmite datos en forma de patrones de bits que las máquinas pueden entender directamente. Suele ser más eficiente en términos de velocidad y uso de ancho de banda, ya que no se desperdicia espacio en caracteres de formato o en la interpretación de texto legible por humanos.

Un protocolo basado en texto envía datos como cadenas legibles utilizando caracteres como letras, números y símbolos. Estos caracteres suelen estar codificados en ASCII o UTF-8. Aunque esto hace que la comunicación entre sistemas sea más comprensible para

los humanos, puede ser menos eficiente en términos de velocidad y uso de ancho de banda, ya que se requiere más información para representar los mismos datos que en formato binario.

HTTP/1.0, HTTP/1.1 son protocolos basados en textos mientras que HTTP/2 es un protocolo binario

20. Responder las siguientes preguntas:

- a. ¿Qué función cumple la cabecera Host en HTTP 1.1? ¿Existía en HTTP 1.0? ¿Qué sucede en HTTP/2? (Ayuda:

<https://undertow.io/blog/2015/04/27/An-in-depth-overview-of-HTTP2.html> para HTTP/2)

La cabecera "Host" en HTTP 1.1 tiene la función de indicar el nombre de dominio (se puede indicar opcionalmente el puerto) al que se está haciendo la solicitud dentro del encabezado de la petición.

Si, existía. En HTTP 1.0, la cabecera "Host" no es obligatoria pero puede ser necesaria dependiendo de cómo el servidor web esté configurado. Esto significa que si la cabecera "Host" no estaba presente en una solicitud HTTP 1.0, el servidor asumiría que la solicitud estaba destinada al dominio asociado con la dirección IP del servidor.

En HTTP/2, la cabecera "Host" es reemplazada por ":authority".

- b. En HTTP/1.1, ¿es correcto el siguiente requerimiento? GET /index.php HTTP/1.1
User-Agent: curl/7.54.0

Si, es correcto.

- c. ¿Cómo quedaría en HTTP/2 el siguiente pedido realizado en HTTP/1.1 si se está usando https?

GET /index.php HTTP/1.1
Host: www.info.unlp.edu.ar

:method: get
:path: /index.php
:scheme: https
:authority: www.info.unlp.edu.ar

PRACTICA 3 - DNS

1. Investigue y describa cómo funciona el DNS. ¿Cuál es su objetivo?

El servicio DNS (Domain Name System) funciona como un sistema distribuido de forma jerárquica, a través de dominios, sub-dominios y nombres finales, con un conjunto de servidores a lo largo del mundo. Cada servidor tiene la responsabilidad de mantener una parte dentro de la jerarquía de nombres.

Su objetivo principal es el de traducir nombres de dominio a direcciones IP para lograr una abstracción de las direcciones de red utilizadas internamente por los protocolos, permitiendo así ubicar a un dispositivo por su nombre sin importar cuál es su dirección IP actual, haciendo que no sea necesario para las personas recordar la dirección IP.

2. ¿Qué es un root server? ¿Qué es un generic top-level domain (gtld)?

Los root servers son los encargados de proporcionar las direcciones IP de los Top Level Domains (la parte más alta de la jerarquía luego de la raíz).

gTLD son una categoría TLD en DNS. Son dominios con propósitos particulares, de acuerdo a diferentes actividades políticas definidas por el ICANN (Unsponsored TLD) o definidas por otra organización (Sponsored TLD). Son los dominios que básicamente se utilizan para identificar categorías amplias y distintos tipos de sitios web. Algunos ejemplos de gTLDs incluyen .com, .org, .net y .info.

3. ¿Qué es una respuesta del tipo autoritativa?

Una respuesta autoritativa es aquella dada por el servidor que tiene la autoridad sobre el nombre que se está consultando. Este responde directamente desde su base de datos de nombres, sin subdelegaciones ni cacheo de direcciones. Caso contrario, si se realiza esto último, se trata de una Respuesta NO Autoritativa.

4. ¿Qué diferencia una consulta DNS recursiva de una iterativa?

La diferencia es que cuando realizo una consulta recursiva, la realizo esperando el resultado final, y además, la realizo yo como usuario.

En este tipo de respuesta, el servidor DNS al que se le solicita la resolución de un dominio se encarga de hacer todo el trabajo. Si no conoce la respuesta, contacta con otros servidores DNS en nombre del cliente, obteniendo la respuesta final. El cliente solo recibe la respuesta completa y no interactúa con otros servidores DNS.

Mientras que cuando se realiza una consulta iterativa, se consulta por IPs para ir acercándose a la respuesta final.

El cliente DNS interactúa con múltiples servidores DNS, haciendo varias solicitudes hasta obtener la respuesta final. El primer servidor consultado no resuelve completamente la consulta, sino que da una pista de a dónde debe ir el cliente para continuar la búsqueda (es decir, le proporciona la dirección de un servidor DNS más específico).

5. ¿Qué es el resolver?

El Resolver se lo podría considerar como un agente encargado de resolver los nombres a solicitud del cliente. Se puede tener un Stub/Dumb Resolver que no realiza ninguna forma de caching y deja que el encargado de esto sea el Servidor Local o un resolver activo, llamado Smart Resolver, que funciona en cada equipo como si fuese un Servidor Local, realizando caching u ofreciendo funcionalidades extras. Este suele hacer consultas recursivas.

6. Describa para qué se utilizan los siguientes tipos de registros de DNS:

- a) **A:** mapean un nombre de dominio a una dirección IPv4. Pueden existir varios registros (A) con el mismo nombre
- b) **NS:** indican los servidores de nombre autoritativos para una sub-dominio. A partir de esto, se puede lograr una delegación de sub-dominios. No hay prioridad, todos los servidores tienen la misma precedencia.
- c) **MX:** indican para un nombre de dominio cuáles son los servidores de mail SMTP encargados de recibir los mensajes para ese dominio. El servidor de mail SMTP que envía el mensaje deberá consultar, vía el servicio de DNS, cuáles son los servidores SMTP

receptores para el dominio dado. Se asignan prioridades para servidores del mismo dominio.

- d) **CNAME**: mapean un nombre de dominio a otros nombres. Hacen el mapeo del alias de un dominio su nombre canónico (vendría a ser el nombre original).
- e) **PTR**: mapean direcciones IP a nombres de dominio. Son el inverso de los registros (A). Trabajan en el dominio especial in-addr.arpa.
- f) **SOA**: se utilizan para proporcionar información autoritaria sobre una zona de dominio, lo que incluye información sobre la administración y configuración de esa zona. Solo se admite un registro SOA por zona. Permite que servidores autoritarios de la misma zona se puedan sincronizar.
- g) **AAAA**: mapean un nombre de dominio a una dirección IPv6.
- h) **TXT**: Son registros que mapean de un nombre de dominio a información extra asociada con el equipo que tiene dicho nombre, por ejemplo pueden indicar finalidad, usuarios, etc. No son utilizados habitualmente. Se los puede ver en uso asociando una clave pública, utilizando por ejemplo IPSec con un esquema de Opportunistic Encryption.
- i) **SRV**: se utilizan para asociar servicios o recursos a nombres de dominio.

7. *En Internet, un dominio suele tener más de un servidor DNS, ¿por qué cree que esto es así?*

Para que se pueda acceder lo más rápido posible (geográficamente hablando): mejora la velocidad de resolución al servir a usuarios más cercanos; para que haya redundancia y disponibilidad: en caso de que un servidor falle se tiene otro como “backup”; para que haya distribución de carga: en caso de que sea un servidor muy consultado, se evita la sobrecarga en un solo servidor.

8. *Cuando un dominio cuenta con más de un servidor, uno de ellos es el primario (o maestro) y todos los demás son secundarios (o esclavos). ¿Cuál es la razón de que sea así?*

La razón de que sea así es para simplificar la configuración de los servidores autoritarios, evitando configurar a cada servidor de un mismo dominio de forma independiente. En lugar de esto, se configura aquel que es primario y el resto de los servidores se sincronizan con este. Esto a su vez garantizar la consistencia de los datos DNS.

9. *Explique brevemente en qué consiste el mecanismo de transferencia de zona y cuál es su finalidad.*

La transferencia de zona es la copia de la base de datos de nombres de un servidor primario a uno secundario. Esto permite mantener la consistencia entre los servidores de una zona de dominio.

10. Imagine que usted es el administrador del dominio de DNS de la UNLP (unlp.edu.ar). A su vez, cada facultad de la UNLP cuenta con un administrador que gestiona su propio dominio (por ejemplo, en el caso de la Facultad de Informática se trata de info.unlp.edu.ar). Suponga que se crea una nueva facultad, Facultad de Redes, cuyo dominio será redes.unlp.edu.ar, y el administrador le indica que quiere poder manejar su propio dominio. ¿Qué debe hacer usted para que el administrador de la Facultad de Redes pueda gestionar el dominio de forma independiente? (Pista: investigue en qué consiste la delegación de dominios). Indicar qué registros de DNS se deberían agregar.

Debo delegarle la administración del dominio. Para ello transfiero la autoridad del subdominio "redes.unlp.edu.ar" al administrador de la Facultad de Redes. Hay que configurar registros NS que apunten a los servidores DNS de la Facultad de Redes como servidores autoritarios para ese subdominio. Para hacerlo, el administrador de la Facultad de Redes debe proporcionarle los nombres y direcciones IP de los servidores DNS que desea utilizar.

11. Responda y justifique los siguientes ejercicios.

a. En la VM, utilice el comando dig para obtener la dirección IP del host www.redes.unlp.edu.ar y responda:

i. ¿La solicitud fue recursiva? ¿Y la respuesta? ¿Cómo lo sabe?

Si, fue recursiva, al igual que la respuesta. Esto se puede conocer gracias a los flags rd y ra.

ii. ¿Puede indicar si se trata de una respuesta autoritativa? ¿Qué significa que lo sea?

Si, puedo indicar que es una respuesta autoritaria, gracias al flag aa.

Una respuesta es **autoritativa** cuando proviene de un servidor DNS que tiene información directa y oficial sobre el dominio en cuestión. En otras palabras, un servidor autoritativo es el que tiene la autoridad de proporcionar la información exacta sobre un dominio porque es el servidor que gestiona los registros DNS para ese dominio.

iii. ¿Cuál es la dirección IP del resolver utilizado? ¿Cómo lo sabe?

La dirección IP del resolver utilizado es 172.28.0.29. Se puede ver en la línea:
;; SERVER: 172.28.0.29#53(172.28.0.29).

b. ¿Cuáles son los servidores de correo del dominio redes.unlp.edu.ar? ¿Por qué hay más de uno y qué significan los números que aparecen entre MX y el nombre? Si se quiere enviar un correo destinado a redes.unlp.edu.ar, ¿a qué servidor se le entregará? ¿En qué situación se le entregará al otro?

mail.redes.unlp.edu.ar con prioridad **10** es el servidor de correo principal.

backupmail.redes.unlp.edu.ar con prioridad **20** es el servidor de correo de respaldo.

Si se quiere enviar un correo destinado a redes.unlp.edu.ar se le entregara a mail.redes.unlp.edu.ar

Si el servidor principal **mail.redes.unlp.edu.ar** no está disponible (por ejemplo, si está caído, no responde o tiene algún problema técnico), entonces el sistema de correo intentará entregar el mensaje a **backupmail.redes.unlp.edu.ar**.

c. ¿Cuáles son los servidores de DNS del dominio redes.unlp.edu.ar?

Son ns-sv-a.redes.unlp.edu.ar y ns-sv-b.redes.unlp.edu.ar

d. Repita la consulta anterior cuatro veces más. ¿Qué observa? ¿Puede explicar a qué se debe?

Se puede observar: Cambia el ID de la consulta - Cambia COOKIE - El TTL del NS y de A es el mismo - Cambia el valor de When - También cambia el Query time

e. Observe la información que obtuvo al consultar por los servidores de DNS del dominio. En base a la salida, ¿es posible indicar cuál de ellos es el primario?

No, para eso se debe hacer: `dig redes.unlp.edu.ar -t soa`.

f. Consulte por el registro SOA del dominio y responda.

i. ¿Puede ahora determinar cuál es el servidor de DNS primario?

Si, se puede.

Es el root es ns-sv-b.redes.unlp.edu.ar.

ii. ¿Cuál es el número de serie, qué convención sigue y en qué casos es importante actualizarlo?

El número de serie es “2020031700”. Hay dos métodos comunes para actualizar el campo SERIAL del registro SOA de zona:

- El primer método es comenzar el número de serie en 1 y aumentarlo en cada cambio.
- El segundo es el siguiente utilizando formato YYYYMMDDSS que permite saber en qué fecha se creó la actualización. Con cada cambio en un mismo día, el número de versión (SS) aumenta en una cifra. Al día siguiente cambia el número de serie y el número de versión vuelve a ponerse a 00.

iii. ¿Qué valor tiene el segundo campo del registro? Investigue para qué se usa y cómo se interpreta el valor.

El segundo campo tiene el valor “604800”. Se trata del campo “Refresh” que indica cada cuanto tiempo los servidores secundarios deben refrescar desde el primario. La RFC1912 recomienda entre 1200 a 43200 segundos.

iv. ¿Qué valor tiene el TTL de caché negativa y qué significa?

Tiene el valor “86400”. Esto quiere decir que si se preguntó por un valor en donde el servidor autoritativo respondió que no lo tiene el cliente no volverá a preguntar por ese nombre de dominio durante 86400 segundos (24 horas) después de recibir la respuesta negativa del servidor autoritativo.

g. Indique qué valor tiene el registro TXT para el nombre saludo.redes.unlp.edu.ar.

Investigue para qué es usado este registro.

El registro TXT para el nombre saludo.redes.unlp.edu.ar tiene el valor “HOLA”.

Los registros TXT en DNS se utilizan para almacenar información de texto arbitraria sobre el dominio. Son versátiles y pueden ser utilizados para diferentes propósitos, incluyendo:

Verificación de dominio.

Configuración de SPF (Sender Policy Framework).

Configuración de DKIM (DomainKeys Identified Mail).

Configuración de DMARC (Domain-based Message Authentication, Reporting, and Conformance).

h. Utilizando dig, solicite la transferencia de zona de redes.unlp.edu.ar, analice la salida y responda.

i. ¿Qué significan los números que aparecen antes de la palabra IN? ¿Cuál es su finalidad?

Es el TTL. Este indica cuánto tiempo debe almacenarse en caché una pieza de información antes de que deba considerarse obsoleta o caduca.

ii. ¿Cuántos registros NS observa? Compare la respuesta con los servidores de DNS del dominio redes.unlp.edu.ar que dio anteriormente. ¿Puede explicar a qué se debe la diferencia y qué significa?

Se observan 4 registros NS debido a que se están obteniendo todos los registros del dominio "redes.unlp.edu.ar", que incluyen los registros que indican a donde delegar cuando se trata del subdominio "practica.redes.unlp.edu.ar" (se está delegando a los servidores "ns1.practica.redes.unlp.edu.ar." y "ns2.practica.redes.unlp.edu.ar.")

i. Consulte por el registro A de www.redes.unlp.edu.ar y luego por el registro A de www.practica.redes.unlp.edu.ar. Observe los TTL de ambos. Repita la operación y compare el valor de los TTL de cada uno respecto de la respuesta anterior. ¿Puede explicar qué está ocurriendo? (Pista: observar los flags será de ayuda).

El TTL de practica.redes.unlp.edu.ar es menor que el de redes.unlp.edu.ar y además el de práctica va disminuyendo a medida que se sigue consultando. Esto ocurre porque redes.unlp.edu.ar es el autoritativo (se puede ver en el flag aa) y practica.redes.unlp.edu.ar debe actualizar su información.

j. Consulte por el registro A de www.practica2.redes.unlp.edu.ar. ¿Obtuvo alguna respuesta? Investigue sobre los códigos de respuesta de DNS. ¿Para qué son utilizados los mensajes NXDOMAIN y NOERROR?

Se obtiene una respuesta con el estado "NXDOMAIN". El mensaje NXDOMAIN se utiliza para informar que no se pudo encontrar el nombre de dominio consultado, mientras que el mensaje NOERROR se utiliza para indicar que la resolución de nombres se realizó con éxito y se encontró una respuesta válida.

12. Investigue los comandos nslookup y host. ¿Para qué sirven? Intente con ambos comandos obtener:

- Dirección IP de www.redes.unlp.edu.ar.

172.28.0.50

- Servidores de correo del dominio redes.unlp.edu.ar.

172.28.0.29

- Servidores de DNS del dominio redes.unlp.edu.ar.

172.28.0.29

ns-sv-b.redes.unlp.edu.ar

ns-sv-a.redes.unlp.edu.ar

13. ¿Qué función cumple en Linux/Unix el archivo /etc/hosts o en Windows el archivo \WINDOWS\system32\drivers\etc\hosts?

La función que cumplen es mapear nombres de host a direcciones IP locales sin la necesidad de consultar un servidor DNS externo. Originalmente, se utilizaba principalmente para realizar la resolución de nombres de host a direcciones IP en una red antes de la existencia generalizada de servidores DNS.

14. Abra el programa Wireshark para comenzar a capturar el tráfico de red en la interfaz con IP 172.28.0.1. Una vez abierto realice una consulta DNS con el comando dig para averiguar el registro MX de `redes.unlp.edu.ar` y luego, otra para averiguar los registros NS correspondientes al dominio `redes.unlp.edu.ar`. Analice la información proporcionada por dig y compárela con la captura.

15. Dada la siguiente situación: "Una PC en una red determinada, con acceso a Internet, utiliza los servicios de DNS de un servidor de la red". Analice:

a. ¿Qué tipo de consultas (iterativas o recursivas) realiza la PC a su servidor de DNS?

Realiza consultas recursivas a su servidor de DNS.

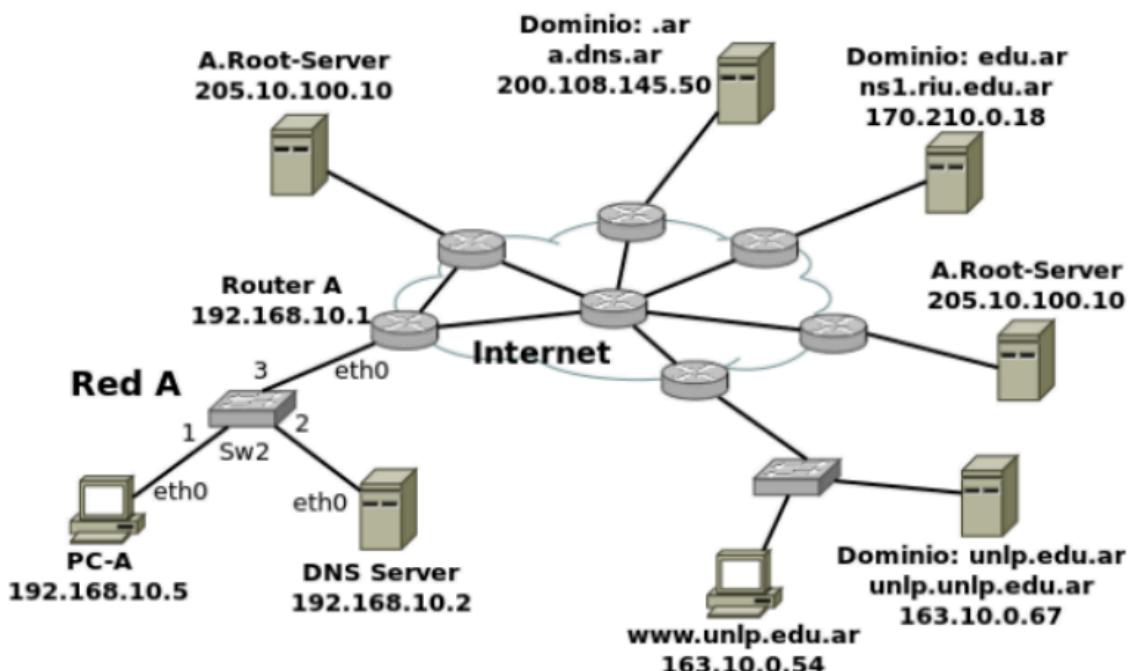
b. ¿Qué tipo de consultas (iterativas o recursivas) realiza el servidor de DNS para resolver requerimientos de usuario como el anterior? ¿A quién le realiza estas consultas?

Realiza consultas iterativas a otros servidores para ir acercándose a la IP deseada.

16. Relacione DNS con HTTP. ¿Se puede navegar si no hay servicio de DNS?

Se podría navegar pero se tornaría difícil y limitado puesto que para acceder a un sitio web se debería conocer la dirección IP.

17. Observar el siguiente gráfico y contestar:



a. Si la PC-A, que usa como servidor de DNS a "DNS Server", desea obtener la IP de `www.unlp.edu.ar`, cuáles serían, y en qué orden, los pasos que se ejecutarán para obtener la respuesta.

b. ¿Dónde es recursiva la consulta? ¿Y dónde iterativa?

1. PC-A (192.168.10.5) consulta primero a su resolver privado sobre la IP del host www.unlp.edu.ar.

2. Si no puede obtener una respuesta (no está cacheada) el resolver primario delega al DNS Server (192.168.10.2).

3. Si este no puede obtenerla de su caché entonces el DNS Server consultará de forma iterativa al A.Root-Server (205.10.100.10) más cercano. Este le responderá (también de forma iterativa) con el NS (y el IP) de .ar, a.dns.ar (200.108.145.50).
4. DNS Server consultara (de forma iterativa) a a.dns.ar.
5. Este le responderá con los NS de .edu.ar, ns1.riu.edu.ar (170.210.0.18)
6. DNS Server consultara a ns1.riu.edu.ar
7. Este le responderá con el NS del servidor autoritativo del dominio unlp.edu.ar, unlp.unlp.edu.ar (163.10.0.67)
8. DNS Server consultará a unlp.unlp.edu.ar que le responderá con la IP de www.unlp.edu.ar (163.10.0.54)
9. El DNS Server cacheará la respuesta y le responderá al resolver de la PC-A con la IP de www.unlp.edu.ar (el resolver también la cacheará)

18. ¿A quién debería consultar para que la respuesta sobre www.google.com sea autoritativa?

Para saber eso se debe hacer dig google.com ns:

@ns1.google.com

19. ¿Qué sucede si al servidor elegido en el paso anterior se lo consulta por www.info.unlp.edu.ar? ¿Y si la consulta es al servidor 8.8.8.8?

Si consulto al servidor elegido en el paso anterior se obtiene el status “Refused” este status quiere decir que el servidor DNS consultado ha denegado explícitamente la solicitud y no proporcionará la información solicitada, en este, porque no la tiene en sus registros la IP de www.info.unlp.edu.ar.

Si consulto a 8.8.8.8 el resultado es un NOERROR.

PRÁCTICA 4 - MAIL

1. ¿Qué protocolos se utilizan para el envío de mails entre el cliente y su servidor de correo? ¿Y entre servidores de correo?

Entre el cliente y su servidor de correo se utilizan SMTP.

Y entre servidores de correo también se utiliza SMTP.

2. ¿Qué protocolos se utilizan para la recepción de mails? Enumere y explique características y diferencias entre las alternativas posibles.

Se utilizan POP o IMAP.

POP3 (Post Office Protocol versión 3):

- **Simplicidad:** POP3 es un protocolo de acceso a correo extremadamente simple. Su simplicidad lo hace fácil de implementar y utilizar.
- **Descarga y Borrado:** POP3 generalmente se configura para descargar los correos electrónicos desde el servidor a la máquina local del usuario. En este modo, los correos se eliminan del servidor después de la descarga (aunque se pueden configurar para mantener una copia en el servidor).
- **No Mantiene Estado:** POP3 no mantiene información de estado entre sesiones. Esto significa que no guarda información sobre carpetas, mensajes marcados o cualquier otra información relacionada con el estado de la cuenta del usuario en el servidor.

- **Limitado para Usuarios Nómadas:** Para usuarios que desean acceder a sus correos electrónicos desde múltiples dispositivos, POP3 puede ser limitante ya que no ofrece una forma sencilla de sincronizar carpetas y correos entre dispositivos.

IMAP (Internet Message Access Protocol):

- **Funcionalidad Avanzada:** IMAP es más avanzado que POP3 y ofrece una amplia gama de funcionalidades. Permite a los usuarios organizar correos electrónicos en carpetas remotas, buscar mensajes, mover mensajes entre carpetas y realizar otras acciones avanzadas.
- **Mantiene Estado:** IMAP mantiene información de estado en el servidor. Esto significa que las carpetas, los mensajes marcados como leídos/no leídos, y otras acciones realizadas en un dispositivo se reflejan en todos los dispositivos conectados, lo que lo hace ideal para usuarios nómadas.
- **Acceso a Partes Componentes de los Mensajes:** IMAP permite a los usuarios acceder a partes específicas de los mensajes, como la cabecera o partes de un mensaje MIME. Esto es útil cuando se necesita descargar solo partes específicas de un mensaje para ahorrar ancho de banda.
- **Complejidad Adicional:** Debido a su mayor funcionalidad, IMAP puede ser más complejo de implementar tanto en el lado del cliente como en el lado del servidor en comparación con POP3.

3. Utilizando la VM y teniendo en cuenta los siguientes datos, abra el cliente de correo (Thunderbird) y configure dos cuentas de correo. Una de las cuentas utilizará POP para solicitar al servidor los mails recibidos para la misma mientras que la otra utilizará IMAP. Al crear cada una de las cuentas, seleccionar Manual config y luego de configurar las mismas según lo indicado, ignorar advertencias por uso de conexión sin cifrado.

- Datos para POP Cuenta de correo: **alumnopop@redes.unlp.edu.ar** Nombre de usuario: **alumnopop** Contraseña: **alumnopopass** Puerto: **110**
- Datos para IMAP Cuenta de correo: **alumnoimap@redes.unlp.edu.ar** Nombre de usuario: **alumnoimap** Contraseña: **alumnoimappass** Puerto: **143**
- Datos comunes para ambas cuentas:

Servidor de correo entrante (POP/IMAP):

- Nombre: **mail.redes.unlp.edu.ar**
- SSL: **None**
- Autenticación: **Normal password**

Servidor de correo saliente (SMTP):

- Nombre: **mail.redes.unlp.edu.ar**
- Puerto: **25**
- SSL: **None**
- Autenticación: **Normal password**

a. Verificar el correcto funcionamiento enviando un email desde el cliente de una cuenta a la otra y luego desde la otra responder el mail hacia la primera.

b. Análisis del protocolo SMTP

- i. Utilizando Wireshark, capture el tráfico de red contra el servidor de correo mientras desde la cuenta **alumnopop@redes.unlp.edu.ar** envía un correo a **alumnoimap@redes.unlp.edu.ar**
- ii. Utilice el filtro SMTP para observar los paquetes del protocolo SMTP en la captura generada y analice el intercambio de dicho protocolo entre el cliente y el

servidor para observar los distintos comandos utilizados y su correspondiente respuesta. Ayuda: filtre por protocolo SMTP y sobre alguna de las líneas del intercambio haga click derecho y seleccione Follow TCP Stream. . .

- c. Usando el cliente de correo Thunderbird del usuario alumnopop@redes.unlp.edu.ar envíe un correo electrónico alumnoimap@redes.unlp.edu.ar el cual debe tener: un asunto, datos en el body y una imagen adjunta.
- i. Verifique las fuentes del correo recibido para entender cómo se utiliza el header “Content-Type: multipart/mixed” para poder realizar el envío de distintos archivos adjuntos.
 - ii. Extraiga la imagen adjunta del mismo modo que lo hace el cliente de correo a partir de las fuentes del mensaje.

4. Análisis del protocolo POP

- a. Utilizando Wireshark, capture el tráfico de red contra el servidor de correo mientras desde la cuenta alumnoimap@redes.unlp.edu.ar le envía una correo a alumnopop@redes.unlp.edu.ar y mientras alumnopop@redes.unlp.edu.ar receptiona dicho correo.

En el envío se observan los protocolos TCP y SMTP, y un SMTP/IMF para el envío del “from: <alumnoimap@redes.unlp.edu.ar>...”.

En la recepción se observan usos del protocolo TCP y POP.

- b. Utilice el filtro POP para observar los paquetes del protocolo POP en la captura generada y analice el intercambio de dicho protocolo entre el cliente y el servidor para observar los distintos comandos utilizados y su correspondiente respuesta.

Comandos:

- **CAPA:** El comando CAPA se utiliza para negociar una capa de seguridad (como SSL/TLS) entre el cliente POP3 y el servidor, lo que permite una conexión segura para el intercambio de correos electrónicos.
- **AUTH PLAIN:** AUTH PLAIN es un comando de autenticación que permite al cliente POP3 enviar su nombre de usuario y contraseña en un formato codificado en base64 para autenticarse en el servidor.
- **STAT:** El comando STAT se utiliza para obtener estadísticas sobre el buzón del usuario, incluyendo el número total de mensajes en el buzón y el tamaño total en octetos.
- **LIST:** El comando LIST se utiliza para obtener una lista de los mensajes en el buzón junto con sus tamaños. También se puede usar para obtener información sobre un mensaje específico proporcionando su número.
- **UIDL:** El comando UIDL se utiliza para obtener una lista de los identificadores únicos de los mensajes en el buzón. Estos identificadores son útiles para realizar un seguimiento de mensajes específicos.
- **RETR:** El comando RETR se utiliza para recuperar un mensaje específico del buzón por su número. Permite al cliente obtener el contenido completo de un mensaje para su lectura.
- **QUIT:** El comando QUIT se utiliza para finalizar una sesión POP3 de manera ordenada. Una vez enviado, el servidor cierra la conexión y el cliente se desconecta.

5. Análisis del protocolo IMAP

a. Utilizando Wireshark, capture el tráfico de red contra el servidor de correo mientras desde la cuenta alumnopop@redes.unlp.edu.ar le envía un correo a alumnoimap@redes.unlp.edu.ar y mientras alumnoimap@redes.unlp.edu.ar receptiona dicho correo.

En el envío se observan los protocolos TCP y SMTP, y un SMTP/IMF para el envío del "from: <alumnopop@redes.unlp.edu.ar>..."

En la recepción se observan usos del protocolo TCP y POP, y un POP/IMF.

b. Utilice el filtro IMAP para observar los paquetes del protocolo IMAP en la captura generada y analice el intercambio de dicho protocolo entre el cliente y el servidor para observar los distintos comandos utilizados y su correspondiente respuesta.

Comandos:

- **DONE**: El comando DONE se utiliza para indicar que se ha completado una transacción abierta en el servidor IMAP. Puede usarse para confirmar la finalización de una secuencia de comandos o una transacción previamente iniciada.

- **CHECK**: El comando CHECK se utiliza para verificar la integridad de una carpeta IMAP y asegurarse de que todos los cambios pendientes se han aplicado correctamente. Es útil para garantizar la coherencia de la información en el servidor IMAP.

- **UID CHECK**: Similar a CHECK, pero se aplica a mensajes específicos identificados por sus identificadores únicos (UID). Permite verificar y sincronizar mensajes específicos en lugar de toda la carpeta.

- **UID FETCH**: El comando UID FETCH se utiliza para recuperar información específica de un mensaje de correo electrónico en una carpeta IMAP, identificándolo mediante su identificador único (UID). Esto permite un acceso preciso a mensajes individuales.

o **UID FETCH 5::** El cliente solicita al servidor que recupere información sobre los mensajes con identificadores únicos (UID) desde el mensaje 5 en adelante.

o **UID FETCH 5 (UID RFC822.SIZE FLAGS BODY.PEEK[]HEADER.FIELDS...):** El cliente solicita información detallada sobre el mensaje con UID 5, incluyendo su tamaño, banderas y encabezado.

o **UID FETCH 5 (UID RFC822.SIZE BODY.PEEK[]):** El cliente solicita el cuerpo completo del mensaje con UID 5.

o **UID FETCH 5 (UID BODY.PEEK[]HEADER.FIELDS...):** El cliente solicita información específica del encabezado del mensaje con UID 5.

- **IDLE**: El comando IDLE permite al cliente IMAP mantener una conexión abierta con el servidor mientras espera notificaciones de nuevos mensajes. Cuando se usa IDLE, el servidor informa inmediatamente al cliente cuando llega un nuevo correo, lo que facilita notificaciones en tiempo real.

- **NOOP**: El comando NOOP (No Operation) es una solicitud simple al servidor IMAP que no realiza ninguna acción significativa. Se utiliza principalmente para mantener una conexión activa sin realizar cambios en el estado de la carpeta o los mensajes. Puede ser útil para mantener la sesión IMAP abierta.

6. IMAP vs POP

a. Marque como leídos todos los correos que tenga en el buzón de entrada de alumnopop y de alumnoimap. Luego, cree una carpeta llamada **POP** en la cuenta de alumnopop y una llamada **IMAP** en la cuenta de alumnoimap. Asegúrese que tiene mails en el **inbox** y en la carpeta recientemente creada en cada una de las cuentas.

b. Cierre la sesión de la máquina virtual del usuario redes e ingrese nuevamente identificándose como usuario root y password packer, ejecute el cliente de correos. De esta forma, iniciará el cliente de correo con el perfil del superusuario (diferente del usuario con el que ya configuró las cuentas antes mencionadas). Luego configure las cuentas POP e IMAP de los usuarios alumnopop y alumnoimap como se describió anteriormente pero desde el cliente de correos ejecutado con el usuario root. Responda:

i. ¿Qué correos ve en el buzón de entrada de ambas cuentas? ¿Están marcados como leídos o como no leídos? ¿Por qué?

En el caso de alumnopop veo los recibidos y están marcados como no leídos.

En el caso de alumnoimap veo los recibidos y los enviados (marcados como leídos).

Con respecto a porque no están marcados como leídos en POP3 los correos electrónicos se descargan del servidor al cliente y se marcan como no leídos en el cliente, mientras que en el protocolo IMAP, los correos se almacenan en el servidor y se reflejan en el cliente. Los correos enviados se consideran leídos porque ya se enviaron desde el cliente. IMAP sincroniza el estado de los correos electrónicos entre el cliente y el servidor.

ii. ¿Qué pasó con las carpetas POP e IMAP que creó en el paso anterior?

La de POP no está pero la de IMAP si. Esto se debe a que POP3 no admite la sincronización de carpetas en el servidor (están localmente), mientras que IMAP permite acceder y sincronizar todas las carpetas en el servidor.

c. En base a lo observado. ¿Qué protocolo le parece mejor? ¿POP o IMAP? ¿Por qué? ¿Qué protocolo considera que utiliza más recursos del servidor? ¿Por qué?

Me parece mejor IMAP ya que almacena los correos en el servidor y los refleja en el cliente, y además sincroniza el estado de los correos electrónicos entre el cliente y el servidor. De esta forma permite que un mismo usuario pueda usar muchos dispositivos de manera más fácil.

POP utiliza menos recursos ya que no mantiene estados, sincronización, carpetas, etc.

7. ¿En algún caso es posible enviar más de un correo durante una misma conexión TCP?

Considera:

- Destinatarios múltiples del mismo dominio entre MUA-MSA y entre MTA-MTA
- Destinatarios múltiples de diferentes dominios entre MUA-MSA y entre MTA-MTA

En ambos casos, entre MUA-MSA si es posible enviar más de un correo durante una misma conexión TCP. Entre MTA-MTA si se trata de destinatarios del mismo dominio se puede enviar en una misma conexión (aunque también podría haber conexiones distintas, verdaderamente depende si el MTA lo permite o cómo está configurado). Si se trata de destinatarios de distintos dominios, siempre va a haber distintas conexiones, porque son dominios separados y responden a distintos servidores.

8. Indique si es posible que el MSA escuche en un puerto TCP diferente a los convencionales y qué implicancias tendría.

Sí, un MSA puede escuchar en un puerto TCP diferente a los convencionales. Hay que tener en cuenta que si se cambia el MSA hay que informar a todos los MUA del dominio que se cambió el puerto del MSA y estos tendrían que configurar el puerto.

9. Indique si es posible que el MTA escuche en un puerto TCP diferente a los convencionales y qué implicancias tendría.

Sí, es posible configurar un MTA para que escuche en un puerto TCP diferente al convencional. Sin embargo, hay que tener en cuenta que si se cambia el MTA se tendría que informar a todos los MTA de los otros dominios de dicho cambio, que a diferencia del cambio de puerto del MSA, es algo prácticamente imposible.

10. Ejercicio integrador HTTP, DNS y MAIL. Suponga que registró bajo su propiedad el dominio redes2024.com.ar y dispone de 4 servidores:

- Un servidor DNS instalado configurado como primario de la zona redes2024.com.ar. (hostname: ns1 - IP: 203.0.113.65).
- Un servidor DNS instalado configurado como secundario de la zona redes2024.com.ar. (hostname: ns2 - IP: 203.0.113.66).
- Un servidor de correo electrónico (hostname: mail - IP: 203.0.113.111). Permitirá a los usuarios enviar y recibir correos a cualquier dominio de Internet.
- Un servidor WEB para el acceso a un webmail (hostname: correo - IP: 203.0.113.8). Permitirá a los usuarios gestionar vía web sus correos electrónicos a través de la URL <https://webmail.redes2024.com.ar>

a. ¿Qué información debería informar al momento del registro para hacer visible a Internet el dominio registrado?

Debería informarle al servidor autoritativo de .com.ar:

- . El NS de los servidores autoritativos del dominio redes2024.com.ar (ns1 y ns2).
- . El A de ambos servidores autoritativos.

b. ¿Qué registros sería necesario configurar en el servidor de nombres? Indique toda la información necesaria del archivo de zona. Puede utilizar la siguiente tabla de referencia (evalúe la necesidad de usar cada caso los siguientes campos): Nombre del registro, Tipo de registro, Prioridad, TTL, Valor del registro.

Sería necesario configurar en el NS los siguientes registros:

- . redes2024.com.ar 86400 IN NS ns1.redes2024.com.ar.
- . redes2024.com.ar 86400 IN NS ns2.redes2024.com.ar.

. redes2024.com.ar 86400 IN MX 5 mail.redes2024.com.ar.

- . ns1.redes2024.com.ar 86400 IN A 203.0.113.65.
- . ns2.redes2024.com.ar 86400 IN A 203.0.113.66.
- . mail.redes2024.com.ar 86400 IN A 203.0.113.111.
- . correo.redes2024.com.ar 86400 IN A 203.0.113.8.

. webmail.redes2024.com.ar 86400 IN CNAME correo.redes2024.com.ar.

. redes2024.com.ar 86400 IN SOA ns1.redes2024.com.ar

root.redes2024.com.ar 2023091300 604800 86400 2419200 86400

c. ¿Es necesario que el servidor de DNS acepte consultas recursivas? Justifique.

No es necesario, porque al ser autoritativo para el dominio redes2024.com.ar no necesitaría resolver la petición consultando a otros servidores. No hay necesidad alguna

de que haga recursión porque es el dueño de los dominios por los que se está consultando. No debe delegar nada.

d. ¿Qué servicios/protocolos de capa de aplicación configuraría en cada servidor?

En los servidores DNS configuraría el protocolo DNS, en el servidor de correo configuraría el SMTP e IMAP y en el servidor web el HTTPS.

e. Para cada servidor, ¿qué puertos considera necesarios dejar abiertos a Internet?. A modo de referencia, para cada puerto indique: servidor, protocolo de transporte y número de puerto.

ns1/ns2 – UDP o TCP (en caso de que la respuesta exceda 512 bytes) – 53

correo – TCP – 80 (http) o 443 (https)

mail – TCP – 25 (SMTP), 110 (POP3) y 143 (IMAP).

f. ¿Cómo cree que se conectaría el webmail del servidor web con el servidor de correo? ¿Qué protocolos usaría y para qué?

El webmail actuaría como MUA, conectándose con el MSA usando el protocolo SMTP para pasarle el mail y que este se lo pase al MTA responsable de conectarse con el MTA receptor (siempre con el protocolo SMTP). Para recibir correos, el webmail utilizaría los protocolos IMAP o POP3 para recuperar los mensajes del servidor de correo, para eso necesitar autenticación. El cliente (las personas) se conectaría al webmail haciendo uso del protocolo HTTP (o HTTPS).

g. ¿Cómo se podría hacer para que cualquier MTA reconozca como válidos los mails provenientes del dominio redes2024.com.ar solamente a los que llegan de la dirección 203.0.113.111? ¿Afectaría esto a los mails enviados desde el Webmail? Justifique.

Se debería configurar en el registro SPF del servidor DNS con el dominio redes2022.com.ar y la dirección 203.0.113.111.

No, esto no afectaría a los mails enviados desde la webmail, ya que esta estaría enviando los mails al MSA y el MSA recibe del MUA y se los pasa al MTA (con ip 203.0.113.111). Este MTA se lo pasará a cualquier otro MTA que reconocerá como válido el mail proveniente de este (ya que tiene la ip que se encuentra en el SPF).

h. ¿Qué característica propia de SMTP, IMAP y POP hace que al adjuntar una imagen o un ejecutable sea necesario aplicar un encoding (ej. base64)?

Fueron diseñados originalmente para el envío de texto plano y caracteres ASCII.

i. ¿Se podría enviar un mail a un usuario de modo que el receptor vea que el remitente es un usuario distinto? En caso afirmativo, ¿Cómo? ¿Es una indicación de una estafa? Justifique

Si, se podría cambiando el encabezado "From", ya que los protocolos de correo electrónico, como SMTP, no tienen un mecanismo integrado para verificar si la dirección del remitente es realmente quien dice ser. En la actualidad existen certificados digitales que ayudan a mitigar la suplantación de identidad en el correo electrónico y en otras comunicaciones en línea.

j. ¿Se podría enviar un mail a un usuario de modo que el receptor vea que el destinatario es un usuario distinto? En caso afirmativo, ¿Cómo? ¿Por qué no le llegaría al destinatario que el receptor ve? ¿Es esto una indicación de una estafa? Justifique
No es posible enviar un correo electrónico de modo que el receptor vea que el destinatario es un usuario distinto. En los protocolos de correo electrónico como SMTP el encabezado "To" para indicar quién es el destinatario real del mensaje, y esta información no puede ser falsificada en el nivel del remitente de manera que el receptor vea otro destinatario. Si no le llegaría al destinatario que el receptor ve, esto podría ser un problema técnico, no una indicación de una estafa (ya que el encabezado "To" no se puede modificar).

k. ¿Qué protocolo usará nuestro MUA para enviar un correo con remitente redes@info.unlp.edu.ar? ¿Con quién se conectará? ¿Qué información será necesaria y cómo la obtendría?

Usará el protocolo SMTP. Se conectará con el MSA. El MUA debe conocer el puerto SMTP que se utilizará para la comunicación con el MSA. El puerto estándar para la comunicación con el MSA en la mayoría de los casos es el puerto 587 (SMTP Submission), pero también se podría usar el puerto 25 (SMTP) si está configurado de esa manera (u otro si no es ninguno de esos). Además necesita la dirección IP del servidor de correo saliente, para ello debe hacer una consulta DNS por el registro A del servidor de correo saliente de info.unlp.edu.ar.

l. Dado que solo disponemos de un servidor de correo, ¿qué sucederá con los mails que intenten ingresar durante un reinicio del servidor?

El servidor de correo local los encolara hasta que puedan ser enviados.

m. Suponga que contratamos un servidor de correo electrónico en la nube para integrarlo con nuestra arquitectura de servicios.

i. ¿Cómo configurar el DNS para que ambos servidores de correo se comporten de manera de dar un servicio de correo tolerante a fallos?

Debería agregar otro registro MX y A de tal manera que quede:

redes2022.com.ar 86400 IN MX 10 nube.redes2022.com.ar
nube.redes2022.com.ar 86400 IN A IP

Si se cae el servidor de correo con mayor prioridad (5) se enviarán a este servidor en la nube.

11. Utilizando la herramienta Swaks envíe un correo electrónico con las siguientes características:

- Dirección destino: Dirección de correo de alumnoimap@redes.unlp.edu.ar
- Dirección origen: redesycomunicaciones@redes.unlp.edu.ar
- Asunto: SMTP-Práctica4
- Archivo adjunto: PDF del enunciado de la práctica
- Cuerpo del mensaje: Esto es una prueba del protocolo SMTP

a. Analice tanto la salida del comando swaks como los fuentes del mensaje recibido para responder las siguientes preguntas:

i. ¿A qué corresponde la información enviada por el servidor destino como respuesta al comando EHLO? Elija dos de las opciones del listado e investigue la funcionalidad de la misma.

La información enviada por el servidor destino como respuesta al comando EHLO corresponde a las capacidades y extensiones soportadas por el servidor de correo. STARTTLS: Esta extensión indica que el servidor de correo es compatible con la encriptación TLS.

CHUNKING: Esta extensión indica que el servidor de correo permite la transmisión eficiente y segura de correos electrónicos en fragmentos más pequeños

ii. Indicar cuáles cabeceras fueron agregadas por la herramienta swaks.

Date: Wed, 13 Sep 2023 12:58:47 -0300

To: alumnoimap@redes.unlp.edu.ar

From: redesycomunicaciones@redes.unlp.edu.ar

Subject: SMTP-Practica4

Message-Id: <20230913125847.005385@debian>

X-Mailer: swaks v20201014.0 jetmore.org/john/code/swaks/

MIME-Version: 1.0

Content-Type: multipart/mixed;

boundary="----=_MIME_BOUNDARY_000_5385"

iii. ¿Cuál es el message-id del correo enviado? ¿Quién asigna dicho valor?

<20230913125847.005385@debian>

Lo agrega el MUA, pero si falta lo agrega el MSA.

iv. ¿Cuál es el software utilizado como servidor de correo electrónico?

Postfix es el servidor de correo electrónico que está siendo utilizado en la dirección "mail.redes.unlp.edu.ar" con la versión "Lihuen-4.01/GNU".

v. Adjunte la salida del comando swaks y los fuentes del correo electrónico.

```
Return-Path: <redesycomunicaciones@redes.unlp.edu.ar>
X-Original-To: alumnoimap@redes.unlp.edu.ar
Delivered-To: alumnoimap@redes.unlp.edu.ar
Received: from debian (unknown [172.28.0.1])
    by mail.redes.unlp.edu.ar (Postfix) with ESMTP id CA6E860169
    for <alumnoimap@redes.unlp.edu.ar>; Wed, 13 Sep 2023 15:58:52 +0000 (UTC)
Date: Wed, 13 Sep 2023 12:58:47 -0300
To: alumnoimap@redes.unlp.edu.ar
From: redesycomunicaciones@redes.unlp.edu.ar
Subject: SMTP-Practica4
Message-Id: <20230913125847.005385@debian>
X-Mailer: swaks v20201014.0 jetmore.org/john/code/swaks/
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="----=_MIME_BOUNDARY_000_5385"

-----=_MIME_BOUNDARY_000_5385
Content-Type: text/plain
```

Esto es una prueba del protocolo SMTP

```
-----=_MIME_BOUNDARY_000_5385
Content-Type: application/octet-stream; name="p04.pdf"
Content-Description: p04.pdf
Content-Disposition: attachment; filename="p04.pdf"
Content-Transfer-Encoding: BASE64
```

```
JVBERI0xLjUKJdDUxdgKNiAwIG9iago8PC9MZW5ndGggMTYwMCAgICAgIC9GaWx0ZXIxRmxhdGVE
ZWNVZGU+PgpzdHJLYW0KeNqtWNtu20YQfddX8JEcms3e15uX1E2TokGd0rVToIjzQJ005oAiFv6c
uF/f2ZtESrIkI4IB7212dubsnNmhcLSIcPTb7jeb2ct3jEU0lKyJLq5jwgsYPivMEqkjJTQKGE6
ullGn+M36Sadv6AqifPCtRerqszSrLxlktVmSsUv3Mqbpm2LxvwLqsi6lsqUGcwRKZiM/vryonMC
```

b. Descargue de la plataforma la captura de tráfico smtp.pcap y la salida del comando swaks smtp.swaks para responder y justificar los siguientes ejercicios.

i. ¿Por qué el contenido del mail no puede ser leído en la captura de tráfico?

Porque esta encriptado ya que se usó el comando STARTTLS para comenzar una comunicación encriptada usando TLS.

c. Realice una consulta de DNS por registros TXT al dominio info.unlp.edu.ar y entre dichos registros evalúe la información del registro SPF. ¿Por qué cree que aparecen muchos servidores autorizados?

El registro SPF determina qué servidores de correo y dominios tienen permitido enviar correo en nombre de un dominio. Aparecen muchos servidores autorizados porque son los distintos servidores y dominios de la facultad de informática.

Se utiliza "a:" para autorizar servidores por nombres de host, debes asegurarte de que estos nombres de host se resuelvan a direcciones IP correctas y actualizadas.

d. Realice una consulta de DNS por registros TXT al dominio outlook.com y analice el registro correspondiente a SPF. ¿Cuáles son los bloques de red autorizados para enviar mails?. Investigue para qué se utiliza la directiva "~all"

include:

spf-a.outlook.com

spf-b.outlook.com

spf.protection.outlook.com

spf-a.hotmail.com

_spf-ssg-b.microsoft.com

_spf-ssg-c.microsoft.com

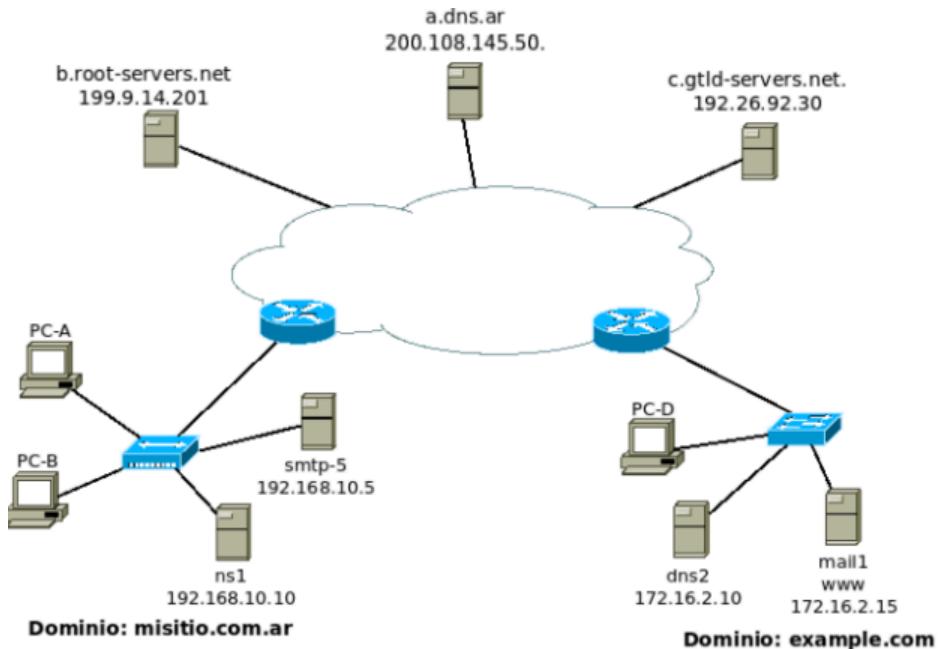
ip4: 157.55.9.128/25

"include" permiten especificar dominios o registros SPF externos que deben ser considerados como parte de la política SPF actual. Esto significa que los servidores autorizados para enviar correos en nombre del dominio se toman de esos registros externos.

Esto significa que los servidores autorizados para enviar correos en nombre de outlook.com se definen en los registros SPF de spfa.outlook.com y spf-b.outlook.com. En lugar de enumerar todas las direcciones IP y servidores en el registro SPF de outlook.com, simplemente se hace referencia a estos registros externos para simplificar y mantener actualizada la política SPF.

"all" especifica una "falla suave" en la política SPF. Esto significa que, si el correo no proviene de ninguna de las fuentes autorizadas mencionadas anteriormente en la política SPF, el correo no se rechazará automáticamente, pero podría ser marcado como sospechoso o marcado de alguna otra manera por el destinatario.

12. Observar el gráfico a continuación y teniendo en cuenta lo siguiente , responder:



- El usuario juan@misitio.com.ar en PC-A desea enviar un mail al usuario alicia@example.com
- Cada organización tiene su propios servidores de DNS y Mail
- El servidor ns1 de misitio.com.ar no tiene la recursión habilitada

a. El servidor de mail, mail1, y de HTTP, www, de example.com tienen la misma IP, ¿es posible esto? Si lo es, ¿cómo lo resolvería?

Si, es posible esto. Para que esto funcione correctamente, se debe asegurar que el servidor de correo y el servidor web estén configurados para escuchar en puertos diferentes. El protocolo SMTP se utiliza para el correo electrónico y generalmente se ejecuta en el puerto 25 o el puerto 587, mientras que HTTP utiliza el puerto 80 o el puerto 443 para conexiones seguras (HTTPS).

b. Al enviar el mail, ¿por cuál registro de DNS consultará el MUA?

El MUA en caso de tener configurado el nombre del servidor de correo electrónico saliente deberá hacer una consulta sobre el registro A para poder saber la dirección IP correspondiente a ese nombre de dominio, en caso de tener configurada la IP no va a necesitar realizar ninguna consulta.

c. Una vez que el mail fue recibido por el servidor smtp-5, ¿por qué registro de DNS consultará?

Este consultará el registro MX del dominio receptor (example.com).

d. Si en el punto anterior smtp-5 recibiese un listado de nombres de servidores de correo, ¿será necesario realizar una consulta de DNS adicional? Si es afirmativo, ¿por qué tipo de registro y de cuál servidor preguntaría?

Si, sería necesario para obtener la IP de los nombres de servidores dados. Deberá preguntar por el registro A (siguiendo la prioridad).

e. Indicar todo el proceso que deberá realizar el servidor ns1 de misitio.com.ar para obtener los servidores de mail de example.com.

El servidor DNS ns1 actúa como servidor DNS y realiza las consultas necesarias en nombre de SMTP-5:

1. Consultará al root server más cercano (b.root-servers.net) y este proporcionará la dirección IP de un servidor DNS autoritativo para .com (c.gtld-servers.net)
2. Consultará con el servidor autoritativo de .com y este proporcionará la dirección IP de un servidor DNS autoritativo para example.com.
3. ns1 consultará al servidor DNS autoritativo de example.com para obtener los registros MX específicos que indican los servidores de correo asociados con example.com.

f. Teniendo en cuenta el proceso de encapsulación/desencapsulación y definición de protocolos, responder V o F y justificar:

- Los datos de la cabecera de SMTP deben ser analizados por el servidor DNS para responder a la consulta de los registros MX

FALSO → Los datos de la cabecera de SMTP deben ser analizados por el MSA para determinar si hay algún campo faltante que debe ser completado. El servidor DNS no debe analizar los datos de la cabecera para responder a la consulta de los registros MX. Simplemente responde la consulta sin analizarlos.

- Al ser recibidos por el servidor smtp-5 los datos agregados por el protocolo SMTP serán analizados por cada una de las capas inferiores.

FALSO → En el modelo de capas de protocolo, cada capa es responsable de procesar y encapsular los datos antes de pasarlo a la capa inferior, por lo que no son analizados por las capas inferiores.

- Cada protocolo de la capa de aplicación agrega una cabecera con información propia de ese protocolo.

?

- Como son todos protocolos de la capa de aplicación, las cabeceras agregadas por el protocolo de DNS pueden ser analizadas y comprendidas por el protocolo SMTP o HTTP

FALSO → Los protocolos son independientes del resto. Cada protocolo de aplicación tiene su propia estructura de datos y cabeceras, y no están necesariamente diseñados para interoperar entre sí de manera directa.

- Para que los clientes en misitio.com.ar puedan acceder al servidor HTTP www.example.com y mostrar correctamente su contenido deben tener el mismo sistema operativo.

FALSO → el protocolo HTTP provee la abstracción necesaria para que clientes que distintos sistemas operativos puedan acceder al mismo contenido sin problemas.

- Un cliente web que desea acceder al servidor www.example.com y que no pertenece a ninguno de estos dos dominios puede usar a ns1 de misitio.com.ar como servidor de DNS para resolver la consulta.

FALSO → No, ya que el ns1 no es un servidor autoritativo de www.example.com, no lo va a tener en ningun registro y como www.example.com no es un subdominio de misitio.com.ar no va a poder delegar a otra zona. A su vez, ns1 no hace consultas recursivas fuera de misitio.com.ar (algo que se aclara en el enunciado). Si se tratara de un cliente web perteneciente al dominio, si podría usarlo como servidor de DNS para resolver la consulta.

h. Cuando Alicia quiera ver sus mails desde PC-D, ¿qué registro de DNS deberá consultarse?

Ninguno. Es un protocolo distinto. Para ver el mail desde PC-D utilizara el protocolo POP3 o IMAP. DNS es un protocolo distinto para resolver nombres de dominios a IPs. El software de correo electrónico en PC-D se comunicaría directamente con el servidor de correo utilizando la dirección IP o el nombre de dominio previamente resuelto durante el proceso de configuración

i. Indicar todos los protocolos de mail involucrados, puerto y si usan TCP o UDP, en el envío y recepción de dicho mail.

Protocolos SMTP (25) para envío y POP3 (110) o IMAP (143) para recepción. Todos estos utilizan TCP.

PRÁCTICA 5 - CAPA DE TRANSPORTE I

1. ¿Cuál es la función de la capa de transporte?

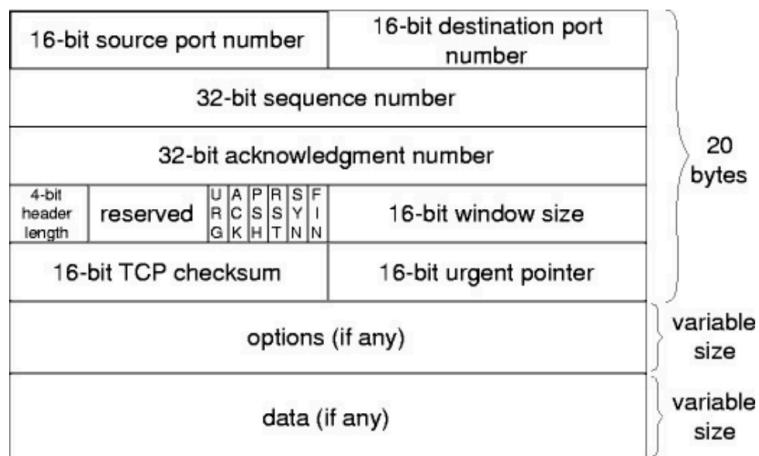
La función de la capa de transporte es gestionar la transmisión de mensajes o datos a través de una red, asegurándose de que lleguen de manera correcta y en el orden adecuado. Es decir, garantiza la entrega confiable de datos entre sistemas finales. Además, brinda servicio a la capa de aplicación y usa servicios de la capa de internet. Y realiza la encapsulación, donde define PDU donde se envían los mensajes de la aplicación. Proporciona, entonces, una comunicación lógica entre procesos de aplicación que se ejecutan en dispositivos diferentes dentro de una red. Esta comunicación lógica permite que los procesos de aplicación se envíen mensajes entre sí sin preocuparse por los detalles de la infraestructura física subyacente.

2. Describa la estructura del segmento TCP y UDP.

. TCP:

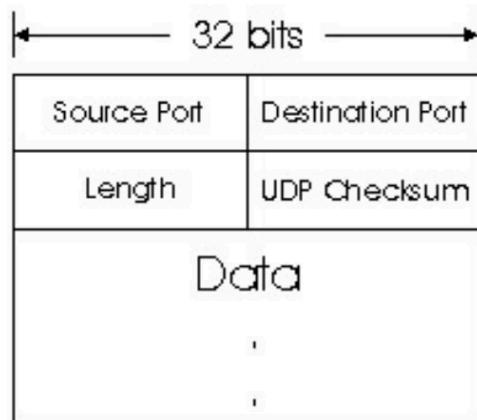
- Puertos: MUX/DEMUX.
- No tiene Longitud total, si de HDR LEN (variable, max 60B Unit=4B).
- Total LEN se computa para PseudoHDR, no viaja en el segmento.
- El tamaño del segmento se calcula dentro del datagrama IP.
- Checksum:
 - Cálculo Ca1. Obligatorio, calculado, igual que UDP.
 - Si tiene error podría pedir retransmisión, implementación de TCP descarta y espera RTO (Retransmisión Timer).
- Necesidad de manejar Timers, RTO (tmout. por cada segmento). (implementaciones lo manejan más eficientemente).
- Campos de Sesiones: Flags: SYN(Synchronize), FIN(Finish), RST (Reset).
- Campo de Detección de Errores: Checksum.

- Campos de Control de Errores: ACK, Num. Sec (#Seq), Num. Ack (#Ack).
- Campo de Control de Flujo: a los de control de errores se agrega, Win.
- Campos de Control de Congestión: se agregan flags si participa la red.



. UDP:

- Puertos: MUX/DEMUX.
- Longitud: UDP HDR + Payload.
- Checksum:
 - Cálculo Ca1, Opcional. 0 = Sin checksum.
 - Calculado HDR + PseudoHDR + Payload.
 - PseudoHDR: IP.SRC + IP.DST + Zero + IP.PROTO + UDP.LENGTH.
 - PseudoHDR: protección contra paquetes mal enrutados.
 - Aplicaciones de LAN por eficiencia lo podrían deshabilitar.
 - Si tiene error se descarta silenciosamente.



3. ¿Cuál es el objetivo del uso de puertos en el modelo TCP/IP?

Se utilizan para distinguir las aplicaciones (y, por lo tanto, protocolos) que están enviando/recibiendo datos. Los puertos actúan como puntos finales en una comunicación y permiten que múltiples aplicaciones en una misma computadora o dispositivo se comuniquen simultáneamente a través de la red.

4. Compare TCP y UDP en cuanto a:

a. Confiabilidad

TCP: Es un modelo confiable ya que garantiza que los datos se entreguen en el orden correcto y sin errores a través de técnicas como la retransmisión de datos perdidos y la detección y corrección de errores utilizando sumas de verificación.

UDP: es menos confiable en comparación con TCP. No garantiza la entrega de datos ni el orden de entrega. Los segmentos UDP pueden perderse o llegar desordenados sin corrección automática.

b. Multiplexación.

TCP: Multiplexación y demultiplexación orientada a la conexión. El socket TCP queda identificado por una tupla de cuatro elementos: dirección IP de origen, número de puerto de origen, dirección IP de destino, número de puerto de destino. Por lo tanto, cuando un segmento TCP llega a un host procedente de la red, el host emplea los cuatro valores para dirigir (demultiplexar) el segmento al socket apropiado.

UDP: Multiplexación y demultiplexación sin conexión. El socket UDP queda completamente identificado por una tupla que consta de una dirección IP de destino y un número de puerto de destino. En consecuencia, si dos segmentos UDP tienen diferentes direcciones IP y/o números de puerto de origen, pero la misma dirección IP de destino y el mismo número puerto de destino, entonces los dos segmentos se enviarán al mismo proceso de destino a través del mismo socket de destino.

c. Orientado a la conexión.

TCP: Establece una conexión antes de la transmisión de datos y asegura que ambas partes estén sincronizadas en términos de secuencia de datos y control de flujo.

UDP: No se necesita conexión para iniciar y finalizar una transferencia de datos

d. Controles de congestión.

TCP: Proporciona mecanismos de control de congestión. Los mecanismos de control de congestión de TCP evitan que cualquier conexión TCP inunde con una cantidad de tráfico excesiva los enlaces y routers existentes entre los hosts que están comunicándose. Esto se consigue regulando la velocidad a la que los lados emisores de las conexiones TCP pueden enviar tráfico a la red.

Posee un mecanismo que indica al emisor cuánto espacio libre hay en el búfer de almacenamiento del receptor (ventana de recepción). Ayuda a controlar el flujo de datos para evitar la congestión y garantizar una comunicación eficiente, permitiendo que el emisor ajuste la cantidad de datos enviados en función de la capacidad disponible en el receptor.

UDP: El tráfico UDP no está regulado. Una aplicación que emplee el protocolo de transporte UDP puede enviar los datos a la velocidad que le parezca, durante todo el tiempo que quiera.

e. Utilización de puertos.

TCP: Como está orientado a la conexión, establece una conexión punto a punto entre dos dispositivos, por lo que cada conexión está limitada a dos procesos que intercambian datos.

Utiliza números de puerto para identificar aplicaciones específicas.

UDP: Permite que muchos clientes o procesos envíen datos por el mismo socket.

Utiliza números de puerto para identificar aplicaciones específicas.

5. La PDU de la capa de transporte es el segmento. Sin embargo, en algunos contextos suele utilizarse el término datagrama. Indique cuando.

Cuando se trata del protocolo UDP, el término datagrama se utiliza para su PDU.

6. Describa el saludo de tres vías de TCP. ¿UDP tiene esta característica?

También conocido como protocolo de enlace de TCP, es un método utilizado por TCP para establecer una conexión confiable entre dos dispositivos en una red. Es un método de tres pasos que requiere que tanto el cliente como el servidor intercambien segmentos SYN y ACK antes de que comience la comunicación de datos real.

Paso 1 (SYN) – El cliente inicia el proceso enviando un segmento al servidor con el bit SYN establecido y un número de secuencia inicial (ISN) generado de manera pseudoaleatoria. Este es importante para identificar y ordenar los datos en la conexión.

Paso 2 (SYN/ACK) – El servidor recibe el segmento del cliente, reconoce el bit SYN y responde enviando un segmento de respuesta con los bits SYN y ACK establecidos. En este, el servidor incluye su propio número de secuencia inicial (ISN), que también es elegido de manera pseudoaleatoria. El servidor también reconoce el ISN del cliente, lo que indica que ha recibido correctamente el paquete de solicitud de conexión.

Paso 3 (ACK) – El cliente recibe la respuesta del servidor, reconociendo el ISN del servidor. El cliente responde enviando un segmento de confirmación con el bit ACK establecido, confirmando que ha recibido correctamente la respuesta del servidor. Ambos establecen una conexión confiable con la cual iniciarán la transferencia de datos real.

En UDP no se utiliza nada similar ya no se establece ninguna conexión

7. Investigue qué es el ISN (Initial Sequence Number). Relacionelo con el saludo de tres vías.

Initial Sequence Number (ISN) se refiere al número de secuencia único de 32 bits asignado a cada nueva conexión en una comunicación TCP. Ayuda a que no entren en conflicto los bytes de datos transmitidos a través de una conexión TCP. Un ISN es único para cada conexión y está separado por cada dispositivo. Para el ISN se utiliza un contador que se incrementa cada 4 mseg.

El ISN ayuda a identificar, controlar el origen y mantener el orden de los segmentos de datos transmitidos entre el cliente y el servidor.

8. Investigue qué es el MSS. ¿Cuándo y cómo se negocia?

El tamaño de la ventana de recepción TCP es la cantidad de datos de recepción (en bytes) que se pueden almacenar en búfer durante una conexión. En lugar de usar un tamaño de ventana de recepción predeterminado codificado de forma rígida, TCP se ajusta a incrementos pares del tamaño máximo de segmento (MSS).

Maximum Segment Size es un campo de los encabezados que indica el tamaño más grande de datos que puede tener un segmento sin ser fragmentado. El MSS mide la parte de un paquete que no tiene encabezado, lo que se conoce como carga útil. El MSS está determinado por otra métrica que tiene que ver con el tamaño de los paquetes: MTU, o la

unidad máxima de transmisión, que sí incluye los encabezados TCP e IP (Protocolo de Internet).

El MSS es igual a la MTU menos el tamaño de un encabezado TCP y un encabezado IP:
MTU - (encabezado TCP + encabezado IP) = MSS

Una de las principales diferencias entre la MTU y el MSS es que si un paquete supera la MTU de un dispositivo, se divide en trozos más pequeños, o "se fragmenta." En cambio, si un paquete supera el MSS, se descarta y no se entrega.

El MSS se negocia durante la configuración de la conexión, es decir, durante el saludo de tres vías.

9. Utilice el comando *ss* (reemplazo de *netstat*) para obtener la siguiente información de su PC:

- a. Para listar las comunicaciones TCP establecidas.
- b. Para listar las comunicaciones UDP establecidas.
- c. Obtener sólo los servicios TCP que están esperando comunicaciones
- d. Obtener sólo los servicios UDP que están esperando comunicaciones.
- e. Repetir los anteriores para visualizar el proceso del sistema asociado a la conexión.
- f. Obtenga la misma información planteada en los ítems anteriores usando el comando *netstat*.

10. ¿Qué sucede si llega un segmento TCP con el flag SYN activo a un host que no tiene ningún proceso esperando en el puerto destino de dicho segmento (es decir, el puerto destino no está en estado LISTEN)?

Si no hay proceso en estado LISTEN en el puerto destino, el host enviará un segmento con la flag RST (reset) activado para indicar que la conexión no se puede establecer en dicho puerto. De esta manera informará al remitente que no hay no se puede establecer la conexión en ese momento para que no siga enviando segmentos.

- a. Utilice *hping3* para enviar paquetes TCP al puerto destino 22 de la máquina virtual con el flag SYN activado.
- b. Utilice *hping3* para enviar paquetes TCP al puerto destino 40 de la máquina virtual con el flag SYN activado.

c. ¿Qué diferencias nota en las respuestas obtenidas en los dos casos anteriores?

¿Puede explicar a qué se debe? (Ayuda: utilice el comando *ss* visto anteriormente).

En el puerto 22 se tiene el flag SA , que corresponde a cuando el puerto destino está abierto, es decir, los flags SYN/ACK están activados y se pudo establecer la comunicación. Por su parte, en el 40 se tiene el flag RA, que corresponde a cuando el puerto destino está cerrado, es decir RST/ACK están activados y no se pudo establecer la comunicación.

11. ¿Qué sucede si llega un datagrama UDP a un host que no tiene ningún proceso esperando en el puerto destino de dicho datagrama (es decir, que dicho puerto no está en estado LISTEN)?

Si no hay proceso en estado LISTEN en el puerto destino se responderá con un ICMP "Destination Unreachable" (esto es otro protocolo de IP). Este mensaje ICMP indica que el puerto o el host destino no están disponibles. Sin embargo, este paquete ICMP se puede perder y UDP no generará ninguna notificación al remitente ya que se trata de un protocolo sin conexión y no confiable.

- a. Utilice hping3 para enviar datagramas UDP al puerto destino 5353 de la máquina virtual.
- b. Utilice hping3 para enviar datagramas UDP al puerto destino 40 de la máquina virtual.
- c. ¿Qué diferencias nota en las respuestas obtenidas en los dos casos anteriores?
¿Puede explicar a qué se debe? (Ayuda: utilice el comando ss visto anteriormente).
La diferencia en este caso es que en el puerto 5353 hay un proceso escuchando (igualmente no se indica que el datagrama llegó y eso es razonable ya que se trata del protocolo UDP) y en el 40 no. En el caso del puerto 40, se envía un ICMP que indica que el puerto es inalcanzable. Se puede ver mediante este comando que en el puerto 5353 hay un proceso activo.

12. Investigue los distintos tipos de estado que puede tener una conexión TCP. Ver https://users.cs.northwestern.edu/~agupta/cs340/project2/TCP/IP_State_Transition_Diagram.pdf

Una conexión atraviesa una serie de estados a lo largo de su ciclo de vida. Estos estados incluyen: LISTEN, SYN-SENT, SYN-RECEIVED, ESTABLISHED, FIN-WAIT-1, FIN-WAIT-2, CLOSE-WAIT, CLOSING, LASTACK, TIME-WAIT y el estado ficticio CLOSED. El estado CLOSED es ficticio porque representa la situación en la que no existe un Bloque de Control de Transmisión (TCB), lo que significa que no hay conexión alguna. Para resumir, estos estados tienen los siguientes significados:

LISTEN representa la espera de una solicitud de conexión procedente de cualquier TCP remoto y puerto.

SYN-SENT representa la espera de una solicitud de conexión coincidente después de haber enviado una solicitud de conexión.

SYN-RECEIVED representa la espera de una confirmación de solicitud de conexión después de haber recibido y enviado una solicitud de conexión.

ESTABLISHED representa una conexión abierta, lo que permite que los datos recibidos sean entregados al usuario. Es el estado normal durante la fase de transferencia de datos de la conexión.

FIN-WAIT-1 representa la espera de una solicitud de terminación de conexión procedente del TCP remoto, o la confirmación de la solicitud de terminación de conexión previamente enviada.

FIN-WAIT-2 representa la espera de una solicitud de terminación de conexión procedente del TCP remoto.

CLOSE-WAIT representa la espera de una solicitud de terminación de conexión procedente del usuario local.

CLOSING representa la espera de una confirmación de la solicitud de terminación de conexión procedente del TCP remoto.

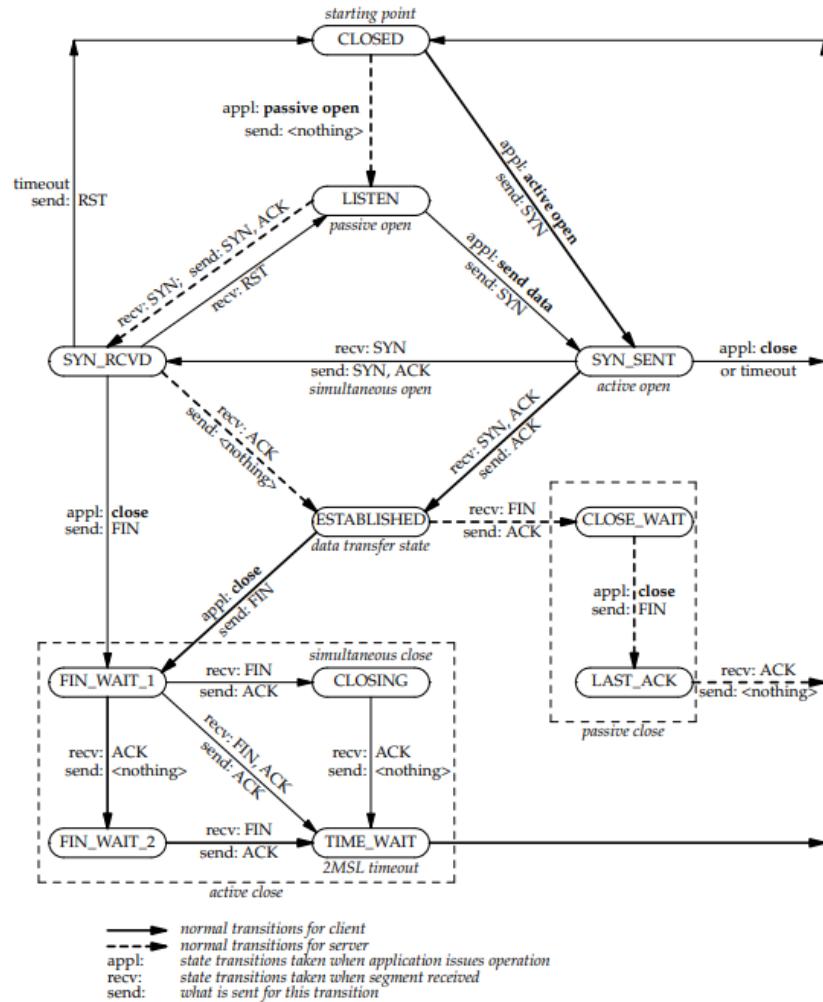
LAST-ACK representa la espera de una confirmación de la solicitud de terminación de conexión previamente enviada al TCP remoto (la cual incluye una confirmación de su solicitud de terminación de conexión).

TIME-WAIT representa la espera de suficiente tiempo para asegurar que el TCP remoto ha recibido la confirmación de su solicitud de terminación de conexión.

CLOSED representa la ausencia total de una conexión activa.

Una conexión TCP avanza de un estado a otro en respuesta a diversos eventos, tales como llamadas del usuario (OPEN, SEND, RECEIVE, CLOSE, ABORT y STATUS), segmentos

entrantes, especialmente aquellos que contienen las banderas SYN, ACK, RST y FIN, así como también mediante el uso de temporizadores."



TCP state transition diagram.

13. Dada la siguiente salida del comando ss, responda:

Netid	State	Recv-Q	Send-Q	Local Address:Port	Peer Address:Port	Process
tcp	LISTEN	0	128	*:22	*:*	users:(("sshd",pid=468,fd=29))
tcp	LISTEN	0	128	*:80	*:*	users:(("apache2",pid=991,fd=95))
udp	LISTEN	0	128	163.10.5.222:53	*:*	users:(("named",pid=452,fd=10))
tcp	ESTAB	0	0	163.10.5.222:59736	64.233.163.120:443	users:(("x-www-browser",pid=1079,fd=51))
tcp	CLOSE-WAI	T 0	0	163.10.5.222:41654	200.115.89.30:443	users:(("x-www-browser",pid=50))
tcp	ESTAB	0	0	163.10.5.222:59737	64.233.163.120:443	users:(("x-www-browser",pid=1079,fd=55))
tcp	ESTAB	0	0	163.10.5.222:33583	200.115.89.15:443	users:(("x-www-browser",pid=1079,fd=53))
tcp	ESTAB	0	0	163.10.5.222:45293	64.233.190.99:443	users:(("x-www-browser",pid=1079,fd=59))
tcp	LISTEN	0	128	*:25	*:*	users:(("postfix",pid=627,fd=3))
tcp	ESTAB	0	0	127.0.0.1:22	127.0.0.1:41220	users:(("sshd",pid=1418,fd=3), ("sshd",pid=1416,fd=3))
tcp	ESTAB	0	0	163.10.5.222:52952	64.233.190.94:443	users:(("x-www-browser",pid=1079,fd=29))
tcp	TIME-WAIT	0	0	163.10.5.222:36676	54.149.207.17:443	users:(("x-www-browser",pid=1079,fd=3))
tcp	ESTAB	0	0	163.10.5.222:52960	64.233.190.94:443	users:(("x-www-browser",pid=1079,fd=67))
tcp	ESTAB	0	0	163.10.5.222:50521	200.115.89.57:443	users:(("x-www-browser",pid=1079,fd=69))
tcp	SYN-SENT	0	0	163.10.5.222:52132	43.232.2.2:9500	users:(("x-www-browser",pid=1079,fd=70))
tcp	ESTAB	0	0	127.0.0.1:41220	127.0.0.1:22	users:(("ssh",pid=1415,fd=3))
udp	LISTEN	0	128	127.0.0.1:53	*:*	users:(("named",pid=452,fd=9))

a. ¿Cuántas conexiones hay establecidas?

Hay 9 (ESTAB)

b. ¿Cuántos puertos hay abiertos a la espera de posibles nuevas conexiones?

Hay 5 (LISTEN)

c. El cliente y el servidor de las comunicaciones HTTPS (puerto 443), ¿residen en la misma máquina?

No, deberían coincidir las IPS.

d. El cliente y el servidor de la comunicación SSH (puerto 22), ¿residen en la misma máquina?

Si, tanto la IP Local como la Destino son la misma. Una esta en el puerto 22 y la otra en el 41220. En el puerto 22 está el proceso SSHD, y en el 41220 está corriendo el proceso SSH.

e. Liste los nombres de todos los procesos asociados con cada comunicación. Indique para cada uno si se trata de un proceso cliente o uno servidor.

Los que están en estado LISTEN y/o en puertos del 0 al 1023 son procesos servidores.

- SSHD: Servidor
- APACHE2: Servidor
- NAMED: Servidor
- X-WWW-BROWSER: Cliente
- POSTFIX: Servidor
- SSH: Cliente

f. ¿Cuáles conexiones tuvieron el cierre iniciado por el host local y cuáles por el remoto?

TIME-WAIT Por el local, CLOSE-WAIT por el remoto

g. ¿Cuántas conexiones están aún pendientes por establecerse?

Hay 1 (SYN-SENT).

14. Dadas las salidas de los siguientes comandos ejecutados en el cliente y el servidor, responder:

```
servidor# ss -natu | grep 110
tcp      LISTEN  0  0                           *:110                  *:*
tcp      SYN-RECV     0  0             157.0.0.1:110  157.0.11.1:52843
```

```
cliente# ss -natu | grep 110
tcp      SYN-SENT     0  1           157.0.11.1:52843        157.0.0.1:110
```

a. ¿Qué segmentos llegaron y cuáles se están perdiendo en la red?

SYN llegó al servidor, pero SYNACK no llegó al cliente.

b. ¿A qué protocolo de capa de aplicación y de transporte se está intentando conectar el cliente?

Al protocolo POP3 de la capa de aplicación con el protocolo TCP

c. ¿Qué flags tendría seteado el segmento perdido?

SYN: 1 ACK: 1

PRACTICA 6 - CAPA DE TRANSPORTE II

1. ¿Cuál es el puerto por defecto que se utiliza en los siguientes servicios? Web / SSH / DNS / Web Seguro / POP3 / IMAP / SMTP Investigue en qué lugar en Linux y en Windows está descrita la asociación utilizada por defecto para cada servicio.

Servicio	Puerto por defecto
Web	80 (HTTP)
SSH	22
DNS	53
Web Seguro	443 (HTTPS)
POP3	110
IMAP	143

En Linux, la asociación de puertos por defecto para los servicios se encuentra en el archivo /etc/services. Este archivo es un archivo de texto que contiene una lista de servicios registrados, junto con sus números de puerto, protocolos y nombres de dominio.

En Windows, la asociación de puertos por defecto para los servicios se encuentra en el archivo %SystemRoot%\System32\drivers\etc\services. Este archivo es similar al archivo /etc/services de Linux.

2. Investigue qué es multicast. ¿Sobre cuál de los protocolos de capa de transporte funciona? ¿Se podría adaptar para que funcione sobre el otro protocolo de capa de transporte? ¿Por qué?

El multicast es una técnica que permite enviar un mensaje a un grupo de destinatarios de forma simultánea. A diferencia del broadcast, que envía un mensaje a todos los dispositivos de una red, el multicast solo envía el mensaje a los dispositivos que están interesados en recibirlo.

La técnica del multicast funciona sobre UDP, ya que no necesita establecer una conexión y se podría usar un mismo socket (un proceso tiene asociado un socket) para recibir datos de varios procesos que se quieren comunicar con un proceso a la vez.

Teóricamente podría intentarse adaptar multicast sobre TCP, pero sería demasiado complejo e iría en contra de la naturaleza del modelo ya que TCP establece una conexión punto a punto entre un único emisor y receptor.

3. Investigue cómo funciona el protocolo de aplicación FTP teniendo en cuenta las diferencias en su funcionamiento cuando se utiliza el modo activo de cuando se utiliza el modo pasivo ¿En qué se diferencian estos tipos de comunicaciones del resto de los protocolos de aplicación vistos?

FTP requiere dos conexiones TCP. Una conexión de control y otra para la transferencia de datos. El cliente escoge cualquier puerto no privilegiado, ($n > 1023$) y genera conexión de control contra el puerto 21 del servidor. El servidor recibe los comandos por dicha conexión y responde/recibe por la conexión de datos aquellos que lo requieran. La conexión de datos se crea y se cierra bajo demanda. El estado de cada operación se transmite por el canal de control.

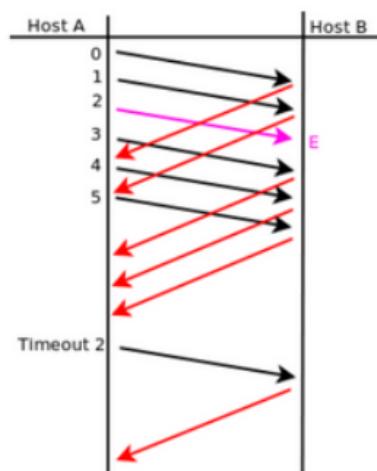
Modo Activo:

- Conexión de control: port 21.
- Conexión de datos: port 20.
- El servidor de forma activa se conecta al cliente para generar la conexión de datos.

Modo Pasivo:

- Conexión de control: port 21.
- Conexión de datos: port no privilegiado.
- El servidor de forma pasiva indica al cliente a que nuevo puerto debe conectarse. La conexión de datos la abre el cliente.

4. Suponiendo Selective Repeat; tamaño de ventana 4 y sabiendo que E indica que el mensaje llegó con errores. Indique en el siguiente gráfico, la numeración de los ACK que el host B envía al Host A.



Envía los ACK 0, 1, 3, 4 y 5, ya que el 2 llega con error. Como no se pueden dejar huecos, no se corre la ventana hasta que 2 se retransmita, y se vuelve a enviar en el timeout 2.

5. ¿Qué restricción existe sobre el tamaño de ventanas en el protocolo Selective Repeat?
El tamaño de la ventana no debe exceder la mitad del tamaño total del espacio de números de secuencia. La razón detrás de esta restricción es evitar la posibilidad de que un número de secuencia se reutilice antes de que el ACK correspondiente haya llegado, ya que la ventana se implementa como un buffer circular, entonces si fuese más grande podría haber paquetes representados por la misma posición en el buffer lo que podría llevar a confusiones en la correcta interpretación de los frames.

6. De acuerdo a la captura TCP de la siguiente figura, indique los valores de los campos borroneados.

No.	Time	Source	Destination	Protocol	Length	Info
1 0.000000	172.20.1.1	172.20.1.100	172.20.1.100	TCP	74	41749 > vce [] Seq= Win=5840 Len=0 MSS=1460 SACK_PERM=1 TStamp=270132 TSectr=0
2 0.001264	172.20.1.100	172.20.1.1	172.20.1.1	TCP	74	vce > 41749 [SYN, ACK] Seq=1047471501 Ack=3933822138 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TStamp=270132 TSectr=1877442
3 0.001341				TCP	66	[] > [] Seq= Ack= Win=5888 Len=0 TStamp=270132 TSectr=1877442

► Internet Protocol Version 4, Src: 172.20.1.100 (172.20.1.100), Dst: 172.20.1.1 (172.20.1.1)

▼ Transmission Control Protocol, Src Port: vce (11111), Dst Port: 41749 (41749), Seq: 1047471501, Ack: 3933822138, Len: 0

Source port: vce (11111)
 Destination port: 41749 (41749)
 [Stream index: 0]
 Sequence number: 1047471501
 Acknowledgement number: 3933822138
 Header length: 40 bytes

▼ Flags: 0x012 (SYN, ACK)

- 000. = Reserved: Not set
- ...0 =Nonce: Not set
- 0.... = Congestion Window Reduced (CWR): Not set
-0.... = ECN-Echo: Not set
-0.... =Urgent: Not set
-1 =Acknowledgement: Set
- 0.... = Push: Not set
-0... = Reset: Not set
-1. = Syn: Set
-0 = Fin: Not set

Window size value: 5792
 [Calculated window size: 5792]
 ► Checksum: 0x9803 [validation disabled]

SYN → Comienzo de 3WH

3933822137 → Se que es ese porque el receptor (línea 2) me indica que espera (ACK) que se le envíe el segmento 3933822138, por lo tanto el que le envíe en 1 es 3833822138 – 1

172.20.1.1 → Source

172.20.1.100 → Destination

41749 → Puerto Destino

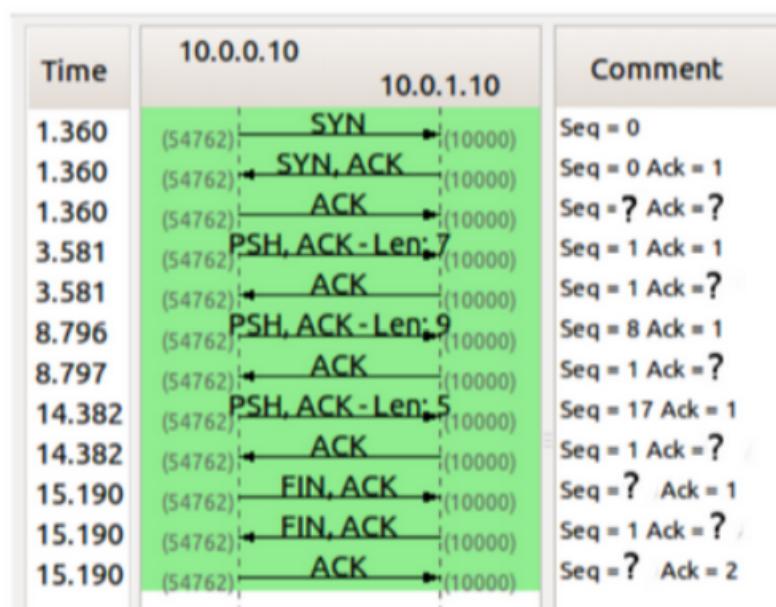
vce → Puerto Origen

ACK → Fin de 3WH

3933822138 → En el segmento anterior a este se indicó que se esperaba 3933822138

1047471502 → Se recibió 1047471501 , por lo que se espera recibir 1047471502

7. Dada la sesión TCP de la figura, completar los valores marcados con un signo de interrogación.



seq = 1 Ack = 1

Ack = 8

Ack = 17
 Ack = 22
 seq = 22
 Ack = 23
 seq = 23

8. ¿Qué es el RTT y cómo se calcula? Investigue la opción TCP timestamp y los campos TSval y TSecr.

El RTT (Round-Trip Time) es el tiempo que tarda un paquete en viajar desde un origen hasta un destino y de vuelta al origen. Se mide desde el momento en que se envía un paquete de datos hasta que el remitente recibe una respuesta. RTT incluye tanto el tiempo de transmisión (de ida y vuelta) como los tiempos de procesamiento en los dispositivos intermedios, como routers o servidores.

La opción de marcas de tiempo en TCP permite a los endpoints mantener una medición más precisa del tiempo de ida y vuelta (RTT) de la red entre ellos. Este valor ayuda a cada pila TCP a configurar y ajustar su temporizador de retransmisión. Hay otros beneficios, pero la medición RTT es el principal.

Para ello se incluye un Timestamp Value TSval en cada segmento que se envía. Los valores TSval se repiten en el lado opuesto de la conexión en el campo Timestamp Echo Reply TSecr . Entonces, cuando se confirma un segmento, el remitente de ese segmento puede simplemente restar su marca de tiempo actual del valor TSecr para calcular una medición precisa del tiempo de ida y vuelta (RTT).

$$\text{RTT}=\text{TSecr} - \text{TSval}$$

9. Para la captura tcp-captura.pcap, responder las siguientes preguntas.

a. ¿Cuántos intentos de conexiones TCP hay?

Hay 6.

tcp.flags.syn eq 1 and tcp.flags.ack eq 0						
No.	Time	Source	Destination	Protocol	Length	Info
3	0.000679	10.0.2.18	10.0.4.19	TCP	74	46987 - 5081 [SYN]
961	82.420045	10.0.2.18	10.0.4.19	TCP	74	45670 - 7002 [SYN]
963	83.540754	10.0.2.18	10.0.4.19	TCP	74	45671 - 7002 [SYN]
967	97.968958	10.0.2.18	10.0.4.19	TCP	74	45672 - 5081 [SYN]
981	135.753852	10.0.2.18	10.0.4.19	TCP	74	54424 - 5080 [SYN]
1396	149.807117	10.0.2.18	10.0.4.19	TCP	74	54425 - 9008 [SYN]

b. ¿Cuáles son la fuente y el destino (IP:port) para c/u?

Fuente	Destino
10.0.2.10:46907	10.0.4.10:5001
10.0.2.10:45670	10.0.4.10:7002
10.0.2.10:45671	10.0.4.10:7002
10.0.2.10:46910	10.0.4.10:5001
10.0.2.10:54424	10.0.4.10:9000
10.0.2.10:54425	10.0.4.10:9000

c. ¿Cuántas conexiones TCP exitosas hay en la captura? ¿Cómo diferencia las exitosas de las que no lo son? ¿Cuáles flags encuentra en cada una?

Hay 4

No.	Time	Source	Destination	Protocol	Length	Info
1	4.0.000116	10.0.2.10	10.0.4.19	TCP	74	5001 - 46997 [SYN, ACK]
968	97.96923	10.0.4.18	10.0.2.19	TCP	74	5081 - 46918 [SYN, ACK]
982	135.754958	10.0.4.18	10.0.2.19	TCP	74	9008 - 54424 [SYN, ACK]
1197	149.807136	10.0.4.18	10.0.2.19	TCP	74	9008 - 54425 [SYN, ACK]

Las exitosas tienen los flags SYN/ACK en 1, las fallidas tienen los flags RST/ACK en 1

d. Dada la primera conexión exitosa responder:

i. ¿Quién inicia la conexión?

La conexión es iniciada por 10.0.2.10:46907

ii. ¿Quién es el servidor y quién es el cliente?

El cliente es el que inicia la conexión 10.0.2.10:46907 y el servidor es el destino 10.0.4.10:7002

iii. ¿En qué segmentos se ve el 3-way handshake?

3 0.000079	10.0.2.10	10.0.4.10	TCP	74 46907 → 5001 [SYN] Seq=0 Win=1
4 0.000116	10.0.4.10	10.0.2.10	TCP	74 5001 → 46907 [SYN, ACK] Seq=1 Ack=1 Win=1
5 0.151614	10.0.2.10	10.0.4.10	TCP	66 46907 → 5001 [ACK] Seq=1 Ack=2 Win=1

iv. ¿Cuáles ISNs se intercambian?

1 –

Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 2218428254
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment number (raw): 0

2 –

Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 1292618479
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 2218428255

3 –

Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 2218428255
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 1292618480

Se intercambian los ISN 2218428254, 1292618479 y 2218428255

v. ¿Cuál MSS se negoció?

- ▼ Options: (20 bytes), Maximum segment size, SACK permitted,
 - ▼ TCP Option - Maximum segment size: 1460 bytes
 - Kind: Maximum Segment Size (2)
 - Length: 4

MSS Value: 1460

Se puede ver el segmento Nro 4 (siguiendo el orden de Wireshark)

vi. ¿Cuál de los dos hosts envía la mayor cantidad de datos (IP:port)?

10.0.2.10:46907, se incrementa su número de secuencia (se incrementa cuando se envían datos), mientras que 10.0.4.10:7002 nunca lo incrementa (salvo en el 3WH). 10.0.2.10:46907 termina con el ISN relativo de 786458 y 10.0.4.10:7002 con 1.

- e. Identificar el primer segmento de datos (origen, destino, tiempo, número de fila y número de secuencia TCP).

5 0.151614	10.0.2.10	10.0.4.10	TCP	66 46907 → 5001 [ACK] Seq=1 Ack=1 Win=14608 Len=0 TSval=120669 TSecr=120650
6 0.151826	10.0.2.10	10.0.4.10	TCP	90 46907 → 5001 [PSH, ACK] Seq=1 Ack=1 Win=24 TSval=120670 TSecr=120650
7 0.151925	10.0.4.10	10.0.2.10	TCP	66 5001 → 46907 [ACK] Seq=1 Ack=25 Win=14480 Len=0 TSval=120688 TSecr=120679
8 0.151975	10.0.2.10	10.0.4.10	TCP	1514 46907 → 5001 [ACK] Seq=25 Ack=1 Win=14608 Len=1448 TSval=120670 TSecr=120650
9 0.151984	10.0.2.10	10.0.4.10	TCP	74 45678 → 7002 [SYN] Seq=0 Win=14600 MSS=1460 SACK_PER=1 TSval=141236 TSecr=0 WS=16

Origen: 10.0.2.10:46907

Destino: 10.0.4.10:7002

Tiempo: 0.151826

Nro. de fila: 6

Nro. de secuencia TCP: 1 (221842855)

- i. ¿Cuántos datos lleva?

Lleva 24 bytes.

- ii. ¿Cuándo es confirmado (tiempo, número de fila y número de secuencia TCP)?

Tiempo: 0.151925

Nro. de fila: 7

Nro. de secuencia TCP: 1 (1292618480)

- iii. La confirmación, ¿qué cantidad de bytes confirma?

Confirma los 24 bytes, ya que indica que espera el byte nro 25.

- f. ¿Quién inicia el cierre de la conexión? ¿Qué flags se utilizan? ¿En cuáles segmentos se ve (tiempo, número de fila y número de secuencia TCP)?

La inicia 10.0.2.10:46907. Utiliza los flags FIN, PSH y ACK

Flags: 0x019 (FIN, PSH, ACK)
000. = Reserved: Not set
...0 = Nonce: Not set
.... 0.... = Congestion Window Reduced (CWR): Not set
.... .0... = ECN-Echo: Not set
.... ..0. = Urgent: Not set
.... ...1 = Acknowledgment: Set
....1... = Push: Set
....0.. = Reset: Not set
....0. = Syn: Not set
....1 = Fin: Set

Se ve en los segmentos (los azules)

957 75.075094	10.0.4.10	10.0.2.10	TCP	66 5001 → 46907 [ACK] Seq=1 Ack=786289 Win=315664 Len=0 TSval=139419 TSecr=137703
958 75.090196	10.0.2.10	10.0.4.10	TCP	234 46907 → 5001 [FIN, PSH, ACK] Seq=786289 Ack=1 Win=168 TSval=137726 TSecr=137707
959 75.091719	10.0.4.10	10.0.2.10	TCP	66 5001 → 46907 [FIN, ACK] Seq=1 Ack=786458 Win=0 TSval=139423 TSecr=137726
960 75.247457	10.0.2.10	10.0.4.10	TCP	66 46907 → 5001 [ACK] Seq=786458 Ack=2 Win=0 TSval=139443 TSecr=139423
961 82.426945	10.0.2.10	10.0.4.10	TCP	74 45678 → 7002 [SYN] Seq=0 Win=14600 MSS=1460 SACK_PER=1 TSval=141236 TSecr=0 WS=16

10. Responda las siguientes preguntas respecto del mecanismo de control de flujo.

- a. ¿Quién lo activa? ¿De qué forma lo hace?

El control de flujo lo activa el receptor enviando ventanas más chicas. Esto deja en evidencia que el receptor tiene poco espacio (o no tiene más lugar) para seguir recibiendo datos. Esto se realiza a través del campo de tamaño de ventana en los encabezados de los segmentos TCP.

b. ¿Qué problema resuelve?

Resuelve el problema de la posible saturación o congestión de los buffers en los endpoints. Al indicar al emisor que reduzca la cantidad de datos que está enviando, evita que el receptor se sobrecargue.

c. ¿Cuánto tiempo dura activo y qué situación lo desactiva?

Cuanto tiempo dura activo depende del receptor (más que nada la velocidad en que lee la aplicación). El control de flujo está activo mientras el receptor envíe ventanas más pequeñas (indicando capacidad limitada). Durará activo hasta que el receptor envíe ventanas más grandes, lo que indica que tiene más capacidad para recibir datos. En todo momento ambos extremos están actualizando su propia ventana.

11. Responda las siguientes preguntas respecto del mecanismo de control de congestión.

a. ¿Quién activa el mecanismo de control de congestión? ¿Cuáles son los posibles disparadores?

El control de congestión lo activa el emisor. El emisor limita la velocidad de transmisión de tráfico a través de su conexión en función de la congestión de red percibida. Este proceso es dinámico y adaptativo, y el emisor ajusta su velocidad de transmisión en respuesta a las condiciones cambiantes de la red.

Los posibles disparadores son:

- Fin de Temporización: La expiración del temporizador asociado con el envío de un segmento TCP puede ser interpretada como una señal de pérdida, indicando posiblemente congestión en la ruta.
- Recepción de TRES ACK Duplicados: La recepción de paquetes ACK duplicados procedentes del receptor también se interpreta como un suceso de pérdida. Este evento puede sugerir la pérdida de un paquete en la red debido a la congestión.

b. ¿Qué problema resuelve?

El objetivo es que no se desborde la propia red. Esto ocurre cuando hay más tráfico de red del que la red puede manejar eficientemente, lo que puede resultar en la pérdida de paquetes, retrasos elevados y un rendimiento de red deficiente. El control de congestión busca evitar que la red se sobrecargue ajustando la tasa de transmisión de datos del emisor para que sea compatible con la capacidad de la red.

c. Diferencie slow start de congestion-avoidance.

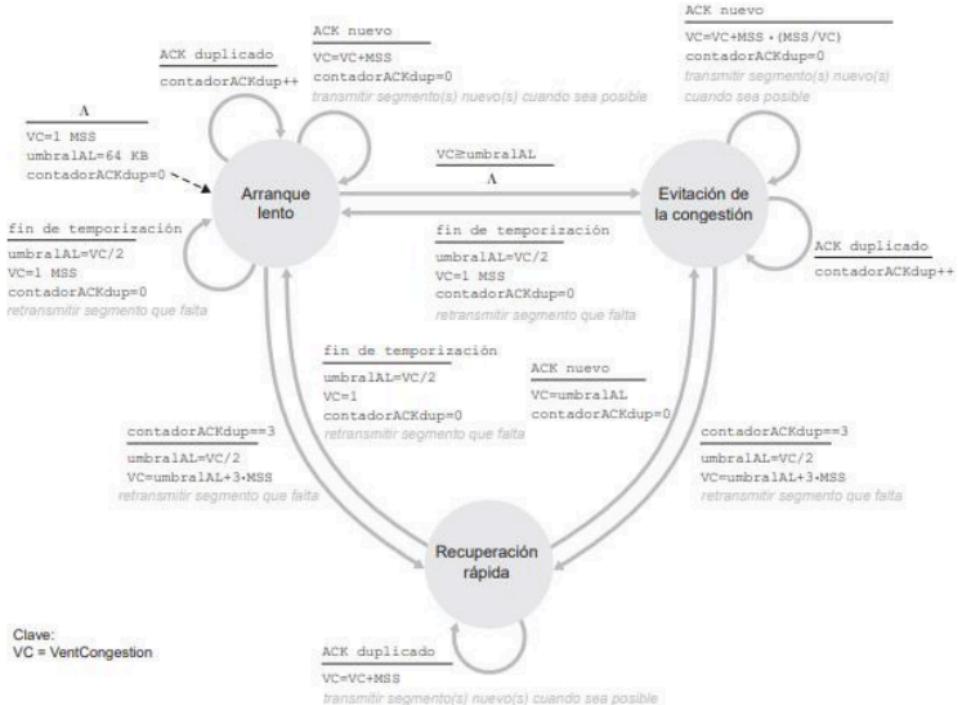
Arranque Lento (Slow Start):

- Inicio de la Conexión: Se utiliza al inicio de una conexión TCP.
- Tamaño de la Ventana de Congestión (VentCongestion): Inicializado con un valor pequeño (1 MSS, tamaño máximo de segmento).
- Crecimiento Exponencial: La ventana de congestión se duplica en cada periodo RTT.
- Finalización del Crecimiento Exponencial: o Al detectarse un suceso de pérdida (fin de temporización). o Cuando el valor de VentCongestion alcanza o sobrepasa el umbral de arranque lento (umbralAL).

Evitación de la Congestión (Congestion Avoidance):

- Transición desde Slow Start: Inicia cuando se detecta congestión y se sale del arranque lento.
- Tamaño de Ventana de Congestión (VentCongestion): Aproximadamente la mitad del valor cuando se detectó congestión por última vez.

- Crecimiento Lineal: Se incrementa en un MSS por RTT, más conservador que el crecimiento exponencial.
- Finalización del Crecimiento Lineal:
 - o Al detectarse un suceso de pérdida (fin de temporización o tres ACK duplicados).
 - o El valor de VentCongestion se fija en 1 MSS y se actualiza el umbral de arranque lento (umbralAL).
 - o En el caso de pérdida detectada por tres ACK duplicados, se realiza un ajuste menos drástico del valor de VentCongestion y umbralAL, entrando en el estado de recuperación rápida.



12. Para la captura `udp-captura.pcap`, responder las siguientes preguntas.

a. ¿Cuántas comunicaciones (`srcIP,srcPort,dstIP,dstPort`) UDP hay en la captura?

En principio son 9, pero hay algunas que se tratan de la misma conversación, así que son 6.

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A	
10.0.2.10	8003	10.0.2.10		0	63	2,646	0	0	63	2,646	0.000000	4.7099	0	4,494
10.0.2.10	9000	10.0.2.10		13	1	46	1	46	0	0	0.000000	—	—	—
10.0.2.10	9004	10.0.3.10		13	1	46	1	46	0	0	0.000000	—	—	—
10.0.2.10	9004	10.0.3.10		4555	1	46	1	46	0	0	0.000000	—	—	—
10.0.3.10	9045	10.0.2.10		9004	4	189	2	96	2	93	50.092837	7.6361	100	97
1.1.1.1	9045	10.0.2.10		9004	630	30k	0	0	630	30k	85.343725	17.8203	0	13k
10.0.2.10	53300	10.0.4.10		9045	1	46	1	46	0	0	112.609197	0.0000	—	—
10.0.2.10	59053	10.0.4.10		8003	5	235	3	139	2	96	118.382957	8.7621	126	87
10.0.2.10	8003	10.0.4.10		8003	2,320	2,473k	2,320	2,473k	0	0	169.166152	0.3529	56M	0

Fuente	Destino
10.0.2.10:0	10.0.30.10:8003
10.0.2.10:9004	10.0.3.10:9045
10.0.2.10:9004	1.1.1.1:9045
10.0.2.10:53300	10.0.4.10:9045
10.0.2.10:59053	10.0.4.10:8003
10.0.2.10:8003	10.0.4.10:8003

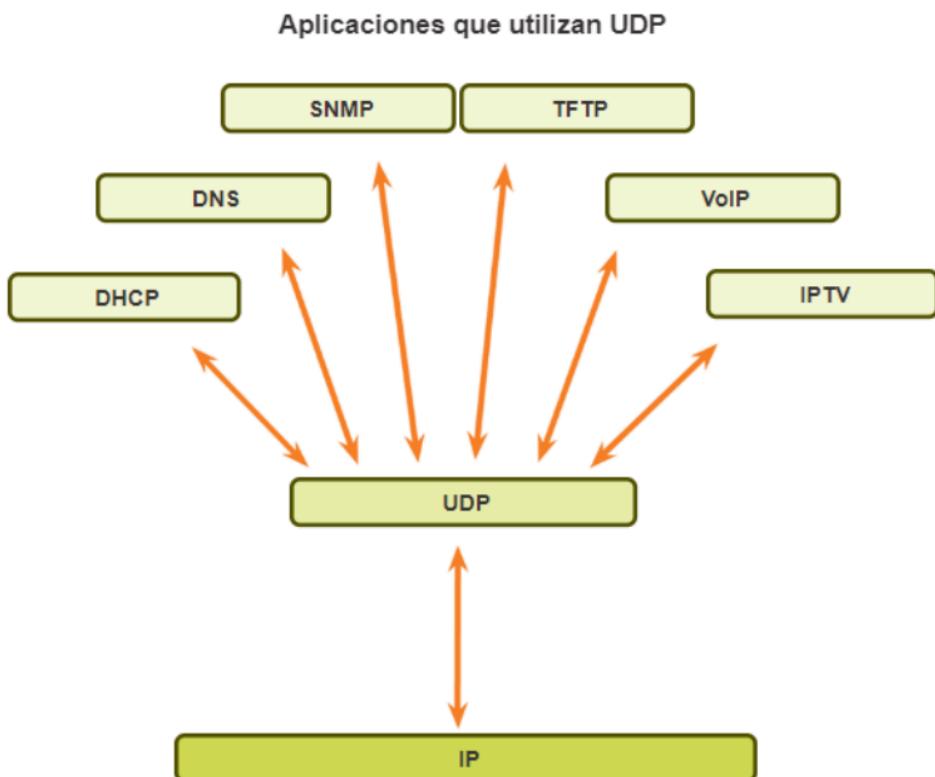
b. ¿Cómo se podrían identificar las exitosas de las que no lo son?

Se puede determinar con los mensajes ICMP.

c. ¿UDP puede utilizar el modelo cliente/servidor?

Como no se establece una conexión, no sigue ningún modelo en particular, no tiene una estructura interna para definir roles específicos de cliente o servidor. Aun así, la mayoría de las aplicaciones que utilizan UDP suelen adoptar un modelo cliente/servidor según las necesidades del servicio que están proporcionando.

d. ¿Qué servicios o aplicaciones suelen utilizar este protocolo? ¿Qué requerimientos tienen?



e. ¿Qué hace el protocolo UDP en relación al control de errores?

Lo único que ofrece es el checksum. Si detecta un error usando el checksum UDP no entrega el datagrama a la aplicación.

f. Con respecto a los puertos vistos en las capturas, ¿observa algo particular que lo diferencie de TCP?

En UDP el puerto origen puede ser 0 si no necesita una respuesta, puede ser simplemente un envío.

g. Dada la primera comunicación en la cual se ven datos en ambos sentidos (identificar el primer datagrama):

i. ¿Cuál es la dirección IP que envía el primer datagrama?, ¿desde cuál puerto?

10.0.2.10:9004

Puerto 47

79	59.092837	10.0.2.10	10.0.3.10	UDP	46	9004 → 9045 Len=4
80	62.173832	10.0.3.10	10.0.2.10	UDP	49	9045 → 9004 Len=7
81	64.116124	10.0.3.10	10.0.2.10	UDP	47	9045 → 9004 Len=5
82	66.728931	10.0.2.10	10.0.3.10	UDP	47	9004 → 9045 Len=5

ii. ¿Cuántos datos se envían en un sentido y en el otro?

12 bytes de 10.0.3.10:9045 a 10.0.2.10:9004

9 bytes de 10.0.2.10:9004 a 10.0.3.10:9045

13. Dada la salida que se muestra en la imagen, responda los ítems debajo.

Netid	State	Local Address:Port	Peer Address:Port	
udp	UNCONN	*:68	*:*	((dhclient",671,5))
udp	UNCONN	*:123	*:*	((ntp",2138,16))
udp	UNCONN	:::123	::*:	((ntp",2138,17))
tcp	LISTEN	*:80	*:*	((nginx",23653,19),("nginx",23652,19))
tcp	LISTEN	*:22	*:*	((sshd",1151,3))
tcp	LISTEN	127.0.0.1:25	*:*	((master",11457,12))
tcp	LISTEN	*:443	*:*	((nginx",23653,20),("nginx",23652,20))
tcp	LISTEN	*:3306	*:*	((mysqld",4556,13))
tcp	ESTAB	127.0.0.1:3306	127.0.0.1:34338	((mysqld",4556,14))
tcp	TIME-WAIT	10.100.25.135:443	43.226.162.110:29148	
tcp	ESTAB	127.0.0.1:48717	127.0.0.1:3306	((ruby",28615,10))
tcp	ESTAB	127.0.0.1:3306	127.0.0.1:48717	((mysqld",4556,17))
tcp	ESTAB	127.0.0.1:34338	127.0.0.1:3306	((ruby",28610,9))
tcp	ESTAB	10.100.25.135:22	200.100.120.210:61576	((sshd",13756,3),("sshd",13654,3))
tcp	LISTEN	:::22	::*:	((sshd",1151,4))
tcp	LISTEN	:125	::*:	((master",11457,13))

- Suponga que ejecuta los siguientes comandos desde un host con la IP 10.100.25.90. Responda qué devuelve la ejecución de los siguientes comandos y, en caso que corresponda, especifique los flags.

a. hping3 -p 3306 –udp 10.100.25.135

ICMP Port Unreachable ya que el puerto no está escuchando para UDP.

b. hping3 -S -p 25 10.100.25.135

Va a devolver flag RST/ACK ya que no hay ningún proceso en estado LISTEN en ese puerto.

c. hping3 -S -p 22 10.100.25.135

Va a devolver flag SYN/ACK ya que hay un proceso en estado LISTEN para cualquiera en ese puerto.

d. hping3 -S -p 110 10.100.25.135

Va a devolver flag RST/ACK ya que no hay ningún proceso en estado LISTEN en ese puerto.

- ¿Cuántas conexiones distintas hay establecidas? Justifique.

Hay 3

- 127.0.0.1:3306 con 127.0.0.1:34338
- 127.0.0.1:48717 con 127.0.0.1:3306
- 10.100.25.135:22 con 200.100.120.210:61576

Si bien se ven 5, esas 2 que faltan son

127.0.0.1:34338 con 127.0.0.1:3306

127.0.0.1:3306 con 127.0.0.1:48717

que son 1 y 2 pero con Local Address y Peer Address al revés ya que el comando presenta ambas para mostrar el flujo bidireccional de la comunicación.

PRACTICA 7 - CAPA DE RED - DIRECCIONAMIENTO

1. ¿Qué servicios presta la capa de red? ¿Cuál es la PDU en esta capa? ¿Qué dispositivo es considerado sólo de la capa de red?

La capa de red proporciona los servicios de enrutamiento y reenvío de paquetes (PDU) entre distintos hosts. El dispositivo principal de esta capa es el router.

2. ¿Por qué se lo considera un protocolo de mejor esfuerzo?

Se lo considera un protocolo de mejor esfuerzo ya que se trata de un protocolo poco confiable, esto quiere decir que hace todo lo posible para entregar los datos, pero no garantiza que todos los paquetes llegarán al destino, ni de que lo harán en el orden correcto.

3. ¿Cuántas redes clase A, B y C hay? ¿Cuántos hosts como máximo pueden tener cada una?

CLASE	REDES	HOSTS
A	128	16777214
B	16384	65534
C	2097152	254

4. ¿Qué son las subredes? ¿Por qué es importante siempre especificar la máscara de subred asociada?

Los prefijos de longitud fija por clase provocan un uso ineficiente en el espacio de direcciones y muchos equipos, produce escasez de direcciones.

Esto supone la aparición de las subredes, que básicamente permite que haya subgrupos en las redes, se utiliza para generar redes dentro de la red. Para ello toma una parte del hostid. La división en subredes plantea que si una red de clase desperdicia muchas direcciones IP entonces la misma sea dividida en N subredes más pequeñas que aprovechen mejor el espacio de direccionamiento. Las máscaras se utilizan para saber en una dirección IP qué bits son de red y qué bits son de host.

5. ¿Cuál es la finalidad del campo Protocol en la cabecera IP? ¿A qué campos de la capa de transporte se asemeja en su funcionalidad?

El campo Protocol indica el tipo de carga útil (payload) que sigue a la cabecera IP, es decir, especifica el protocolo de la capa superior al que se le entrega el paquete IP. Este campo es útil para que el dispositivo de destino sepa cómo interpretar y procesar los datos contenidos en el paquete. Es un campo de 8 bits y puede contener valores numéricos que representan diferentes protocolos de capa de transporte.

Se asemeja la funcionalidad al campo que indica el puerto destino en las cabeceras de los protocolos de capa de transporte.

6. Para cada una de las siguientes direcciones IP (172.16.58.223/26, 163.10.5.49/27, 128.10.1.0/23, 10.1.0.0/24, 8.40.11.179/12) determine:

a. ¿De qué clase de red es la dirección dada (Clase A, B o C)?

172.16.58.223/26: Clase B

163.10.5.49/27: Clase B

128.10.1.0/23: Clase B

10.1.0.0/24: Clase A

8.40.11.179/12: Clase A

b. ¿Cuál es la dirección de subred?

Para obtener la subred de la dirección IP 172.16.58.223/26, necesitamos analizar la máscara de subred /26:

Convertir la máscara de subred: /26 significa que los primeros 26 bits son 1 y los restantes 6 bits son 0. En formato decimal, esto corresponde a:

255.255.255.192

1. Esto significa que cada subred tiene 64 direcciones (de 0 a 63 en el último octeto).

2. **Identificar la dirección base de la subred:**

- La dirección IP 172.16.58.223 en binario es

10101100.00010000.00111010.11011111.

- Aplicando la máscara 255.255.255.192 (o
11111111.11111111.11111111.11000000 en binario), obtenemos la dirección base de la subred:

172.16.58.192

172.16.58.223/26: 10101100.00010000.00111010.11011111 AND
11111111.11111111.11111111.11000000 = 172.16.58.192

163.10.5.49/27: 10100011.00001010.00000101.00110001 AND
11111111.11111111.11111111.11000000 = 163.10.5.32

128.10.1.0/23: 10000000.00001010.00000001.00000000 AND
11111111.11111111.11111110.00000000 = 128.10.0.0

10.1.0.0/24: 00001010.00000001.00000000.00000000 AND
11111111.11111111.11111111.00000000 = 10.1.0.0

8.40.11.179/12: 00001000.00101000.00001011.10110011 AND
11111111.11110000.00000000.00000000 = 8.32.0.0

c. ¿Cuál es la cantidad máxima de hosts que pueden estar en esa subred?

172.16.58.223/26

- **Máscara:** /26 tiene 6 bits para hosts.
- **Cantidad de hosts:** $2^6 - 2 = 64 - 2 = 62$ hosts.

163.10.5.49/27: 30
128.10.1.0/23: 510
10.1.0.0/24: 254
8.40.11.179/12: 1,048,574

d. ¿Cuál es la dirección de broadcast de esa subred?

Subred 172.16.58.223/26

- **Máscara:** /26 = 255.255.255.192
- Cada subred cubre 64 direcciones.
- La dirección base de la subred es 172.16.58.192.
- **Broadcast:** 172.16.58.255

163.10.5.49/27: 163.10.5.63
128.10.1.0/23: 128.10.1.255
10.1.0.0/24: 10.1.0.255
8.40.11.179/12: 8.47.255.255

e. ¿Cuál es el rango de direcciones IP válidas dentro de la subred?

Subred 172.16.58.223/26

- **Dirección de red:** 172.16.58.192
- **Broadcast:** 172.16.58.255
- **Rango de IP válidas:** 172.16.58.193 a 172.16.58.254

163.10.5.49/27: 163.10.5.33- 163.10.5.62
128.10.1.0/23: 128.10.0.1 - 128.10.1.254
10.1.0.0/24: 10.1.0.1 - 10.1.0.254
8.40.11.179/12: 8.32.0.1 - 8.47.255.254

7. Su organización cuenta con la dirección 128.50.10.0. Indique:

a. ¿Es una dirección de red o de host?

Es de host puesto que todos sus bits de hosts no están en 0.

Se trata de una dirección de clase B cuya máscara por defecto es 255.255.0.0.

128.50.10.0 en binario es 10000000 00110010 00001010 00000000 La máscara de red es 11111111 11111111 00000000 00000000

Podemos ver como los bits que corresponden a la parte de host no están en 0, por lo que se trata de una dirección de host.

b. Clase a la que pertenece y máscara de clase.

Pertenece a la clase B y la máscara de la clase es 255.255.0.0

c. Cantidad de hosts posibles.

$$2^{16} - 2 = 65534$$

d. Se necesitan crear, al menos, 513 subredes. Indique:

i. Máscara necesaria.

Dado que necesitamos al menos 513 subredes, debemos encontrar el número de bits necesarios para alcanzar esta cantidad.

1. **Cálculo de bits de subred:**

- El valor más cercano a 513 en potencia de 2 es $2^9 = 512$, pero esto no es suficiente. Entonces necesitamos al menos **10 bits** de subred para cubrir 513 subredes (ya que $2^{10} = 1024$).

2. **Determinar la máscara de subred:**

- La IP original es **128.50.10.0**, que pertenece a una dirección de clase B, con una máscara de red por defecto de **/16** (255.255.0.0).
- Si añadimos 10 bits para las subredes, la nueva máscara será **/26** (16 bits de la clase B + 10 bits adicionales).

3. **Máscara de subred resultante:** **/26** o **255.255.255.192**

ii. Cantidad de redes asignables.

Con una máscara de **/26**, usamos 10 bits para las subredes, lo cual permite:

$2^{10} = 1024$ subredes asignables

Por lo tanto, **la cantidad de redes asignables es 1024**.

iii. Cantidad de hosts por subred.

Con una máscara de **/26**, quedan **6 bits** para los hosts.

$$2^6 - 2 = 64 - 2 = 62 \text{ hosts por subred}$$

iv. Dirección de la subred 710.

La subred 710 en binario sería la 709 ya que se empieza a contar desde 0. 710 en binario es 10110001 01 (separo en octetos).

Por lo que la dirección para la subred seria: 10000000 00110010 10110001 01000000
128.50.177.64

v. Dirección de broadcast de la subred 710.

10000000 00110010 10110001 01111111

128.50.177.127

8. Si usted estuviese a cargo de la administración del bloque IP 195.200.45.0/24

a. ¿Qué máscara utilizaría si necesita definir al menos 9 subredes?

Para obtener al menos 9 subredes, necesitamos una máscara que nos permita dividir la red original (195.200.45.0/24) en un mínimo de 9 subredes. La máscara original /24 equivale a 255.255.255.0, lo que deja 8 bits para asignar a las subredes y los hosts.

1. **Calcular cuántos bits extra necesitamos para crear 9 subredes:**
 - $2^n \geq 9$
 - Para que esto se cumpla, necesitamos al menos $n=4$ bits, ya que $2^4=16$ subredes.
2. **Nueva máscara:**
 - Al tomar 4 bits adicionales de los 8 bits disponibles para los hosts, pasamos de /24 a /28.
 - La nueva máscara sería **255.255.255.240**.
3. **Número de hosts por subred:**
 - Con una máscara /28, quedan 4 bits para los hosts, lo que da $2^4-2=14$ hosts utilizables por subred.

Máscara: 11111111 11111111 11111111 11110000 | 195.200.45.240

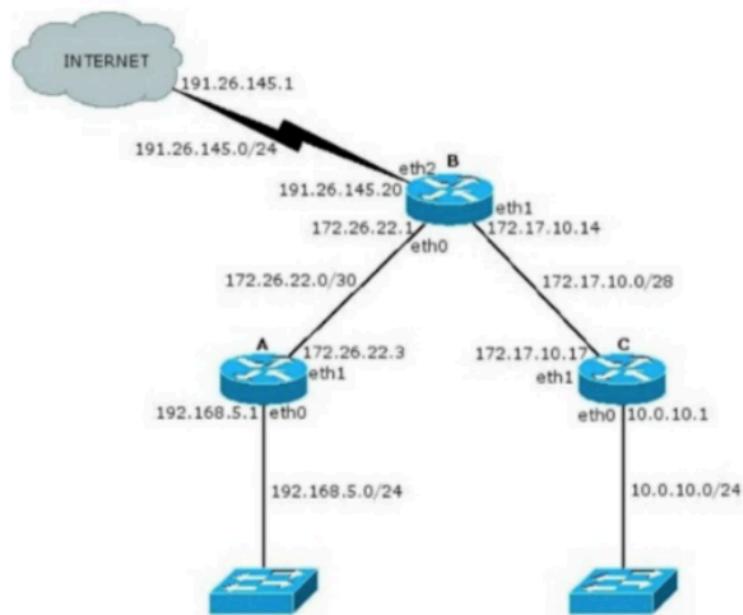
b. Indique la dirección de subred de las primeras 9 subredes.

11111111 11111111 11111111 00000000 - 195.200.45.0
11111111 11111111 11111111 00010000 - 195.200.45.16
11111111 11111111 11111111 00100000 - 195.200.45.32
11111111 11111111 11111111 00110000 - 195.200.45.48
11111111 11111111 11111111 01000000 - 195.200.45.64
11111111 11111111 11111111 01010000 - 195.200.45.80
11111111 11111111 11111111 01100000 - 195.200.45.96
11111111 11111111 11111111 01110000 - 195.200.45.112
11111111 11111111 11111111 10000000 - 195.200.45.128

c. Seleccione una e indique dirección de broadcast y rango de direcciones asignables en esa subred.

Subred 1: 195.200.45.0/28 (rango de 195.200.45.1 a 195.200.45.14, broadcast 195.200.45.15)

9. Dado el siguiente gráfico:



a. Verifique si es correcta la asignación de direcciones IP y, en caso de no serlo, modifique la misma para que lo sea.

192.168.5.0 /24

11000000 10101000 00000101 00000000

11111111 11111111 11111111 00000000

192.168.5.1

11000000 10101000 00000101 00000001

Está bien.

172.26.22.0 /30

10101100 00011010 00010110 00000000

11111111 11111111 11111111 11111100

172.26.22.3

10101100 00011010 00010110 00000011

Dirección de broadcast de la subred, está mal, esta debería ser 172.26.22.2.

172.26.22.1

10101100 00011010 00010110 00000011

Esta bien.

172.17.10.0 /28

10101100 00010001 00001010 00000000

11111111 11111111 11111111 11110000

172.17.10.14

10101100 00010001 00001010 00001110

Esta bien.

172.17.10.17

10101100 00010001 00001010 00010001

Esta mal, esta fuera del rango de los hosts de la red.

10.0.10.0 /24

00001010 00000000 00001010 00000000

11111111 11111111 11111111 00000000

10.0.10.1

00001010 00000000 00001010 00000001

Esta bien.

191.26.145.0 /25

10111111 11111010 10010001 00000000

11111111 11111111 11111111 10000000

191.26.145.1

10111111 11111010 10010001 00000001

Esta bien.

191.26.145.20

10111111 11111010 10010001 00010100

Esta bien.

b. ¿Cuántos bits se tomaron para hacer subredes en la red 10.0.10.0/24? ¿Cuántas subredes se podrían generar?

Se tomaron 16, ya que se trata de una dirección de clase A cuya máscara default es 255.0.0.0 y acá se está usando 255.255.255.0 por lo que se tomaron 16 bits más.

c. Para cada una de las redes utilizadas indique si son públicas o privadas.

Para saber si una red es pública o privada, debes comparar la dirección IP con los rangos reservados para redes privadas. Los rangos de IP privadas son los siguientes:

1. **Clase A:** 10.0.0.0 a 10.255.255.255 (máscara /8 o 255.0.0.0)
2. **Clase B:** 172.16.0.0 a 172.31.255.255 (máscara /12 o 255.240.0.0)
3. **Clase C:** 192.168.0.0 a 192.168.255.255 (máscara /16 o 255.255.0.0)

Si la IP pertenece a alguno de estos rangos, entonces es **privada**. Las direcciones IP fuera de estos rangos son **públicas** y son enrutables a través de internet.

Privadas:

- 192.168.5.1
- 172.26.22.1
- 172.17.10.14
- 10.0.10.1

Públicas:

- 191.26.145.1
- 191.26.145.20

10. ¿Qué es CIDR (Class Interdomain routing)? ¿Por qué resulta útil?

CIDR es una estrategia para frenar algunos problemas que se habían comenzado a manifestar con el crecimiento de Internet. Los mismos son:

- Agotamiento del espacio de direcciones de clase B.
- Crecimiento de las tablas de enrutamiento más allá de la capacidad del software y hardware disponibles.
- Eventual agotamiento de las direcciones IP en general.

CIDR consiste básicamente en permitir máscaras de subred de longitud variable (VLSM) para optimizar la asignación de direcciones IP y utilizar resumen de rutas para disminuir el tamaño de las tablas de enrutamiento.

11. ¿Cómo publicaría un router las siguientes redes si se aplica CIDR?

- a. 198.10.1.0/24
- b. 198.10.0.0/24
- c. 198.10.3.0/24
- d. 198.10.2.0/24

Para publicar estas redes usando CIDR (Classless Inter-Domain Routing), se pueden agrupar en el bloque más grande posible para reducir la cantidad de rutas que el router necesita anunciar.

Al observar los bits en común en cada dirección, podemos ver que los primeros 22 bits de todas las direcciones son iguales: **198.10.0.0/22**.

11111111 11111111 11111100 00000000

198.10.0.0/22

Esta red contiene todas las direcciones mencionadas.

12. Listar las redes involucradas en los siguientes bloques CIDR:

- 200.56.168.0/21
- Clase C. Máscara Default /24

11001000 00111000 10101000 00000000 Dirección

11111111 11111111 11111111 00000000 Mascara Default

11111111 11111111 11111000 00000000 CIDR

Las redes involucradas van desde:

11001000 00111000 10101000 00000000 – 200.56.168.0/24

Hasta:

11001000 00111000 10101111 00000000 – 200.56.175.0/24

- 195.24.0.0/13

Clase C. Máscara Default /24

11000011 00011000 00000000 00000000

11111111 11111111 11111111 00000000 Mascara Default

11111111 11111000 00000000 00000000 CIDR

Las redes involucradas van desde:

11000011 00011000 00000000 00000000 – 195.24.0.0/24

Hasta:

11000011 00011111 11111111 00000000 – 195.31.255.0/24

- 195.24/13

Clase C. Mascara Default /24

11000011 00011000 00000000 00000000

11111111 11111111 11111111 00000000 Mascara Default

11111111 11111000 00000000 00000000 CIDR

Las redes involucradas van desde:

11000011 00011000 00000000 00000000 – 195.24.0.0/24

Hasta:

11000011 00011111 11111111 00000000 – 195.31.255.0/24

13. *El bloque CIDR 128.0.0.0/2 o 128/2, ¿Equivale a listar todas las direcciones de red de clase B? ¿Cuál sería el bloque CIDR que agrupa todas las redes de clase A?*

Si, equivale a listar todas las direcciones de clase B. El bloque CIDR que agrupa todas las redes de clase A es 0.0.0.0/1

14. *¿Qué es y para qué se usa VLSM?*

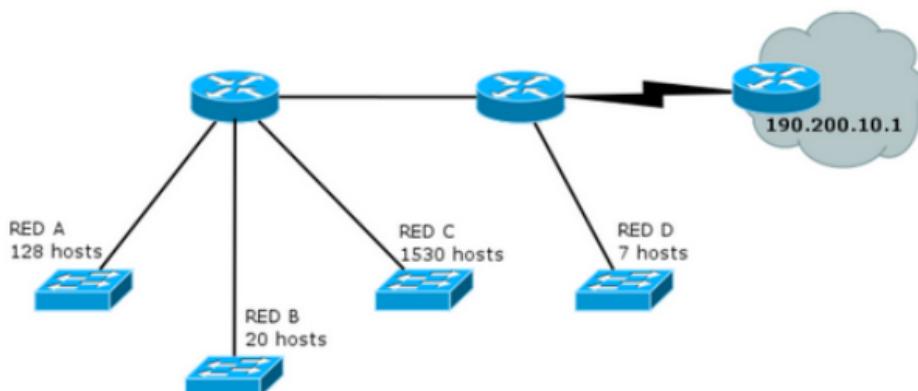
VLSM es realizar divisiones en subredes con máscaras de longitud variable. Sugiere hacer varios niveles de división en redes para lograr máscaras óptimas para las subredes. Se utiliza para evitar el agotamiento y desperdicio de direcciones IP.

15. *Describa, con sus palabras, el mecanismo para dividir subredes utilizando VLSM.*

- 1) Subnetear para la red con mayor cantidad de hosts.
- 2) De las subredes obtenidas, asignar todas las que se puedan con el menor desperdicio posible.
- 3) Si quedan segmentos de red sin una subred asignada volver al paso 1.

16. *Suponga que trabaja en una organización que tiene la red que se ve en el gráfico y debe armar el direccionamiento para la misma, minimizando el desperdicio de direcciones IP.*

Dicha organización posee la red 205.10.192.0/19, que es la que usted deberá utilizar.



a. ¿Es posible asignar las subredes correspondientes a la topología utilizando subnetting sin VLSM? Indique la cantidad de hosts que se desperdicia en cada subred.

Necesito 6 subredes (una por cada red y otra por las que comunican a los routers, ahí necesito una punto a punto) por lo tanto necesito 3 bits

205.10.192.0/19

11001101 00001010 11000000 00000000

11111111 11111111 11100000 00000000 Máscara de red

11111111 11111111 11111100 00000000 Máscara de subred

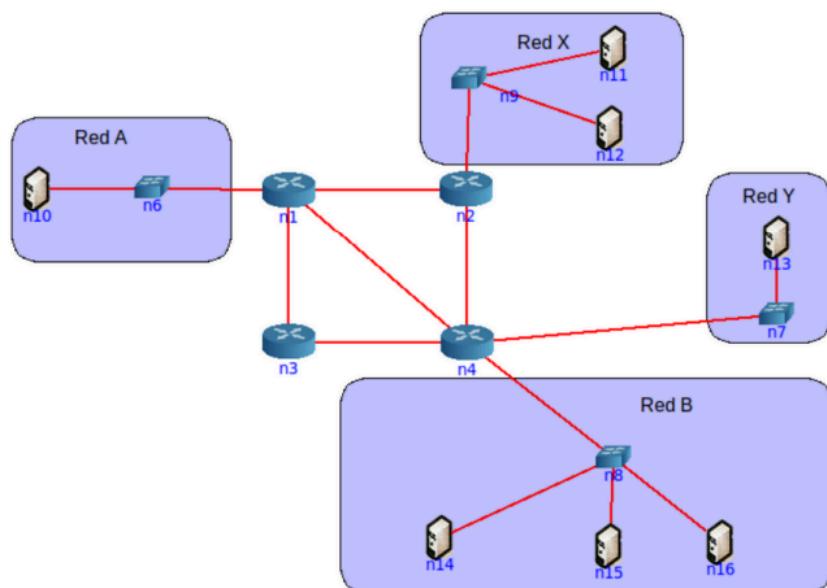
Red C necesita 1530 hosts, necesita 11 bits que generarían un total de 2048 hosts. No se tienen los bits suficientes en la parte de host para asignarle a la red C los que necesita por lo que no se podrían usar.

b. Asigne direcciones a todas las redes de la topología. Tome siempre en cada paso la primera dirección de red posible.

c. Para mantener el orden y el inventario de direcciones disponibles, haga un listado de todas las direcciones libres que le quedaron, agrupándolas utilizando CIDR.

d. Asigne direcciones IP a todas las interfaces de la topología que sea posible.

17. Utilizando la siguiente topología y el bloque asignado, arme el plan de direccionamiento IPv4 teniendo en cuenta las siguientes restricciones:



a. Utilizar el bloque IPv4 200.100.8.0/22.

b. La red A tiene 125 hosts y se espera un crecimiento máximo de 20 hosts.

c. La red X tiene 63 hosts.

d. La red B cuenta con 60 hosts

e. La red Y tiene 46 hosts y se espera un crecimiento máximo de 18 hosts.

f. En cada red, se debe desperdiciar la menor cantidad de direcciones IP posibles. En este sentido, las redes utilizadas para conectar los routers deberán utilizar segmentos de red /30 de modo de desperdiciar la menor cantidad posible de direcciones IP

Red A necesita 147 hosts, necesita 8 bits que generarían 256 hosts

11001000 01100100 00001000 00000000

11111111 11111111 11111100 00000000 Máscara de red

11111111 11111111 11111111 00000000 Máscara de subred

Quedan 2 bits para ser usados para subredes

11001000 01100100 00001000 00000000 – 200.100.8.0/24 – Asignada a la Red A

11001000 01100100 00001001 00000000 – 200.100.9.0/24 – Libre para seguir siendo dividida.

11001000 01100100 00001010 00000000 – 200.100.10.0/24

11001000 01100100 00001011 00000000 – 200.100.11.0/24

Red Y y Red X necesitan 64 y 63 hosts respectivamente, necesitan 7 bits que generarían 128 hosts

11001000 01100100 00001001 00000000

11111111 11111111 11111111 00000000 Máscara de subred

11111111 11111111 11111111 10000000 Nueva máscara de subred

Queda 1 bits para ser usados para subredes

11001000 01100100 00001001 00000000 – 200.100.9.0/25 – Asignada a la Red Y

11001000 01100100 00001001 10000000 – 200.100.9.128/25 – Asignada a la Red X

Red B necesita 62 hosts, necesita 6 bits que generarían 64 hosts

11001000 01100100 00001010 00000000

11111111 11111111 11111111 00000000 Máscara de subred

11111111 11111111 11111111 11000000 Nueva máscara de subred

Quedan 2 bits para ser usados para subredes

11001000 01100100 00001010 00000000 – 200.100.10.0/26 – Asignada a la Red B

11001000 01100100 00001010 01000000 – 200.100.10.64/26 – Libre para seguir siendo dividida.

11001000 01100100 00001010 10000000 – 200.100.10.128/26

11001000 01100100 00001010 11000000 – 200.100.10.192/26

Redes N1-N2, N2-N4, N4-N3, N3-N1, N1-N4 necesitan 4 hosts, necesitan 2 bits que generarían 4 hosts

11001000 01100100 00001010 01000000

11111111 11111111 11111111 11000000 Mascara de subred

11111111 11111111 11111111 11111100 Nueva mascara de subred

Quedan 4 bits para ser usados para subredes

11001000 01100100 00001010 01000000 – 200.100.10.64/30 – Asignada a la Red N1-N2

11001000 01100100 00001010 01000100 – 200.100.10.68/30 – Asignada a la Red N2-N4

11001000 01100100 00001010 01001000 – 200.100.10.72/30 – Asignada a la Red N4-N3

11001000 01100100 00001010 01001100 – 200.100.10.76/30 – Asignada a la Red N3-N1

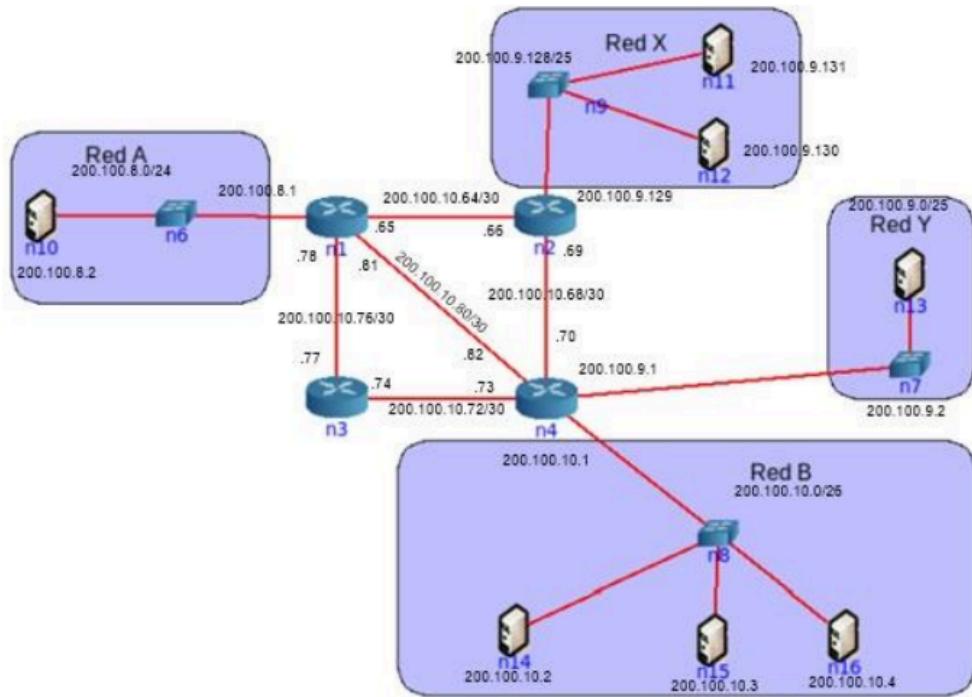
11001000 01100100 00001010 01010000 – 200.100.10.80/30 – Asignada a la Red N1-N4

11001000 01100100 00001010 01010100 – 200.100.10.84/30 – Libre para seguir siendo dividida.

11001000 01100100 00001010 01011000 – 200.100.10.88/30 – Libre para seguir siendo dividida.

11001000 01100100 00001010 01011100 – 200.100.10.92/30 – Libre para seguir siendo dividida.

18. Asigne direcciones IP en los equipos de la topología según el plan anterior.



19. Describa qué es y para qué sirve el protocolo ICMP.

Internet Control Message Protocol es un protocolo “helper” de IP. Brinda un “feedback” para poder resolver problemas en la red. Este protocolo se encapsula en IP.

a. Analice cómo funciona el comando ping.

El comando "ping" se utiliza para probar la conectividad entre dos hosts en una red IP. Básicamente, envía un mensaje de solicitud (Echo Request) a un host y espera una respuesta (Echo Reply). Esto permite medir el tiempo que tarda en viajar la solicitud y regresar la respuesta. Esto se conoce como el RTT (Round-Trip Time), y el "ping" muesras estadísticas como el RTT mínimo, promedio, máximo y desviación estándar, junto con la pérdida de paquetes lo que puede ayudar a diagnosticar problemas de conectividad. Cuando un nodo recibe una solicitud "Echo Request", debe responder copiando el contenido del mensaje con un "Echo Reply" (pong).

i. Indique el tipo y código ICMP que usa el ping.

Ping envía un paquete ICMP tipo 8 (Echo Request) con código 0. Este paquete contiene un mensaje de solicitud de eco. El código 0 especifica que es una solicitud estándar sin código específico.

ii. Indique el tipo y código ICMP que usa la respuesta de un ping.

Cuando el destino recibe una solicitud de eco (paquete ICMP tipo 8), responde con un paquete ICMP tipo 0 (Echo Reply) con código 0. El código 0 especifica que es una respuesta estándar sin código específico.

b. Analice cómo funcionan comandos como traceroute/tracert de Linux/Windows y cómo manipulan el campo TTL de los paquetes IP.

"traceroute" y "tracert" rastrean la ruta de un paquete IP ajustando el campo TTL del paquete. Comienzan con un TTL bajo y lo aumentan progresivamente. Cada salto de red reduce el TTL y envía una respuesta ICMP "Time Exceeded." El comando registra las direcciones IP de los saltos intermedios, lo que permite mostrar la ruta desde el origen hasta el destino.

c. Indique la cantidad de saltos realizados desde su computadora hasta el sitio www.nasa.gov. Analice:

```
PS C:\Users\frand> tracert -d www.nasa.gov

Traza a la dirección nasa-gov.go-vip.net [192.0.66.108]
sobre un máximo de 30 saltos:

 1      1 ms    <1 ms      1 ms  192.168.0.1
 2      *          *          *      Tiempo de espera agotado para esta solicitud.
 3      *          *          *      Tiempo de espera agotado para esta solicitud.
 4      *          *          *      Tiempo de espera agotado para esta solicitud.
 5      *          *          *      Tiempo de espera agotado para esta solicitud.
 6     11 ms    11 ms      *      181.96.113.234
 7     12 ms    11 ms    10 ms  200.25.50.80
 8    40 ms      *      40 ms  200.25.51.193
 9      *      42 ms    38 ms  200.25.57.147
10    41 ms    39 ms    39 ms  192.0.66.108

Traza completa.
```

i. Cómo hacer para que no muestre el nombre del dominio asociado a la IP de cada salto.

Para que no muestre el nombre del dominio asociado a la IP de cada salto, se puede usar la opción -d para evitar la resolución de nombres.

*ii. La razón de la aparición de * en parte o toda la respuesta de un salto.*

Cuando aparece un asterisco (*) en parte o en toda la respuesta de un salto, significa que ese enrutador o dispositivo de red no respondió a la solicitud de "traceroute" o "tracert". Puede ser una medida de seguridad, configuración o simplemente que el enrutador no responde a las solicitudes ICMP utilizadas por "traceroute" para rastrear la ruta.

d. Verifique el recorrido hacia los servidores de nombre del dominio unlp.edu.ar. En base al recorrido realizado, ¿podría confirmar cuál de ellos toma un camino distinto?

No, no es posible determinar el camino que siguen los servidores de nombres del dominio unlp.edu.ar debido a que todas las respuestas muestran "Tiempo de espera agotado para esta solicitud.". Esto puede ser porque los servidores de nombres de dominio están configurados para no responder a traceroute o porque hay un problema en la red que impide que las respuestas lleguen de vuelta.

20. ¿Para qué se usa el bloque 127.0.0.0/8? ¿Qué PC responde a los siguientes comandos?

El bloque de direcciones IP 127.0.0.0/8 está reservado para el uso en la red de loopback. La dirección IP más comúnmente utilizada en este bloque es 127.0.0.1, que se conoce como "localhost". La dirección de loopback se utiliza para permitir que un dispositivo se

comunique consigo mismo, lo que es útil en el diagnóstico y la prueba de aplicaciones y servicios de red sin la necesidad de acceder a una red real.

a. *ping 127.0.0.1*

El comando ping 127.0.0.1 recibirá una respuesta de la propia computadora.

b. *ping 127.0.54.43*

El comando ping 127.0.54.43 recibirá una respuesta de la propia computadora.

21. *Investigue para qué sirven los comandos ifconfig y route. ¿Qué comandos podría utilizar en su reemplazo? Inicie una topología con CORE, cree una máquina y utilice en ella los comandos anteriores para practicar sus diferentes opciones, mínimamente:*

- Configurar y quitar una dirección IP en una interfaz.
- Ver la tabla de ruteo de la máquina

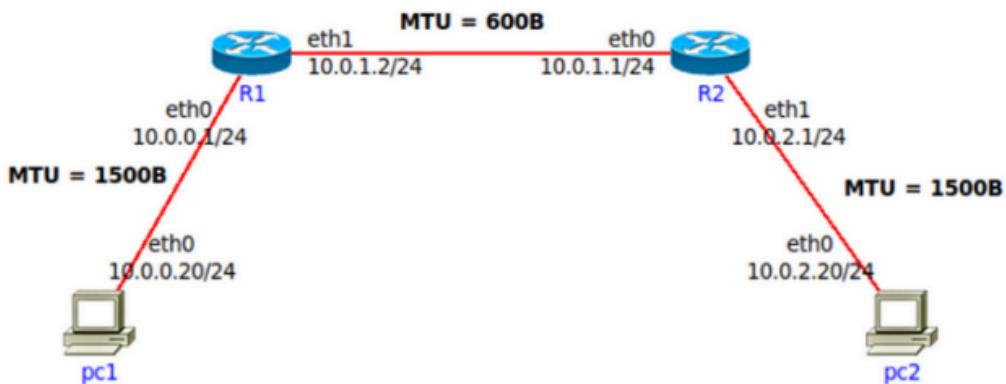
ifconfig se utiliza para configurar y visualizar información de interfaces de red en sistemas Unix/Linux. Alternativamente, se recomienda utilizar ip para una funcionalidad más avanzada.

route muestra y modifica la tabla de enrutamiento en sistemas Unix/Linux. En sistemas más recientes, se puede usar ip route o netstat -r para ver la tabla de enrutamiento, y ip route add y ip route del para agregar o eliminar rutas.

PRACTICA 8 - RUTEO

FRAGMENTACIÓN

1. Se tiene la siguiente red con los MTUs indicados en la misma. Si desde pc1 se envía un paquete IP a pc2 con un tamaño total de 1500 bytes (cabecera IP más payload) con el campo Identification = 20543, responder:



- Indicar IPs origen y destino y campos correspondientes a la fragmentación cuando el paquete sale de pc1

IP origen: 10.0.0.020/24

IP destino: 10.0.2.20/24

Header: 20

Tamaño total: 1500

Identificación: 20543
DF Flag: 0
MF Flag: 0
Fragment Offset: 0

- *¿Qué sucede cuando el paquete debe ser reenviado por el router R1?*

Como el enlace entre el router R1 y el R2 tiene un MTU de 600B, el paquete se debe fragmentar.

- *Indicar cómo quedarían los paquetes fragmentados para ser enviados por el enlace entre R1 y R2.*

Para fragmentar hay que tomar el valor máximo del MTU y restarle el valor del header (20), luego hay que encontrar el múltiplo de 8 más cercano a ese número.

1
Header: 20
Tamaño total: 596
Identificación: 20543
DF Flag: 0
MF Flag: 1
Fragment Offset: 0

2
Header: 20
Tamaño total: 596
Identificación: 20543
DF Flag: 0
MF Flag: 1
Fragment Offset: 72

3
Header: 20
Tamaño total: 348
Identificación: 20543
DF Flag: 0
MF Flag: 0
Fragment Offset: 144

Anotaciones:

- Al tamaño total le sumo el header. La suma de los totales de los fragmentos me debería dar el total del original + 20 * (cantidad de fragmentos – 1)
- El offset se calcula como la suma del tamaño de datos (SIN HEADERS) de los fragmentos anteriores dividido por 8.
- El último fragmento tiene el MF Flag en 0.
- El primer fragmento tiene el offset en 0.

- ¿Dónde se unen nuevamente los fragmentos? ¿Qué sucede si un fragmento no llega? Se reúnen de nuevo en los sistemas terminales. Si se pierde un fragmento, se deben retransmitir todos los fragmentos del paquete original. Sin embargo, IP no tiene mecanismos para comprobar la llegada de los fragmentos, así que depende de las decisiones de los protocolos de las capas superiores.

- Si un fragmento tiene que ser reenviado por un enlace con un MTU menor al tamaño del fragmento, ¿qué hará el router con ese fragmento?

Lo vuelve a fragmentar.

2. ¿Qué es el ruteo? ¿Por qué es necesario?

El ruteo consiste en seleccionar la interfaz de salida y el próximo salto. Involucra a los routers y hosts. Es necesario para que un paquete vaya de un extremo a otro.

3. En las redes IP el ruteo puede configurarse en forma estática o en forma dinámica. Indique ventajas y desventajas de cada método.

- Ventajas

Estática	Dinámica
Simplicidad: El enrutamiento estático es fácil de configurar y entender, especialmente en redes pequeñas y simples.	Adaptabilidad: El enrutamiento dinámico se ajusta automáticamente a cambios en la red, como enlaces caídos o nuevas rutas disponibles, lo que mejora la resiliencia de la red.
Control total: El administrador de red tiene un control total sobre las rutas y puede diseñar la red según sus necesidades específicas.	Escalabilidad: Es más adecuado para redes grandes y complejas, ya que la configuración se propaga automáticamente a través de la red.
Menos carga en la red: El enrutamiento estático generalmente genera menos tráfico de enrutamiento en la red, ya que las rutas se configuran manualmente y no cambian automáticamente.	Eficiencia de recursos: Enrutamiento dinámico puede encontrar rutas óptimas en función de métricas como la velocidad o la carga de los enlaces, lo que mejora la eficiencia del tráfico.

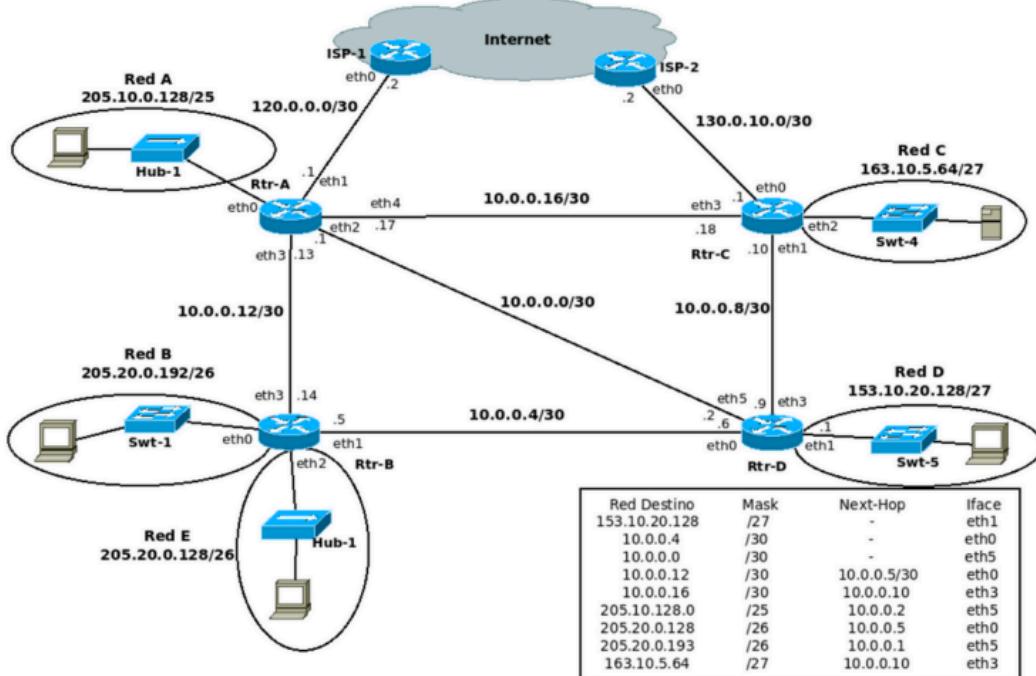
- Desventajas

Estática	Dinámica
No se adapta a cambios: El enrutamiento estático no se ajusta automáticamente a cambios en la topología de la red, lo que significa que si una ruta falla o cambia, debe actualizarse manualmente.	Mayor complejidad: La configuración y el mantenimiento del enrutamiento dinámico pueden ser más complejos que el enrutamiento estático, lo que requiere un conocimiento más profundo.
No es escalable: En redes grandes y complejas, la gestión manual de rutas puede volverse abrumadora y propensa a errores.	Mayor tráfico de enrutamiento: El enrutamiento dinámico genera más tráfico de enrutamiento en la red, ya que los routers intercambian información sobre las rutas, lo que puede consumir ancho de banda.
Menos eficiente en términos de tiempo: En una red grande, configurar y mantener el enrutamiento estático puede ser más demorado que utilizar enrutamiento dinámico.	Possible inestabilidad: Si no se configura adecuadamente, el enrutamiento dinámico puede causar problemas de estabilidad en la red.

4. Una máquina conectada a una red pero no a Internet, ¿tiene tabla de ruteo?

Una máquina conectada a una red local, incluso si no está conectada a Internet, tiene una tabla de enrutamiento para gestionar la comunicación dentro de la red local. La tabla de enrutamiento contiene información sobre las rutas disponibles en la red y cómo alcanzar otras máquinas dentro de esa red. En una red local, las rutas pueden ser bastante simples, ya que generalmente solo hay unos pocos dispositivos interconectados, como computadoras y dispositivos de red. Sin embargo, aún se necesita una tabla de enrutamiento para determinar cómo enviar datos entre estos dispositivos.

5. Observando el siguiente gráfico y la tabla de ruteo del router D, responder:



a. ¿Está correcta esa tabla de ruteo? En caso de no estarlo, indicar el o los errores encontrados. Escribir la tabla correctamente (no es necesario agregar las redes que conectan contra los ISPs).

Next-Hop 10.0.0.5/30 → No se puede esto, no debe tener la máscara.

Falta 10.0.0.8

205.10.128.0 no es una dirección de red que está presente en el gráfico. Además a 205.10.0.128 el Next-Hop es el router 10.0.0.1

205.20.0.193 es una dirección de host y no de red.

Red Destino	Mask	Next-Hop	Iface
153.10.20.128	/27	-	eth1
10.0.0.4	/30	-	eth0
10.0.0.0	/30	-	eth5
10.0.0.8	/30	-	eth3
10.0.0.12	/30	10.0.0.5	eth0
10.0.0.16	/30	10.0.0.10	eth3
205.10.128.0	/25	10.0.0.1	eth5
205.20.0.192	/26	10.0.0.5	eth0
205.20.0.128	/26	10.0.0.5	eth0
205.20.0.193	/26	10.0.0.1	eth5
163.10.5.64	/27	10.0.0.10	eth3

b. Con la tabla de ruteo del punto anterior, Red D, ¿tiene salida a Internet? ¿Por qué?
 ¿Cómo lo solucionaría? Suponga que los demás routers están correctamente configurados, con salida a Internet y que Rtr-D debe salir a Internet por Rtr-C.

No, no tiene salida a Internet, porque la tabla de ruteo no tiene ninguna entrada que lleve a algún ISP. Para solucionarlo habría que agregar una red default que tenga como Next-Hop a Rtr-C.

Red Destino	Mask	Next-Hop	Iface
0.0.0.0	/0	10.0.0.10	eth3

c. Teniendo en cuenta lo aplicado en el punto anterior, si Rtr-C tuviese la siguiente entrada en su tabla de ruteo, ¿qué sucedería si desde una PC en Red D se quiere acceder un servidor con IP 163.10.5.15?

Red Destino	Mask	Next-Hop	Iface
163.10.5.0	/24	10.0.0.9	eth1

Se entraría en un loop hasta que finalice el TTL del paquete IP y se descarte, ya que 10.0.0.9 no existe.

d. ¿Es posible aplicar la summarización en la tabla del router Rtr-D? ¿Por qué? ¿Qué debería suceder para poder aplicarla?

En 10.0.0.4 y 10.0.0.8 se podría aplicar si no tuvieran distinta interfaz.

En 205.20.0.192 y 205.20.0.128 si se puede aplicar ya que tiene el mismo salto e interfaz.

e. La summarización aplicada en el punto anterior, ¿se podría aplicar en Rtr-B? ¿Por qué?

No se podría aplicar ya que son redes que están directamente conectadas con interfaces distintas.

f. Escriba la tabla de ruteo de Rtr-B teniendo en cuenta lo siguiente:

- Debe llegar a todas las redes del gráfico
- Debe salir a Internet por Rtr-A
- Debe pasar por Rtr-D para llegar a Red D
- Sumarizar si es posible

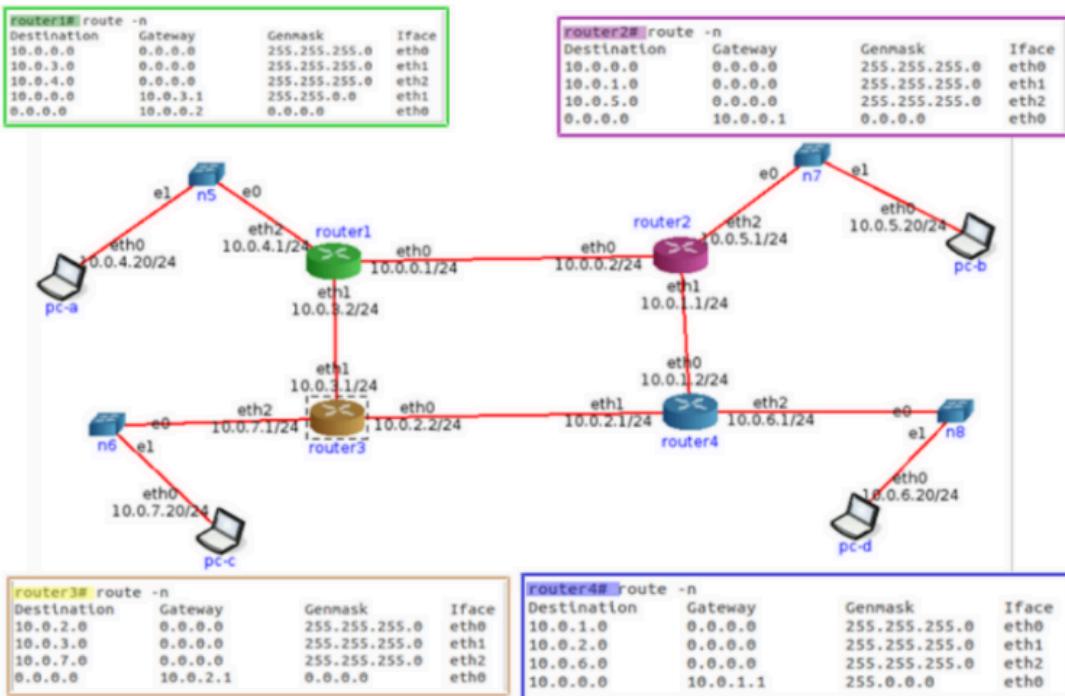
Red Destino	Mask	Next-Hop	Iface
205.20.0.192	/26	-	eth0
205.20.0.128	/26	-	eth2
10.0.0.12	/30	-	eth3
10.0.0.4	/30	-	eth1
10.0.0.8	/30	10.0.0.6	eth1
10.0.0.0	/30	10.0.0.13	eth3
10.0.0.16	/30	10.0.0.13	eth3

153.10.20.128	/27	10.0.0.6	eth1
163.10.5.64	/27	10.0.0.6	eth1
205.10.0.128	/25	10.0.0.13	eth3
120.0.0.0	/30	10.0.0.13	eth3
130.0.10.0	/30	10.0.0.13	eth3
0.0.0.0	/0	10.0.0.13	eth3

g. Si Rtr-C pierde conectividad contra ISP-2, ¿es posible restablecer el acceso a Internet sin esperar a que vuelva la conectividad entre esos dispositivos?

Se podría restablecer el acceso a Internet si los routers tienen en su tabla de ruteo la red ISP-1, es decir, a la red destino 120.0.0.0/30 para la cual se debe pasar por el router A.

6. Evalúe para cada caso si el mensaje llegará a destino, saltos que tomará y tipo de respuesta recibida en el emisor.



- Un mensaje ICMP enviado por PC-B a PC-C.

- Se debe enviar a 10.0.7.20/24:
- PC-B envia a 10.0.5.1/24 - Router2
- Como no hay ninguna entrada que coincida (ningún rango) lo envía al default que es el Router2
- El Router2 coincide con la ruta 10.0.0.0 con la mascara 255.255.0.0 por lo que envia al Router3
- El mensaje llega a PC-C desde el Router3 por la interfaz eth2
- Se realizan 4 saltos y se responde ICMP tipo 0 y código 0

- *Un mensaje ICMP enviado por PC-C a PC-B.*
 - Se debe enviar a 10.0.5.20/24:
 - PC-C envia a 10.0.7.1/24 - Router3
 - Como Router3 es default envía a Router4.
 - El Router4 se fija en la entrada 10.0.0.0 (se puede por la máscara que tiene) y el paquete se envía a Router2 por eth0.
 - El paquete llega a PC-B desde el Router2 por la interfaz eth2.
 - Se realizan 4 saltos y se recibe un ICMP tipo 0 y código 0 (eco).

- *Un mensaje ICMP enviado por PC-C a 8.8.8.8.*
 - Se debe enviar a 8.8.8.8:
 - PC-C envia a 10.0.7.1/24 - Router3
 - No coincide con ninguno y como Router3 es default envía a Router4.
 - En el Router4 no se tiene por default y no coincide con ninguno por lo que se descarta el mensaje.
 - Se realizan 2 saltos y se responde ICMP tipo 3 y código 0 (red inalcanzable)

- *Un mensaje ICMP enviado por PC-B a 8.8.8.8.*
 - Se debe enviar a 8.8.8.8:
 - PC-B envia a 10.0.5.1/24 - Router2
 - Lo envía por el default por lo que envía por al Router1.
 - En el router1 también entra por default por lo que es enviado al router2. Se entra en un loop hasta que termina el TTL.
 - Se realizan tantos saltos como sea el TTL y se responde ICMP tipo 11 y código 0 (TTL caducado).

DHCP Y NAT

7. Con la máquina virtual con acceso a Internet realice las siguientes observaciones respecto de la autoconfiguración IP vía DHCP:

- Inicie una captura de tráfico Wireshark utilizando el filtro bootp para visualizar únicamente tráfico de DHCP.*
- En una terminal de root, ejecute el comando \$ sudo /sbin/dhclient eth0 y analice el intercambio de paquetes capturado.*
- Analice la información registrada en el archivo /var/lib/dhcp/dhclient.leases, ¿cuál parece su función?*

Se mantiene un registro de las asignaciones de direcciones IP y otra información de configuración que se obtuvo del servidor DHCP.

- Ejecute el siguiente comando para eliminar información temporal asignada por el servidor DHCP. \$ rm /var/lib/dhcp/dhclient.leases*
- En una terminal de root, vuelva a ejecutar el comando \$ sudo /sbin/dhclient eth0 y analice el intercambio de paquetes capturado nuevamente ¿a que se debió la diferencia con lo observado en el punto "b"?*

En el punto "b" el cliente DHCP solicita una dirección IP al servidor DHCP en la red. El servidor DHCP asigna una dirección IP y otros parámetros de configuración que se registra en el archivo /var/lib/dhcp/dhclient.leases. Cuando se elimina el archivo

`dhclient.leases` y luego se ejecuta `sudo /sbin/dhclient enp0s3`, el cliente DHCP no puede encontrar un archivo `dhclient.leases` previamente existente para consultar información de arrendamientos anteriores. Esto lleva a un comportamiento ligeramente diferente: Al eliminar `dhclient.leases`, el cliente DHCP no tiene registro de direcciones IP anteriores ni de otros parámetros de configuración. Por lo tanto, inicia una solicitud DHCP desde cero, como si fuera la primera vez que se conecta a la red. Dado que el cliente DHCP inicia una nueva solicitud, el servidor DHCP en la red asigna una dirección IP y otros parámetros de configuración nuevamente al cliente. Esto significa que habrá un nuevo intercambio de paquetes DHCP entre el cliente y el servidor.

f. Tanto en “b” como en “e”, ¿qué información es brindada al host que realiza la petición DHCP, además de la dirección IP que tiene que utilizar?

Dirección IP asignada.

Máscara de subred.

Puerta de enlace predeterminada.

Servidores DNS.

Configuración proxy por WPAD (Web Proxy Auto-Discovery Protocol).

Dirección IP del servidor DHCP que atendió la solicitud.

Duración del arrendamiento (lease time).

8. ¿Qué es NAT y para qué sirve? De un ejemplo de su uso y analice cómo funcionaría en ese entorno. Ayuda: analizar el servicio de Internet hogareño en el cual varios dispositivos usan Internet simultáneamente.

Network Address Translation es un proceso de traducción de direcciones. Se utiliza para traducir direcciones privadas dentro de un espacio no privado (no “enrutable” en Internet) a direcciones públicas para un espacio público. Permite que múltiples dispositivos en una red compartan una única dirección IP pública. Por ejemplo, en una red doméstica donde hay varios dispositivos que desean acceder a Internet a través de un router. NAT traduce las direcciones IP privadas de estos dispositivos en una única dirección IP pública, lo que permite que se comuniquen con Internet. El router lleva un registro de estas traducciones para dirigir correctamente los datos a los dispositivos locales. Esto permite que haya un ahorro de direcciones públicas IPv4 debido a que las privadas se pueden repetir en los diferentes espacios privados (pero no dentro de uno mismo) y esto permite que varios dispositivos que están en una misma red privada puedan usar la misma dirección pública o que necesariamente no haya una dirección pública para cada dirección privada. NAPT tiene en cuenta el puerto y toca también la capa de transporte.

9. ¿Qué especifica la RFC 1918 y cómo se relaciona con NAT?

La RFC 1918 especifica un conjunto de direcciones IP reservadas para uso en redes privadas.

La RFC 1918 establece tres bloques de direcciones IP privadas en el rango de direcciones IPv4:

10.0.0.0 a 10.255.255.255

172.16.0.0 a 172.31.255.255

192.168.0.0 a 192.168.255.255

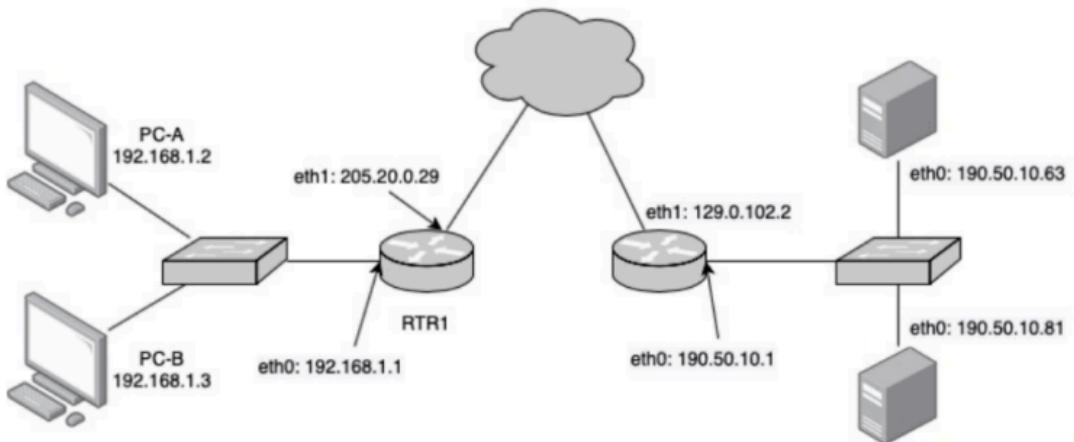
La relación entre esta RFC y NAT es que NAT se utiliza para permitir que dispositivos con direcciones IP privadas en una red local se comuniquen a través de una única dirección IP pública, que es visible en Internet.

10. En la red de su casa o trabajo verifique la dirección IP de su computadora y luego acceda a www.cualesmiip.com. ¿Qué observa? ¿Puede explicar qué sucede? ipconfig.

Salen distintas ip. Con ipconfig salen las privadas de IPv4 y en www.cualesmiip.com sale la pública IPv4.

11. Resuelva las consignas que se dan a continuación.

a. En base a la siguiente topología y a las tablas que se muestran, complete los datos que faltan.



PC-A (ss)

Local Address:Port Peer Address:Port

192.168.1.2:49273 _____

_____ 190.50.10.63:25

192.168.1.2:_____ 190.50.10.81:8080

190.50.10.63:80

192.168.1.2:37484

51238

PC-B (ss)

Local Address:Port Peer Address:Port

192.168.1.3:52734 _____

192.168.1.3:39275 _____

190.50.10.81:8081

190.50.10.81:8080

RTR-1 (Tabla de NAT)

Lado LAN	Lado WAN
192.168.1.2:49273	205.20.0.29:25192
192.168.1.2:51238	_____
192.168.1.3:52734	205.20.0.29:51091
192.168.1.2:37484	205.20.0.29:41823
192.168.1.3:39275	205.20.0.29:9123
205.20.0.29:16345	

SRV-A (ss)

Local Address:Port	Peer Address:Port
190.50.10.63:80	205.20.0.29:25192
190.50.10.63:25	205.20.0.29:41823

SRV-B (ss)

Local Address:Port	Peer Address:Port
190.50.10.81:8080	205.20.0.29:16345
190.50.10.81:8081	205.20.0.29:51091
190.50.10.81:8080	205.20.0.29:9123

b. En base a lo anterior, responda:

i. ¿Cuántas conexiones establecidas hay y entre qué dispositivos?

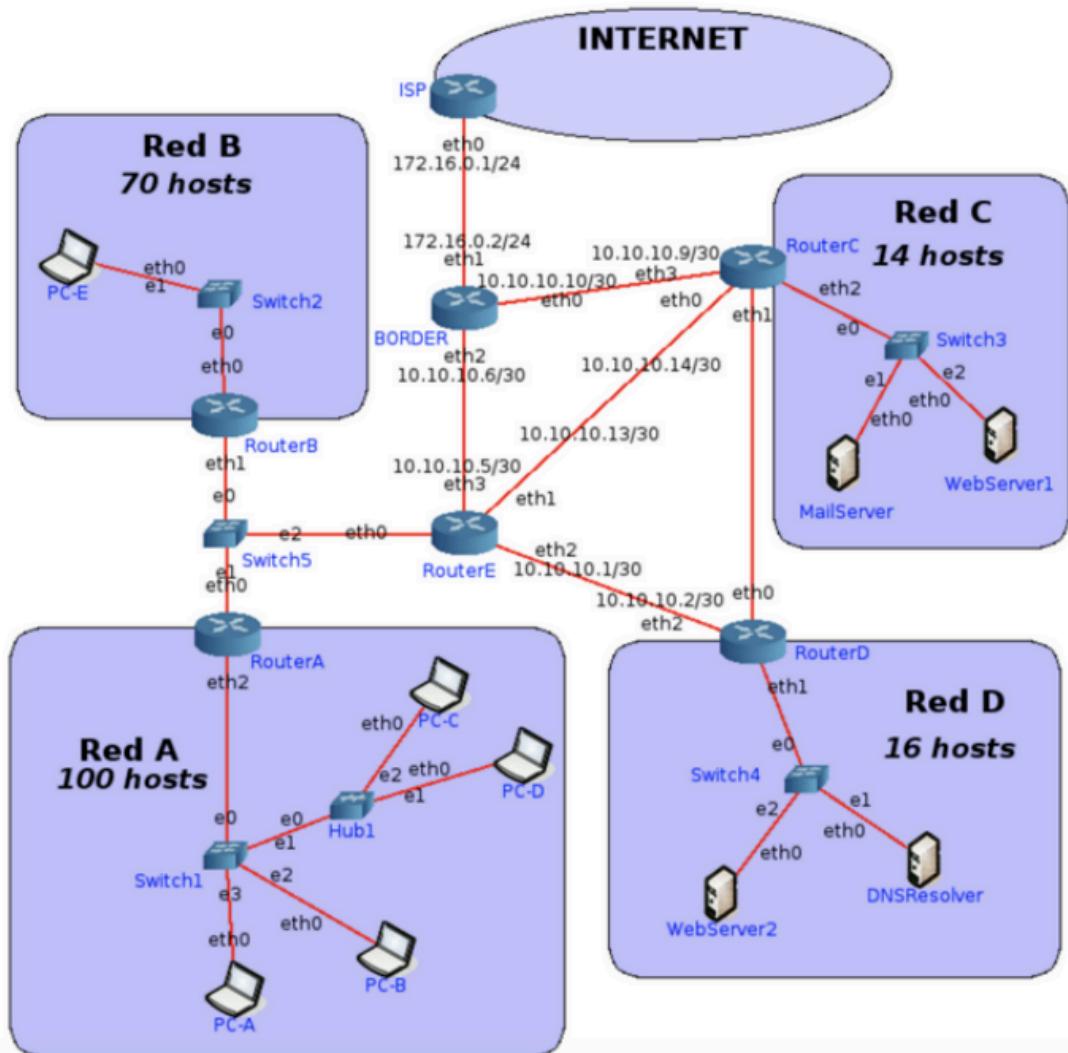
Hay 5 conexiones establecidas:

- PC-A 192.168.1.2:49273 y 190.50.10.63:80 SRV-A
- PC-A 192.168.1.2:37484 y 190.50.10.63:25 SRV-A
- PC-A 192.168.1.2: 51238 y 190.50.10.81:8080 SRV-B
- PC-B 192.168.1.3:52734 y 190.50.10.81:8081 SRV-B
- PC-B 192.168.1.3:39275 y 190.50.10.81:8080 SRV-B

ii. ¿Quién inició cada una de las conexiones? ¿Podrían haberse iniciado en sentido inverso? ¿Por qué? Investigue qué es port forwarding y si serviría como solución en este caso.

Las conexiones fueron iniciadas por los clientes ya que estos tienen direcciones privadas. Si se tiene Port Forwarding en el router para dirigir el tráfico hacia dispositivos específicos en la red local se podría realizar la conexión en el sentido inverso.

EJERCICIOS DE REPASO



12. Asigne las redes que faltan utilizando los siguientes bloques y las consideraciones debajo:

226.10.20.128/27	200.30.55.64/26	127.0.0.0/24	192.168.10.0/29
224.10.0.128/27	224.10.0.64/26	192.168.10.0/24	10.10.10.0/27

- Red C y la Red D deben ser públicas.
- Los enlaces entre routers deben utilizar redes privadas.
- Se debe desperdiciar la menor cantidad de IP posibles.
- Si va a utilizar un bloque para dividir en subredes, asignar primero la red con más cantidad de hosts y luego las que tienen menos.
- Las redes elegidas deben ser válidas.

226.10.20.100 00000 /27 – No puedo utilizar, reservada para multicast - Pública

224.10.0.100 00000 /27 – No puedo utilizar, reservada para multicast - Pública

200.30.55.01 000000 /26 – Libre para usar - Pública

224.10.0.01 000000 /26 – No puedo utilizar, reservada para multicast - Pública

127.0.0. 00000000 /24 – No puedo utilizar, reservada para loopback - Pública

192.168.10. 00000000 /24 – Si utilizo esta para subnetting no puedo utilizar 192.168.10.0/29 porque se solapan - Privada

192.168.10. 00000 000 /29 – Considerar la de arriba - Privada

10.10.10. 000 00000 /27 – Puedo utilizarla pero debo considerar las subredes /30 que ya se asignaron en el gráfico - Privada

RED A

Necesita 100 hosts. Necesito una máscara /25 (7 bits = 128 direcciones).

Puedo utilizar 192.168.10. 00000000 /24

192.168.10.0/29 no puedo utilizar

255.255.255. 00000000 Máscara de red

255.255.255. 1 00000000 Máscara de Subred

Queda 1 bit para ser usados para subredes.

192.168.10.00000000/25 - 192.168.10.0/25 - Asignado para la Red A

192.168.10.10000000/25 - 192.168.10.128/25 - Libre para seguir haciendo subnetting.

RED B

Necesita 70 hosts. Necesito una máscara /25 (7 bits = 128 direcciones). /26 = 64 direcciones, no alcanza.

Puedo utilizar lo que me quedó del subnetting para la red A. Utilizo 192.168.10.128/25.

RED D

Necesita 16 hosts. Necesito una máscara /27 (5 bits = 32 direcciones).

Tiene que ser pública.

Puedo utilizar 200.30.55.01 000000 /26.

255.255.255. 11000000 Máscara de Red.

255.255.255. 11100000 Máscara de Subred.

Queda 1 bit para ser usado por subredes.

200.30.55.01000000/27 – 200.30.55.64/27 – Asignado para la Red D.

200.30.55.01100000/27 – 200.30.55.96/27 – Libre para seguir haciendo subnetting.

RED C

Necesita 14 hosts. Necesito una máscara /28 (4 bits = 16 direcciones).

Tiene que ser pública.

Puedo utilizar 200.30.55.011 00000 /27 - Lo que me quedó del subnetting anterior.

255.255.255.11100000 Máscara de red.

255.255.255.11110000 Máscara de subred.

Queda 1 bit para ser usado para subredes.

200.30.55.01100000/28 - 200.30.55.96/28 – Asignado para la Red C.

200.30.55.01110000/28 - 200.30.55.112/28 – Libre para seguir haciendo subnetting.

Router C - Router D

Necesitan 4 hosts, por lo que con 2 bits se generarian correctamente. Necesito una máscara de /30.

Debe ser una red privada.

subnetear 10.10.10.0/27 evitando que se solapen con las que están en el gráfico. No puedo utilizar el bloque 192.168.10.0/29 porque se solaparía con 192.168.10.0/25 que ya fue asignada a la Red A.

10.10.10.00000000

255.255.255.11100000 Máscara de red

255.255.255.11111100 Máscara de subred

Quedan 3 bits para ser usados para subredes:

10.10.10.00000000 – 10.10.10.0/30 – Asignada para Router E y Router D

10.10.10.00000100 – 10.10.10.4/30 – Asignada para Router E y Border

10.10.10.00001000 – 10.10.10.8/30 – Asignada para Router C y Border

10.10.10.00001100 – 10.10.10.12/30 – Asignada para Router C y Router E

10.10.10.00010000 - 10.10.10.16/30 – Asigno a Router D - Router C

10.10.10.00010100 - 10.10.10.20/30 – Libre para ser asignada.

Quedo libre este bloque 10.10.10.24/29 (me di cuenta por CIDR).

10.10.10.00011000/29 - 10.10.10.24/29 - Asigno a Router A - Router B – Router E

13. Asigne IP a todas las interfaces de las redes listadas a continuación. Nota: Los routers deben tener asignadas las primeras IP de la red. Para enlaces entre routers, asignar en el siguiente orden: RouterA, RouterB, RouterC, RouterD y RouterE.

- Red A, Red B, Red C y Red D.

RED A

192.168.10.0/25 para Red A.

192.168.10.1 para RouterA.

192.168.10.2 para PC-A.

192.168.10.3 para PC-B.

192.168.10.4 para PC-C.

192.168.10.5 para PC-D.

RED B

192.168.10.128/25 para Red B.

192.168.10.129 para RouterB.

192.168.10.130 para PC-E.

RED C

200.30.55.96/28 para Red C.

200.30.55.97 para RouterC.

200.30.55.98 para WebServer1.

200.30.55.99 para MailResolver.

RED D

200.30.55.64/27 para Red D.

200.30.55.65 para RouterD.

200.30.55.66 para WebServer2.

200.30.55.67 para DNSResolver.

- *Red entre RouterA-RouterB-RouterE.*

10.10.10.24/29 para Red entre RouterA-RouterB-RouterE.

10.10.10.25 para RouterA.

10.10.10.26 para RouterB.

10.10.10.27 para RouterC.

- *Red entre RouterC-RouterD.*

10.10.10.16/30 para Red entre RouterC-RouterD.

10.10.10.27 para RouterC.

10.10.10.28 para RouterD.

14. Realice las tablas de rutas de RouterE y BORDER considerando:

- Siempre se deberá tomar la ruta más corta.
- Sumarizar siempre que sea posible.
- El tráfico de Internet a la Red D y viceversa debe atravesar el RouterC.
- Todos los hosts deben poder conectarse entre sí y a Internet.

RouterE

DESTINATION	MASK	NEXT HOP	INTERFACE
10.10.10.24	/29	-	eth0
10.10.10.4	/30	-	eth3
10.10.10.0	/30	-	eth2
10.10.10.12	/30	-	eth1
192.168.10.0	/25	10.10.10.25	eth0
192.168.10.128	/25	10.10.10.26	eth0
200.30.55.96	/28	10.10.10.14	eth1
200.30.55.64	/27	10.10.10.2	eth2
10.10.10.16	/29	10.10.10.2	eth2
0.0.0.0	/0	10.10.10.6	eth3

BORDER

DESTINATION	MASK	NEXT HOP	INTERFACE
10.10.10.4	/30	-	eth2
10.10.10.8	/30	-	eth0

172.16.0.0	/24	-	eth1
10.10.10.24	/29	10.10.10.5	eth3
10.10.10.0	/30	10.10.10.5	eth3
200.30.55.96	/28	10.10.10.9	eth3
10.10.10.12	/30	10.10.10.5	eth3
10.10.10.16	/30	10.10.10.9	eth3
200.30.55.64	/27	10.10.10.28	eth0
192.168.10.0	/25	10.10.10.5	eth0
192.168.10.128	/25	10.10.10.27	eth1

PRACTICA 9 - IPv6

1. *¿Qué es IPv6? ¿Por qué es necesaria su implementación?*

Es la versión mas nueva del protocolo IP. Proporciona mayor espacio de direcciones (128 bits), un formato de cabecera simplificado y menor overhead de procesamiento. Es necesaria su implementación para solucionar las limitaciones (en cuanto a direcciones IP) que traía IPv4. Garantiza que haya suficientes direcciones IP únicas para todos los dispositivos. Además, IPv6 proporciona mejoras en seguridad y eficiencia en comparación con IPv4.

2. *¿Por qué no es necesario el campo “Header Length” en IPv6?*

Porque en IPv4 había un campo opcional cuyo tamaño podría variar, haciendo que varíe la longitud del encabezado. En IPv6 todos los campos tienen un tamaño fijo, haciendo que el encabezado tenga una longitud constante. Y además se eliminan las opciones.

3. *¿En qué se diferencia el checksum de IPv4 e IPv6? Y en cuánto a los campos checksum de TCP y UDP, ¿sufren alguna modificación en cuanto a su obligatoriedad de cálculo?*

En IPv6, el campo de checksum es eliminado para simplificar el procesamiento de los paquetes en los routers y dispositivos, dejando esta verificación a las capas superiores (TCP y UDP). En cuanto a estas, su obligatoriedad no ha cambiado.

4. *¿Qué sucede con el campo “Opciones” en IPv6? ¿Existe, en IPv6, alguna forma de enviar información opcional?*

Se reemplazaron por las siguientes extensiones de encabezado:

- Permiten la extensibilidad del protocolo.
- Se encuentran a continuación del header.
- En general, son procesadas por los extremos.

5. *Si quisiese que IPv6 soporte una nueva funcionalidad, ¿cómo lo haría?*

Esta se implementaría como una extensión de encabezado.

6. ¿Es necesario el protocolo ICMP en IPv6? ¿Cumple las mismas funciones que en IPv4?

Mientras que ICMP podría ser prescindible en IPv4, en IPv6 es obligatorio. En IPv6 cumple funciones similares a las que desempeña en IPv4, aunque con algunas diferencias:

1. Descubrimiento de vecinos: ICMPv6 ND reemplaza ARP en IPv4, mapea direcciones IPv6 a direcciones de enlace para envío de paquetes.
2. Gestión de errores: ICMPv6 informa sobre errores de entrega, como paquetes demasiado grandes, tiempo de vida agotado y destino inalcanzable.
3. Redirección de rutas: ICMPv6 informa a los hosts sobre rutas más eficientes en la red.
4. Pruebas de conectividad: ICMPv6 incluye mensajes Echo Request y Echo Reply para pruebas de conectividad, similar a ping en IPv4.
5. MLD (Multicast Listener Discovery): ICMPv6 se utiliza para el descubrimiento de escuchadores de multidifusión en redes IPv6.

7. ¿Qué funciones cumple el protocolo Neighbour Discovery? ¿Puede funcionar IPv6 sin él? ¿Y sin una dirección de tipo link-local?

Las funciones del protocolo Neighbour Discovery son las de mapear direcciones lógicas (IPv6) a direcciones de Hardware (MAC, EUI-48, EUI-64):

- . Descubrimiento de vecinos: Permite que los nodos en una red determinen la dirección de enlace local (dirección MAC) de otros nodos dentro de la misma red, similar a lo que hace el protocolo ARP (Address Resolution Protocol) en IPv4.
- . Se utiliza para resolver direcciones IP en direcciones de capa de enlace.
- . Descubrimiento de vecinos inalcanzables: Facilita la detección de nodos vecinos que ya no están disponibles o accesibles en la red. Esto asegura que un nodo no intente comunicarse con un vecino no funcional, optimizando el uso de recursos.
- . Descubrimiento de routers: Permite a los nodos identificar la presencia de routers en la red local, obteniendo información sobre los routers disponibles y seleccionando uno para la comunicación con redes externas.
- . Determinación de prefijos de red y configuración sin estado: A través de mensajes de "Router Advertisement" (RA), un nodo puede aprender el prefijo de red y otra información esencial para auto-configurarse sin requerir un servidor DHCP.
- . Redirección de tráfico: Los routers utilizan NDP para informar a un nodo que hay una mejor ruta para llegar a un destino específico. Esto es útil para optimizar el enrutamiento en una red local.
- . Duplicated Address Detection (DAD): Garantiza que una dirección IPv6 no esté duplicada dentro de la red antes de asignársela a un nodo. Esto evita conflictos de direcciones.

No, IPv6 no puede funcionar sin él, ya que no hay otros protocolos que reemplacen las funciones que lleva a cabo NDP.

Sin una dirección de tipo link-local, IPv6 no puede funcionar correctamente. Las direcciones tipo link-local son fundamentales para funciones básicas como NDP, descubrimiento de routers y comunicación dentro de la red local.

8. ¿Cuál de las siguientes direcciones IPv6 no son válidas?

- 2001:0:1019:afde::1

Válida.

- 2001::1871::4

Invlida, tiene 2 compresiones.

- **3ffg:8712:0:1:0000:aede:aaaa:1211**

Inválida, 'g' no es válida en la notación hexadecimal.

- **3::1**

Válida.

- **::**

Válida.

- **2001::**

Válida.

- **3ffe:1080:1212:56ed:75da:43ff:fe90:affe**

Válida.

- **3ffe:1080:1212:56ed:75da:43ff:fe90:affe:1001**

Inválida, contiene 9 grupos de 4 caracteres/dígitos, solo debe tener 8 (= 128 bits).

9. ¿Cuál sería una abreviatura correcta de **3f80:0000:0000:0a00:0000:0000:0000:0845**?

- **3f80::a00::845**

Inválida, tiene 2 compresiones.

- **3f80::a:845**

Inválida, solo se pueden suprimir los 0 a la izquierda.

- **3f80::a00:0:0:0:845:4567**

Inválida, :4567 no es parte de la dirección.

- **3f80:0:0:a00::845**

Válida.

- **3f8:0:0:a00::845**

Inválida, solo se pueden suprimir los 0 a la izquierda.

10. Indique si las siguientes direcciones son de link-local, global-address, multicast, etc.

- **fe80::1/64**

Link-local.

- **3ffe:4543:2:100:4398::1/64**

Global-address.

- **::**

Unspecified.

- **::1**

Loopback.

■ **ff02::2**

Multicast.

■ **2818:edbc:43e1::8721:122**

Global-address.

■ **ff02::9**

Multicast.

11. Al autogenerarse una dirección IPv6 sus últimos 64 bits en muchas ocasiones no se deducen de la dirección MAC, se generan de forma random, ¿por qué sucede esto? ¿Qué es lo que se intenta evitar? (Ver direcciones temporarias, RFC 8981).

Es una medida de privacidad y seguridad. Esta práctica se utiliza para evitar la asociación directa y constante entre la dirección MAC de un dispositivo y su dirección IPv6 ya que cuando se utilizan las direcciones MAC en la construcción de direcciones IPv6, se puede rastrear la identidad de un dispositivo de manera más fácil y constante a lo largo del tiempo. Para abordar este problema, se introdujo la idea de las "direcciones temporales" en la RFC 4941 y, posteriormente, se actualizó con la RFC 8981. Las direcciones temporales permiten generar los últimos 64 bits de una dirección IPv6 de forma aleatoria, lo que dificulta el rastreo constante de un dispositivo a través de su dirección MAC. Al generar direcciones temporales de forma aleatoria, se mejora la privacidad del usuario al hacer que sea más difícil vincular de manera persistente la actividad en línea con una identidad específica basada en la dirección MAC.

PRACTICA 10 - CAPA DE ENLACE

1. *¿Qué función cumple la capa de enlace? Indique qué servicios presta esta capa.*

La función de la capa de enlace es mover un datagrama desde un nodo hasta otro adyacente a través de un único enlace de comunicaciones. Su función principal es proporcionar una interfaz entre la capa de red (capa 3) y el medio físico subyacente, como cables, fibra óptica o enlaces inalámbricos. En RED LAN.

Servicios que presta:

1. Entramado (framing):

- Encapsulado del datagrama en la trama, agregando encabezado (header) y cola (trailer).

2. Acceso al enlace:

- Acceso al canal si es un medio compartido.
- Direcciones "MAC" utilizadas en los encabezados de las tramas para identificar el origen y el destino.

3. Entrega confiable:

- Entre nodos adyacentes.
- Rara vez utilizados en enlaces de pocos errores (fibra óptica).

4. Control de flujo:

- Acuerdo entre nodos emisor y receptor (adyacentes).

5. Detección de errores

- Errores causados por atenuación de señal.
- El receptor detecta presencia de errores.

6. Corrección de errores.

7. Half-duplex y full-duplex:

- Half-duplex puedo recibir y transmitir pero no al mismo tiempo.

2. Compare los servicios de la capa de enlace con los de la capa de transporte.

Los servicios de detección y corrección de errores y control de flujo son ofrecidos también por la capa de transporte. La diferencia entre ambos radica en que la capa de enlace se enfoca en aspectos locales del enlace, mientras que la capa de transporte aborda la transferencia extremo a extremo a través de redes más amplias. Además la capa de transporte proporciona una fiabilidad y garantías que la capa de enlace no.

3. Direccionamiento Ethernet:

- ¿Cómo se identifican dos máquinas en una red Ethernet?

Mediante la dirección MAC.

- ¿Cómo se llaman y qué características poseen estas direcciones?

Las direcciones MAC también se conocen como direcciones de capa de enlace. Son direcciones físicas de 48 bits (6 bytes) y se expresan en hexadecimal. Los primeros 24 bits (3 bytes) identifican al fabricante de la tarjeta (OUI) y los siguientes 24 bits son únicos para interfaz de red.

- ¿Cuál es la dirección de broadcast en la capa de enlace? ¿Qué función cumple?

FF:FF:FF:FF:FF:FF.

La función principal de la dirección de broadcast es enviar información a todos los dispositivos en la red sin la necesidad de conocer sus direcciones MAC individuales.

4. Sobre los dispositivos de capa de enlace:

- Enumere dispositivos de capa de enlace y explique sus diferencias.

HUB: Actúa como un repetidor y simplemente repite las señales a todos los puertos. No divide dominios de colisión ni de broadcast.

Switch: Examina las direcciones MAC para enviar tramas solo al puerto específico donde se encuentra el destinatario. Divide dominios de colisión. No divide dominios de broadcast.

Bridge: Conecta dos segmentos de red, examina las direcciones MAC y aprende las ubicaciones de las direcciones MAC en ambos lados. Puede dividir dominios de colisión, no divide dominios de broadcast (es como el switch solo que tiene menos puertos).

- ¿Qué es una colisión?

Dos dispositivos intentan transmitir datos simultáneamente en una red compartida, causando una interferencia y resultando en la pérdida de datos.

- ¿Qué dispositivos dividen dominios de broadcast?

El Router.

- ¿Qué dispositivos dividen dominios de colisión?

Router, Switch y Bridge.

5. ¿Para qué sirve el algoritmo de acceso al medio en Ethernet? ¿Es orientado a la conexión?

El algoritmo de acceso al medio en Ethernet es fundamental para regular cómo los dispositivos conectados a una red Ethernet comparten y acceden al medio físico (como un cable) para transmitir datos, evitando colisiones y garantizando una comunicación eficiente. Este algoritmo, conocido como CSMA/CD (Carrier Sense Multiple Access with Collision Detection), tiene varias funciones clave:

Evitar colisiones: Garantiza que dos dispositivos no transmitan simultáneamente en el mismo medio, lo que provocaría una colisión de datos.

Coordinar el acceso: Permite que múltiples dispositivos compartan un mismo medio de comunicación de manera ordenada y equitativa.

Maximizar la eficiencia: Reduce el tiempo perdido en retransmisiones innecesarias, mejorando el rendimiento de la red.

Recuperarse de colisiones: En caso de que ocurra una colisión, el algoritmo establece cómo los dispositivos deben detectarla y retransmitir sus datos.

Funcionamiento:

Carrier Sense (CS): Antes de transmitir, un dispositivo "escucha" el medio para verificar si está ocupado.

Si detecta actividad, espera hasta que el medio esté libre.

Multiple Access (MA): Como múltiples dispositivos comparten el medio, cada uno debe esperar su turno para transmitir, basado en la disponibilidad del medio.

Collision Detection (CD): Si dos dispositivos transmiten al mismo tiempo, el algoritmo detecta la colisión porque la señal resultante es diferente de la esperada.

Ambos dispositivos interrumpen la transmisión y emiten una señal de jam (ruido) para indicar la colisión.

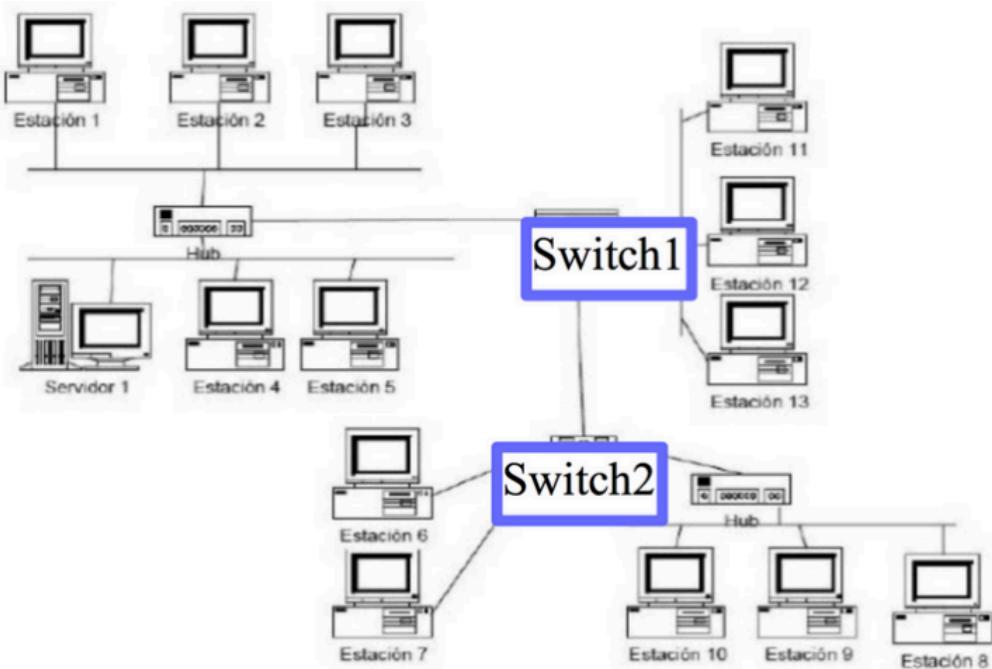
Backoff (retroceso): Cada dispositivo espera un tiempo aleatorio antes de intentar retransmitir, reduciendo la probabilidad de una nueva colisión.

Ethernet no es orientado a la conexión. Cada estación en una red Ethernet opera de manera independiente y no establece una conexión dedicada antes de transmitir datos. Cada estación compite por el acceso al medio según sea necesario

6. ¿Cuál es la finalidad del protocolo ARP?

Mapear direcciones IP a direcciones MAC. Una estación emite una solicitud ARP para conocer la dirección MAC asociada a una dirección IP y recibe una respuesta con la información correspondiente. La tabla ARP en caché almacena estas asociaciones para futuras referencias.

7. Dado el siguiente esquema de red, responda:



a. Suponiendo que las tablas de los switches (tablas CAM) están llenas con la información correcta, responda quién escucha el mensaje si:

i. La estación 1 envía una trama al servidor 1.

Estación 2, Estación 3, Servidor 1, Estación 4 y Estación 5.

ii. La estación 1 envía una trama a la estación 11.

Estación 2, Estación 3, Servidor 1, Estación 4, Estación 5, Estación 11.

iii. La estación 1 envía una trama a la estación 9.

Estación 2, Estación 3, Servidor 1, Estación 4, Estación 5, Estación 10, Estación 9 y Estación 8.

iv. La estación 4 envía una trama a la MAC de broadcast.

Todos.

v. La estación 6 envía una trama a la estación 7.

Estación 7.

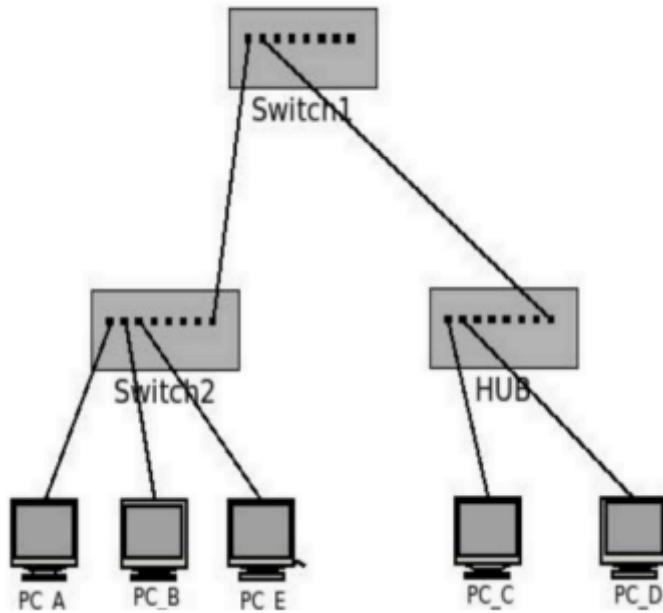
vi. La estación 6 envía una trama a la estación 10.

Estación 10, Estación 9, Estación 8.

b. ¿En qué situaciones se pueden producir colisiones?

En donde hay HUB, ya que todos envían y todos escuchan.

8. En la siguiente topología de red indique:



a. ¿Cuántos dominios de colisión hay?

Hay 5. 1 por el HUB, 1 compartido entre Switch1 y Switch2 y los 3 puertos restantes del Switch2.

b. ¿Cuántos dominios de broadcast hay?

Hay 3, uno por cada componente (HUB y Switches).

c. Indique cómo se va llenando la tabla de asociaciones MAC → PORT de los switches SW1 y SW2 durante el siguiente caso:

i. A envía una solicitud ARP consultando la MAC de C.

Switch2	
MAC	PORT
MAC_PC-A_eth0	0

Switch1	
MAC	PORT
MAC_PC-A_eth0	0

ii. C responde esta solicitud ARP.

Switch2	
MAC	PORT
MAC_PC-A_eth0	0
MAC_PC-C_eth0	7

Switch1	
MAC	PORT
MAC_PC-A_eth0	0
MAC_PC-C_eth0	1

iii. A envía una solicitud ARP consultando la MAC de B.

Switch2	
MAC	PORT
MAC_PC-A_eth0	0
MAC_PC-C_eth0	7

Switch1	
MAC	PORT
MAC_PC-A_eth0	0
MAC_PC-C_eth0	1

iv. B responde esta solicitud ARP.

Switch2	
MAC	PORT
MAC_PC-A_eth0	0
MAC_PC-C_eth0	7
MAC_PC-B_eth0	1

Switch1	
MAC	PORT
MAC_PC-A_eth0	0
MAC_PC-C_eth0	1

d. Si la PC E y la PC D hubiesen estado realizando un *tcpdump* para escuchar todo lo que pasa por su interfaz de red, ¿cuáles de los requerimientos/resuestas anteriores hubiesen escuchado cada una?

Las consultas las habrían escuchado todos porque son broadcast. Las respuestas solo escucharan los destinatarios y los casos donde hay un HUB.

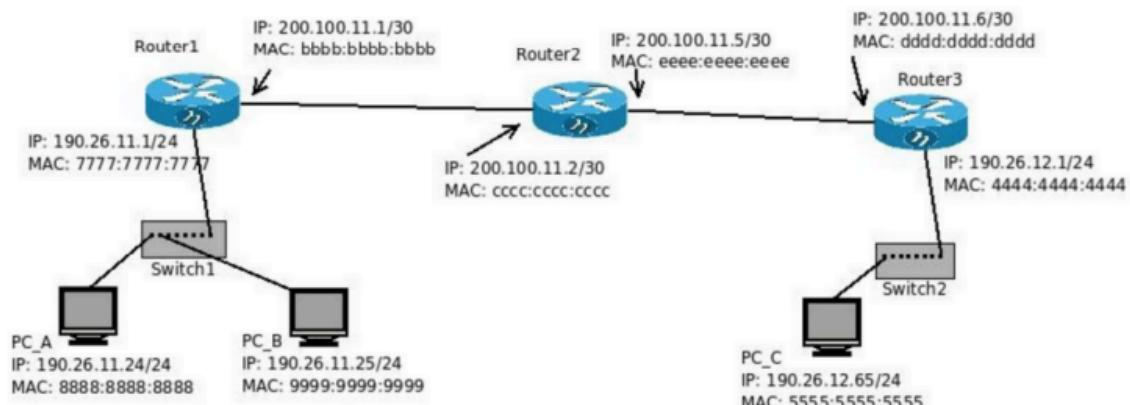
La PC E habría escuchado:

- La consulta de la MAC C de A
- La consulta de la MAC B de A

La PC D habría escuchado:

- La consulta de la MAC C de A
- La respuesta de C sobre la consulta de su MAC.
- La consulta de la MAC B de A

9. En la siguiente topología:



Suponiendo que todas las tablas ARP están vacías, tanto de PCs como de routers. Si la PC_A le hace un ping a la PC_C, indique:

- ¿En qué dominios de broadcast hay tráfico ARP? ¿Con qué direcciones de origen y destino?

En todos los dominios hay tráfico de ARP, lo que cambia son las direcciones de origen y destino MAC. Las de IP son las mismas siempre. En la ida la dirección destino MAC va a ser la FF:FF:FF:FF:FF y en la vuelta ya se sabe la de destino por lo que es la de destino que se aprendió en la ida y vuelta ARP.

- ¿En qué dominios de broadcast hay tráfico ICMP?

En todos.

- ¿Con qué direcciones de origen y destino de capa 2?

La dirección destino MAC van cambiando en las distintas redes ya que se utilizan las MAC de los defaults getaways (de los routers).

- ¿Con qué direcciones de origen y destino de capa 3?

Las direcciones IP siempre serán las mismas.

- ¿Cuál es la secuencia correcta en la que se suceden los anteriores?

Paso a paso sobre los intercambios entre PC A y Router 1 y entre el resto. Toda la secuencia de ARP y envío de PING.

10. Si la PC A está en una red y se quiere comunicar con la PC B que está en otra red:

- ¿Cómo se da cuenta la PC A de esto?

Se da cuenta porque la dirección IP pertenece a otra subred, ya que analiza la máscara de subred y dirección IP.

- Si la tabla ARP de la PC A está vacía, ¿qué dirección MAC necesita la PC A para poder comunicarse con la PC B?

Si la tabla ARP de la PC A está vacía, la PC A necesitará la dirección MAC del default gateway para poder enviar tráfico a otras redes.

- En base a lo anterior, ¿qué dirección IP destino tiene el requerimiento ARP? ¿Es la dirección IP del default gateway o es la dirección IP de la PC B? Complete los campos:

Trama Ethernet: (mac origen: _MAC_PC-A_ mac destino: _FF:FF:FF:FF:FF:FF_)

Solicitud ARP: (mac origen: _PC-A_ ip origen: _IP_PC-A_)

(mac destino: _00:00:00:00:00:00_ ip destino:
_IP_ROUTER_PC-A_)

- En base a lo anterior, indique la información de capa 2 y 3 del ICMP ECHO REQUEST que la PC A le envía a la PC B cuando ejecuta un ping, en el segmento de LAN de la PC B.

Se supone que la tabla de ARP de la PC-B esta vacía, por lo que debe hacerse una solicitud ARP.

Trama Ethernet:(mac origen: MAC_Router_PC_B mac destino: FF:FF:FF:FF:FF:FF)

Solicitud ARP: (mac origen: MAC_Router_PC_B ip origen: : IP_Router_PC_B)

(mac destino: 00:00:00:00:00:00 ip destino: IP_PC_B)

Del paquete ICMP la IP origen es la IP de PC A y la IP destino es la IP de PC B.