



UTPL
La Universidad Católica de Loja

Vicerrectorado de Modalidad Abierta y a Distancia

Redes de Dispositivos

Guía didáctica





Facultad Ingenierías y Arquitectura

Redes de Dispositivos

Guía didáctica

Carrera	PAO Nivel
Tecnologías de la Información	VI

Autores:

Katty Alexandra Rohoden Jaramillo
Javier Francisco Martínez Curipoma

Reestructurada por:

Liliana Elvira Enciso Quispe
Patricia Jeanneth Ludeña González



D R B D _ 3 0 2 1



Redes de Dispositivos



Guía didáctica

Katty Alexandra Rohoden Jaramillo

Javier Francisco Martínez Curipoma

Reestructurada por:

Liliana Elvira Enciso Quispe

Patricia Jeanneth Ludeña González



Diagramación y diseño digital



Ediloja Cía. Ltda.

Marcelino Champagnat s/n y París

edilojacialtda@ediloja.com.ec

www.ediloja.com.ec



ISBN digital -978-9942-25-933-2

Año de edición: octubre, 2020

Edición: primera edición reestructurada en julio 2025 (con un cambio del 50%)

Loja-Ecuador



Los contenidos de este trabajo están sujetos a una licencia internacional Creative Commons Reconocimiento-NoComercial-CompartirIgual 4.0 (CC BY-NC-SA 4.0). Usted es libre de **Compartir – copiar y redistribuir el material en cualquier medio o formato. Adaptar – remezclar, transformar y construir a partir del material citando la fuente, bajo los siguientes términos: Reconocimiento- debe dar crédito de manera adecuada, brindar un enlace a la licencia, e indicar si se han realizado cambios.** Puede hacerlo en cualquier forma razonable, pero no de forma tal que sugiera que usted o su uso tienen el apoyo de la licenciatante. **No Comercial-no puede hacer uso del material con propósitos comerciales. Compartir igual-Si remezcla, transforma o crea a partir del material, debe distribuir su contribución bajo la misma licencia del original.** No puede aplicar términos legales ni medidas tecnológicas que restrinjan legalmente a otras a hacer cualquier uso permitido por la licencia. <https://creativecommons.org/licenses/by-nc-sa/4.0/>

Índice

1. Datos de información	9
1.1 Presentación de la asignatura.....	9
1.2 Competencias genéricas de la UTPL.....	9
1.3 Competencias específicas de la carrera	9
1.4 Problemática que aborda la asignatura	9
2. Metodología de aprendizaje	10
3. Orientaciones didácticas por resultados de aprendizaje.....	11
Primer bimestre	11
 Resultado de aprendizaje 1:	11
 Contenidos, recursos y actividades de aprendizaje recomendadas.....	11
 Semana 1	11
Unidad 1. Generalidades, capa de red	12
1.1. Procesos y dispositivos de la capa de red	12
1.2. Protocolos de la capa de red.....	24
1.3. Datagrama IPv4.....	25
1.4. Datagrama IPv6.....	26
1.5. Dispositivos de red.....	27
Actividades de aprendizaje recomendadas	33
Autoevaluación 1.....	37
 Resultado de aprendizaje 2:	40
 Contenidos, recursos y actividades de aprendizaje recomendadas.....	40
 Semana 2	40
Unidad 2. Direccionamiento de capa de red.....	40
2.1. Direccionamiento IPv4.....	40
2.2. Direccionamiento IPv6.....	49
Actividades de aprendizaje recomendadas	57
Autoevaluación 2.....	58
 Contenidos, recursos y actividades de aprendizaje recomendadas.....	60

Semana 3	60
Unidad 3. Subredes	60
3.1. División en subredes	60
Actividades de aprendizaje recomendadas	69
Autoevaluación 3.....	71
Resultado de aprendizaje 3:	74
Contenidos, recursos y actividades de aprendizaje recomendadas.....	74
Semana 4	74
Unidad 4. Generalidades de protocolos de enrutamiento	74
4.1. Reenvío y enrutamiento	74
4.2. Funcionamiento de un router	78
4.3. Enrutamiento estático.....	82
Actividades de aprendizaje recomendadas	84
Autoevaluación 4.....	85
Resultado de aprendizaje 4:	89
Contenidos, recursos y actividades de aprendizaje recomendadas.....	89
Semana 5	89
Unidad 5. Algoritmos de enrutamiento	89
5.1. Introducción.....	89
5.2. Algoritmos de enrutamiento.....	92
Actividades de aprendizaje recomendadas	98
Autoevaluación 5.....	99
Resultado de aprendizaje 3:	102
Contenidos, recursos y actividades de aprendizaje recomendadas.....	102
Semana 6	102
Unidad 6. Protocolos de Enrutamiento Dinámico RIP	102
6.1. Protocolo RIP.....	102
Actividades de aprendizaje recomendadas	112
Autoevaluación 6.....	112

Resultado de aprendizaje 5:	115
Contenidos, recursos y actividades de aprendizaje recomendadas.....	115
Semana 7	115
Unidad 7. Protocolos de Enrutamiento Dinámico OSPF.....	115
7.1. Protocolo OSPF	115
Actividades de aprendizaje recomendadas	126
Autoevaluación 7.....	127
Resultados de aprendizaje 1 a 5:.....	130
Contenidos, recursos y actividades de aprendizaje recomendadas.....	130
Semana 8	130
Actividades finales del bimestre	130
Repaso de unidades 1-7	130
Segundo bimestre.....	132
Resultado de aprendizaje 4:	132
Contenidos, recursos y actividades de aprendizaje recomendadas.....	132
Semana 9	132
Unidad 8. Servicios de la capa de transporte.....	133
8.1. Conexión entre capa de red y capa de transporte	133
8.2. La capa de transporte en internet	135
8.3. Multiplexación y demultiplexación.....	136
Actividades de aprendizaje recomendadas	138
Autoevaluación 8.....	139
Contenidos, recursos y actividades de aprendizaje recomendadas.....	141
Semana 10	141
Unidad 9. Transporte sin conexión - UDP	141
9.1. Características de UDP	142
9.2. Estructura de un segmento UDP	142
9.3. Proceso de comunicación en UDP.....	144
Actividades de aprendizaje recomendadas	147

Autoevaluación 9.....	147
Contenidos, recursos y actividades de aprendizaje recomendadas.....	149
Semana 11	149
Unidad 9. Transporte sin conexión - UDP	149
9.4. Aplicaciones que utilizan UDP.....	149
9.5. Diferencias entre UDP y TCP	150
Actividades de aprendizaje recomendadas	152
Autoevaluación 10.....	152
Resultado de aprendizaje 2:	155
Contenidos, recursos y actividades de aprendizaje recomendadas.....	155
Semana 12	155
Unidad 10. Principios de un servicio de transferencia de datos fiable.....	155
10.1. Construcción de un protocolo de transferencia de datos fiable....	156
10.2. Protocolo de transferencia de datos fiable con procesamiento en cadena.....	159
10.3. Retroceder N (GBN)	162
10.4. Repetición Selectiva (SR)	163
Actividades de aprendizaje recomendadas	164
Autoevaluación 11.....	165
Contenidos, recursos y actividades de aprendizaje recomendadas.....	167
Semana 13	167
Unidad 11. Transporte orientado a la Conexión – TCP	168
11.1. Características de TCP	168
11.2. La conexión TCP	169
11.3. Estructura del segmento TCP	171
11.4. Temporización	173
11.5. Transferencia de datos fiable.....	174
Actividades de aprendizaje recomendadas	175
Autoevaluación 12.....	175

Contenidos, recursos y actividades de aprendizaje recomendadas.....	178
Semana 14.....	178
Unidad 11. Transporte orientado a la Conexión – TCP	178
11.6. Control de flujo.....	178
11.7. Gestión de conexión TCP	180
Actividades de aprendizaje recomendadas	182
Autoevaluación 13.....	183
Contenidos, recursos y actividades de aprendizaje recomendadas.....	185
Semana 15.....	185
Unidad 12. Control de congestión.....	185
12.1. Introducción a la congestión.....	185
12.2. Métodos para controlar la congestión	186
12.3. Mecanismo de control de congestión de TCP	187
Actividades de aprendizaje recomendadas	190
Autoevaluación 14.....	191
Resultados de aprendizaje 2 y 4:	194
Contenidos, recursos y actividades de aprendizaje recomendadas.....	194
Semana 16.....	194
Actividades finales del bimestre	194
Repaso de unidades 8-12	194
4. Solucionario	195
5. Referencias bibliográficas	213



1. Datos de información

1.1 Presentación de la asignatura



1.2 Competencias genéricas de la UTPL

Comportamientos éticos.

1.3 Competencias específicas de la carrera

Administrar los servicios de Tecnologías de Información de la organización utilizando buenas prácticas de la industria, asegurando la continuidad operacional del negocio.

1.4 Problemática que aborda la asignatura

La asignatura aborda los aspectos básicos sobre la transmisión de la información en las redes de telecomunicaciones a nivel lógico, y cómo la información es enrutada desde su origen hacia su destino. Además, aborda sobre el manejo de herramientas, configuraciones y dispositivos necesarios para implementar una red de telecomunicaciones.



2. Metodología de aprendizaje

Con el objetivo de aportar al logro de los resultados de aprendizajes, durante el periodo académico se aplicará el proceso metodológico de Aprendizaje por Indagación, que permitirá contribuir con su pensamiento crítico, para que pueda procesar la información mediante el análisis y la síntesis de la misma. Esta metodología permitirá que usted pueda revisar fuentes de consulta como la guía didáctica, libros de consulta, páginas web, artículos científicos, videos tutoriales, que a su vez le permitirán resolver los problemas que se plantean en la asignatura.





3. Orientaciones didácticas por resultados de aprendizaje



Primer bimestre

Resultado de aprendizaje 1:

Diseña y construye múltiples redes y las conecta entre sí.

A través de este resultado de aprendizaje, usted identificará los conceptos básicos sobre la capa de red, aprenderá cómo está estructurada la información y como se direcciona la misma a lo largo de la red, esto se logrará realizando una lectura comprensiva de la guía didáctica, el análisis de los recursos complementarios como videos y la realización de las actividades interactivas.

Contenidos, recursos y actividades de aprendizaje recomendadas

Recuerde revisar de manera paralela los contenidos con las actividades de aprendizaje recomendadas y actividades de aprendizaje evaluadas.



Semana 1

Antes de comenzar, que usted realice las siguientes actividades:

- Instale en su PC el programa [Wireshark](#), que es un software que permite capturar tráfico de red para poder analizar, protocolos, paquetes y tramas que circulan por una red. Le recomendamos seguir las instrucciones de la página de descarga para la [instalación de Wireshark](#).
- Ingrese al portal de [curso de Packet Tracer de Netacad de Cisco®](#), que es un curso gratuito sobre el manejo de una herramienta llamada *Packet*



Tracer, que permite la simulación de redes de datos, una vez inscrito, podrá descargar e instalar esta herramienta. Es recomendable que lo estudie.

- Revise el vídeo titulado [Redes desde cero hasta avanzado](#), del canal de YouTube Master IT, donde podrá recordar los conceptos básicos sobre el modelo OSI y generalidades sobre las redes de datos.

Bienvenido al presente ciclo académico donde le espera conocer mucho sobre el fascinante mundo de las redes de dispositivos. ¡Empecemos!

Unidad 1. Generalidades, capa de red

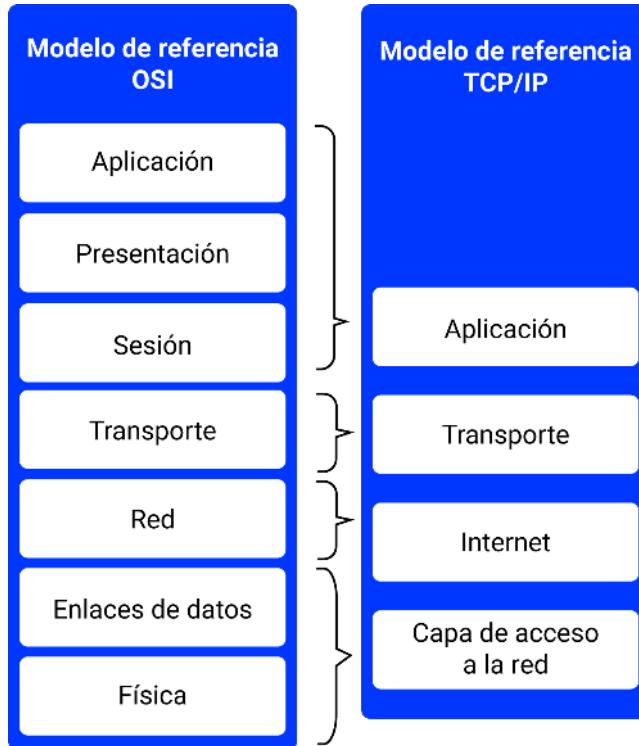
En esta unidad revisaremos los conceptos básicos sobre dispositivos de red y en especial hablaremos de las generalidades de la capa de red del modelo OSI y sobre los protocolos de red. La guía está diseñada de manera que Ud. pueda aprender por su cuenta los conceptos más importantes.

1.1. Procesos y dispositivos de la capa de red

Los contenidos a revisar a continuación están basados en (CISCO, 2019a; Kurose & Ross, 2017; Sánchez et al., 2020). Los hosts o dispositivos en una red usan protocolos que determinan los diferentes intercambios de mensajes y permiten a los mismos ejecutar las funciones para lo que fueron creados. Se debe recordar que en las redes de dispositivos se establecen modelos de referencia de capas que permiten establecer funciones de manera estructurada a los diferentes dispositivos y aplicaciones de la red. En la Figura 1 están el Modelo OSI, el Modelo TCP/IP y las capas que componen cada uno de ellos.

Figura 1

Comparación entre modelos de referencia de 7 capas (OSI) y 4 capas (TCP/IP)



Nota. Tomado de *El modelo OSI y su evolución desde TCP/IP [Ilustración]*, por Marcelo, 2019, [CCNA Desde Cero](#), CC BY 4.0.

Esta asignatura se enfocará en la revisión de las funciones y dispositivos de las capas de ambos modelos que son equivalentes, estas son las capas de red o *Internet* en el primer bimestre y la capa de transporte en el segundo bimestre. A continuación, revisaremos las principales funciones de la capa de red, que son:

- **Encapsulamiento:** agrega el encabezado de la capa de red a los segmentos provenientes de la capa de transporte.
- **Desencapsulamiento:** eliminación de encabezados de las capas inferiores a la capa de red.
- **Direccionamiento lógico:** es la asignación de direcciones a dispositivos e interfaces de la red, que los identifica dentro de la misma.

- **Reenvío y enrutamiento:** dirige los paquetes o datagramas hacia los destinos escogiendo la mejor ruta posible.

Ahora revisemos más a detalle cada uno de estos procesos.

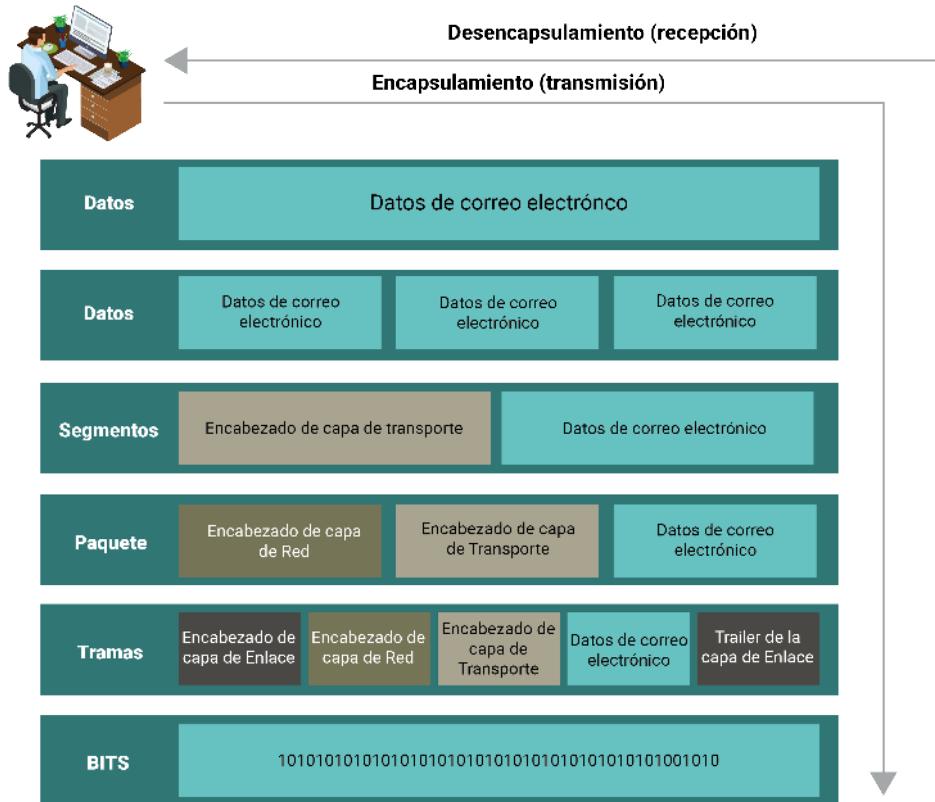
1.1.1. Encapsulamiento y desencapsulamiento

La capa de red o *Internet* es la encargada de enviar, recibir y encapsular los paquetes, que son la unidad de datos de protocolo o por sus siglas en inglés PDU (*Protocol Data Unit*), estos paquetes también son conocidos como *datagramas*. Es necesario identificar las distintas PDU de cada una de las capas y observar cómo se realiza el proceso de encapsulamiento de los datos tanto para transmisión como para recepción.

En la Figura 2, se puede revisar un ejemplo de cómo se realizan estos dos procesos, para lo cual se usa los datos generados por un servicio de correo electrónico. El proceso de encapsulamiento se realiza de arriba hacia abajo donde los datos de la capa de aplicación se dividen en segmentos con su respectivo encabezado del segmento TCP, luego el segmento TCP es encapsulado en un paquete IP y este a su vez es encapsulado en una trama *Ethernet*, luego los *bits* son transmitidos por el medio físico hacia su destino.

Figura 2

Procesos de encapsulamiento y desencapsulamiento de los datos en las diferentes capas



Nota. Tomado de *El modelo OSI y su evolución desde TCP/IP [Ilustración]*, por Marcelo, 2019, [CCNADesdeCero](#), CC BY 4.0.

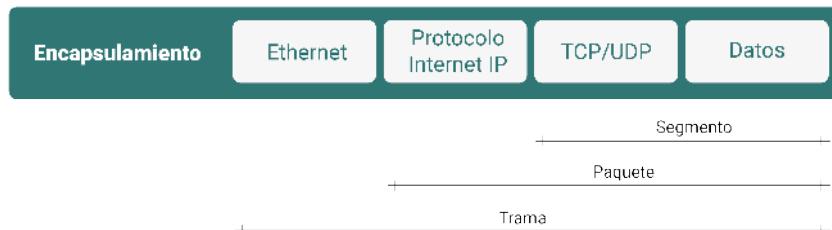
Las PDU de las distintas capas son los siguientes:

- La PDU de la capa de aplicación son los datos.
 - La PDU de la capa de transporte son los segmentos.
 - La PDU de la capa de red o *Internet* son los paquetes o datagramas.
 - La PDU de la capa de enlace son las tramas.
 - La PDU de la capa física son los bits.

Estas PDU se encapsulan de acuerdo a los distintos protocolos de cada capa, siendo su estructura la que se observa en la Figura 3.

Figura 3

Estructura del encapsulamiento de protocolos de acuerdo a la PDU

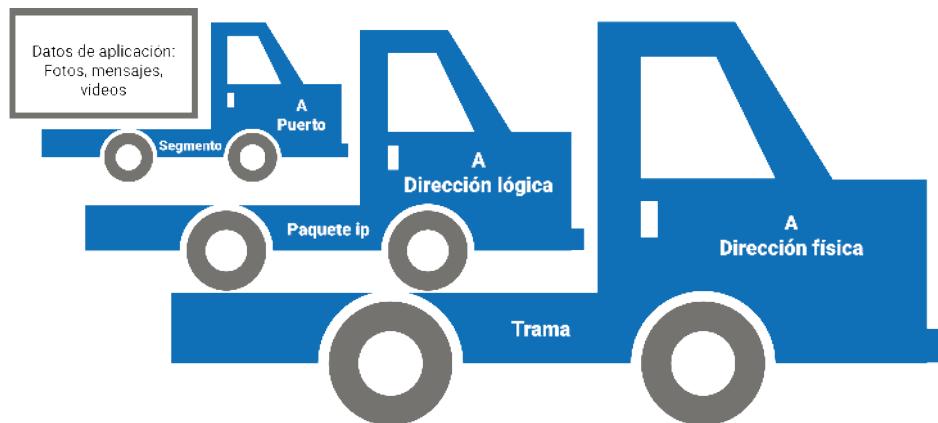


Nota. Rohoden, K., 2024.

En la Figura 3 podemos observar, que los segmentos de la capa de transporte están contenidos en los paquetes IP, y los paquetes IP están contenidos dentro de las tramas Ethernet. Hay que recalcar que en los encabezados se introduce información necesaria para que la información llegue a su destino, como por ejemplo direcciones lógicas, físicas y puertos de aplicaciones. Si hacemos una analogía del proceso de encapsulamiento y PDUs con grúas de plataforma, el encapsulamiento sería como se muestra la Figura 4.

Figura 4

Analogía del encapsulamiento en redes de datos

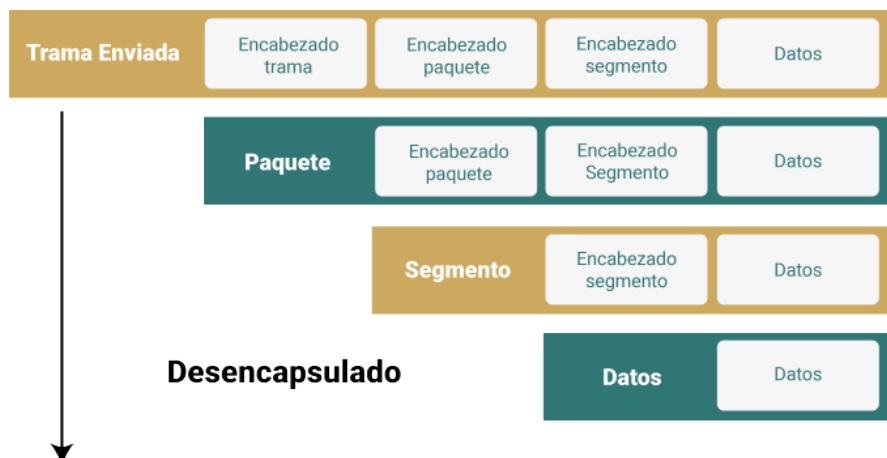


Nota. Rohoden, K., 2024.

Una vez entendido el proceso de encapsulamiento, podemos revisar el proceso de desencapsulamiento que es el proceso en orden inverso, es decir, desde la capa física hasta la de aplicación donde se obtiene cada una de las PDUs. Una vez se recibe las tramas se desecha el encabezado para obtener los paquetes y luego se descarta el encabezado de la capa de red para obtener los segmentos (ver Figura 5).

Figura 5

Proceso de desencapsulamiento realizado para obtención de datos



Nota. Adaptado de *¿Cómo funciona la encapsulación en red? [Ilustración]*, por Pathack, A., 2024, [Geekflare](#), CC BY 4.0.

1.1.2. Direcciónamiento físico

Ahora vamos a aprender sobre la información que permite enviar información del origen al destino, para lo cual se requiere, al igual que cuando enviamos una carta o paquete, conocer el remitente y el destinatario.

En la capa de enlace se usan direcciones físicas o direcciones MAC (*Media Access Control*) que se compone de 48 bits (6 bytes) generalmente representada por caracteres hexadecimales separados por guiones, que son agregadas en el encabezado de trama de la capa de enlace. Por ejemplo, una dirección MAC sería: **AB-CD- EF-01-02-03**, donde los primeros seis caracteres

hexadecimales son denominados como Identificador Único de la Organización (OUI) que es único para cada fabricante asignado por IEEE (Instituto de Ingeniería Eléctrica y Electrónica) y los otros seis restantes se usan para identificar la interfaz de red del dispositivo y que es asignado por el fabricante, igualmente debe ser único (ver Figura 6).

Figura 6

Estructura de una dirección física MAC

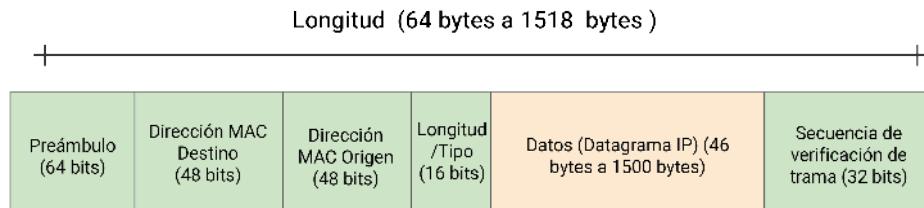


Nota. Rohoden, K., 2024.

Esta dirección es grabada en la memoria del dispositivo y no puede ser cambiada, es usada por los dispositivos de capa de enlace como los switches para realizar la conmutación de las tramas entre las interfaces de los dispositivos mediante direcciones MAC de origen y destino. En la Figura 7, podemos observar el formato de una trama de capa 2 IEEE 802.3 (Ethernet).

Figura 7

Formato de trama Ethernet IEEE 802.3



Nota. Adaptado de *Ethernet II* [Ilustración], por Equipo editorial de IONOS, 2020, [IONOS](#), CC BY 4.0.

Toda trama que tenga un tamaño menor a 64 bytes o mayor a 1518 bytes es desechada por los dispositivos. Cuando en la dirección MAC de destino se tiene todos los bits en uno, es decir FF-FF-FF-FF-FF-FF se envía la trama a todos los hosts en el segmento de red.

1.1.3. Direccionamiento lógico

En la capa de red, se usan las denominadas direcciones lógicas, que son definidas por los protocolos de *Internet* versión 4 (IPv4) y la versión 6 (IPv6). Si hacemos una analogía, una dirección lógica sería el número de cédula o identidad de una persona y la dirección física sería la dirección del domicilio donde vive. A diferencia de las direcciones MAC, estas pueden ser configuradas en la interfaz de red.

El Protocolo de *Internet* IP agrega un encabezado IP al segmento de la capa de transporte, donde se agrega las direcciones IP (direcciones lógicas) que permiten enviar los datos desde el *host* de origen al destino. El protocolo IP es un protocolo que envía al destino sin establecer una conexión previa, por lo que no fue diseñado para monitorear a los paquetes o controlar el flujo de los mismos. Con esto se logra que IP sea un protocolo con bajos requerimientos y que no sobrecarga los sistemas.

El protocolo IP se considera un protocolo no confiable, ya que no garantiza la entrega de paquetes, debido a que los destinatarios pueden o no existir, o ser accesibles para realizar la entrega. Tampoco permite recuperar paquetes no recibidos o dañados. El protocolo IP es independiente del medio en el que viajan los datos como cobre, fibra óptica o inalámbricos. Más adelante en el curso aprenderemos cómo están estructurados los encabezados en las dos versiones del protocolo IP y el formato de las direcciones IP.

Ahora revisaremos unos de los procesos más importantes en la capa de red, el enrutamiento.



1.1.4. Reenvío y enrutamiento

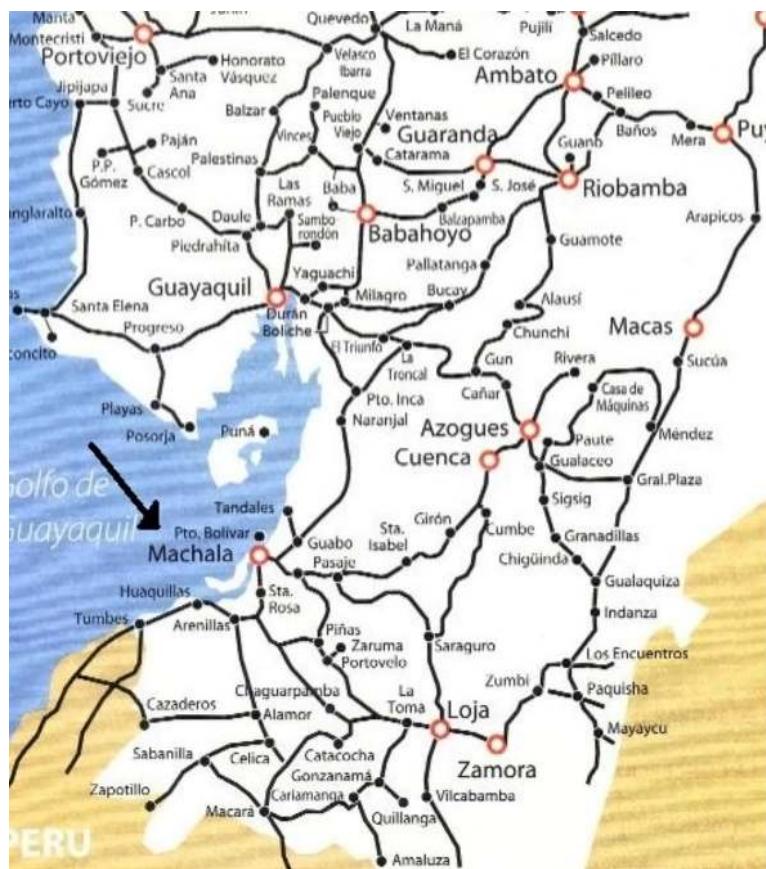
Como revisamos anteriormente en la capa de red se añaden las direcciones lógicas que permiten enviar los paquetes a su destino, ahora veamos cómo es el proceso para enviar estos paquetes a través de la red, por la mejor ruta posible. Pero ¿cómo se lleva a cabo la elección de la mejor ruta?, veamos un ejemplo cotidiano. Cuando decidimos ir de una ciudad a otra, en este caso Loja a Guayaquil.

Según la Figura 8 donde se muestra el mapa vial, existen varias opciones para llegar al destino, los criterios que se utilizan para elegir la mejor ruta serían la longitud, las condiciones de la vía, la congestión, número de carriles, condiciones climáticas, entre otras. Una vez analizado estos aspectos se toma una decisión y escogemos una ruta.



Figura 8

Las rutas posibles de conexión entre Loja y Guayaquil



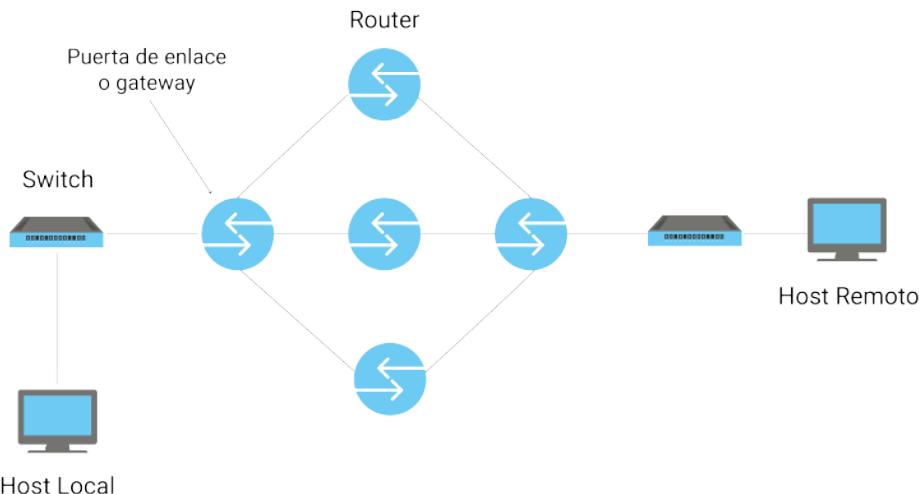
Nota. Tomado de Machala [Ilustración], por Aroma de Café, s.f., [WordPress](#), CC BY 4.0.

De la misma manera, esto se realiza en las redes de dispositivos, donde los datos deben viajar desde el *host* donde se originan, a otro *host* de destino ubicado por ejemplo en otro continente, en el proceso de enrutamiento se debe elegir la mejor ruta, tomando diversos criterios como ancho de banda, número de saltos, velocidad, entre otros. Este proceso es implementado por los dispositivos de capa de red como son los *routers* o enrutadores que usan las direcciones IP para la toma de decisiones y elección de la mejor ruta.

En la Figura 9 se puede observar una red de dispositivos, con varios enruteadores interconectados entre sí, que dan varias rutas que pueden seguir los paquetes para llegar desde el *host local* que emite la información, al *host remoto* que se encuentra en otra red.

Figura 9

Ejemplo de red para comunicación remota entre *host local* y *host remoto*



Nota. Rohoden, K., 2024.

Es necesario definir algunos elementos que intervienen en el proceso de enruteamiento, como son:

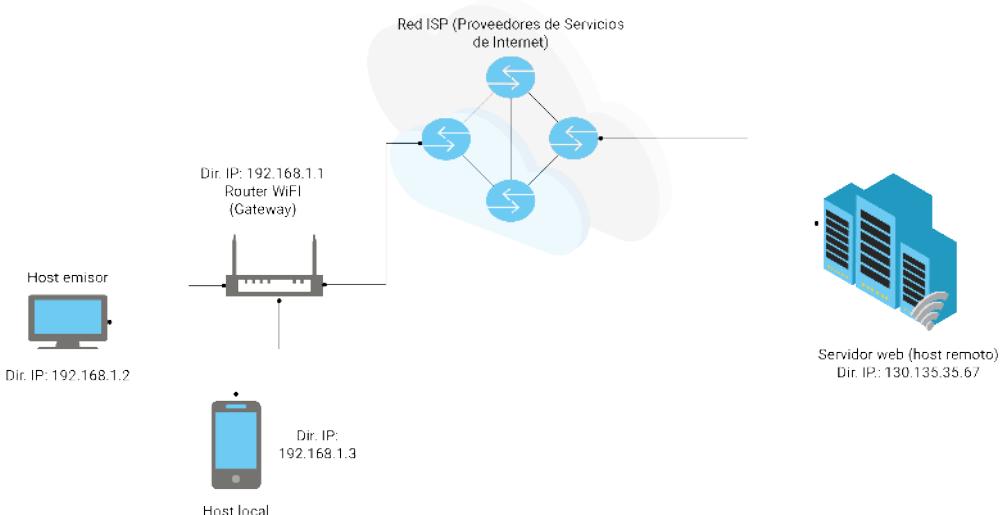
- **Host local:** es el dispositivo que se encuentra en la misma red que el dispositivo que genera la información, es decir que pueden tener la misma dirección lógica de red.
- **Host remoto:** es un *host* en una red remota, es decir que no tiene la misma dirección de red que el dispositivo que emite la información.
- **Puerta de enlace o gateway:** es el dispositivo que permite enrutar el tráfico a redes remotas. Todo dispositivo que quiere comunicarse con host remoto debe enviar primero la información al gateway y este a su vez, lo reenviará a las redes remotas.

Pero ¿cómo se comunica mi computadora al *Internet*?

Para responder esta pregunta veamos el diagrama en la Figura 10, donde se muestra un ejemplo básico de una red doméstica conectada al Internet.

Figura 10

Ejemplo de red doméstica conectada a internet



Nota. Rohoden, K., 2024.

Veamos cómo se realiza el proceso de enrutamiento al establecer una comunicación desde la computadora que sería el *host emisor*:

El *host emisor* desea comunicarse con servidor web (*host remoto*), para lo cual debe enviar una trama a la interfaz de su puerta de enlace o *gateway* agregando un encabezado de capa 2 con la dirección física MAC de esa interfaz como destino, que en este caso es el *router* inalámbrico por medio de wifi. Fíjese que tanto el *host emisor* como el *gateway* tienen la misma dirección IP de red (192.168.1.x).

1. El *gateway* descarta el encabezado de capa 2 y añade nueva información, envía la nueva trama a la interfaz de otro *router* que pertenece a *Internet* o red de Proveedores de Servicios de Internet ISP, usando cable de cobre, fibra óptica o medio inalámbrico.

2. En la red de *Internet* se realizan la toma decisiones por medio de los *routers*, los paquetes pasarán por muchos *routers* y tipos de medios físicos como cobre, fibra óptica, saltos satelitales, cables submarinos. Aquí se elige la mejor ruta para llegar hacia el *host remoto*.
3. Una vez que se enrutan los paquetes hacia el *host remoto*, este verifica que sean para él y los procesa, y luego envía la información solicitada, y el proceso se repite para llegar hacia el *host emisor*.

Por último, también veamos cómo se puede comunicar el *host emisor* con el *host local*, en este caso el *host emisor* envía directamente la trama a la interfaz del *host local* usando la dirección MAC de la misma como destino, y en el paquete se usa la dirección IP del *host local* como destino, los paquetes pasan por el *gateway* sin ser procesados, y son reenviados al *host local*. Note que tanto el *host emisor*, *host local* y *gateway* tienen la misma dirección de red (192.168.1.x).

Una vez revisado el tema anterior, estudiemos los dispositivos de red y los datagramas IPv4 e IPv6, así como los principales protocolos que operan en la capa de red, para entender mejor cómo se gestionan y transmiten los datos en una red.

Fundamentos y dispositivos de la capa de red

1.2. Protocolos de la capa de red

Existen varios protocolos de red, los más usados actualmente son Protocolos de *Internet* versión 4(IPv4) y la versión 6 (IPv6). Estos protocolos están definidos en las RFC (*Request For Comment*) que establecen los lineamientos y arquitectura de los mismos, en el caso de IPv4 se define en la RFC791 e IPv6 se define en el RFC2460 y RFC4291. Estos protocolos soportan a los procesos de capa de red como son encapsulamiento, desencapsulamiento, enrutamiento y direccionamiento.

Veamos más a fondo el proceso de direccionamiento; este proceso permite asignar direcciones lógicas a los dispositivos de la red que en conjunto con las direcciones físicas de los mismos permiten establecer la comunicación entre dispositivos. Para las comunicaciones deben agregarse una dirección IP de origen y una de destino en el encabezado del paquete IP, que son procesadas por los dispositivos de red. Estos protocolos son fundamentales en el funcionamiento de las redes de dispositivos, por ello es muy importante que usted domine los mismos.

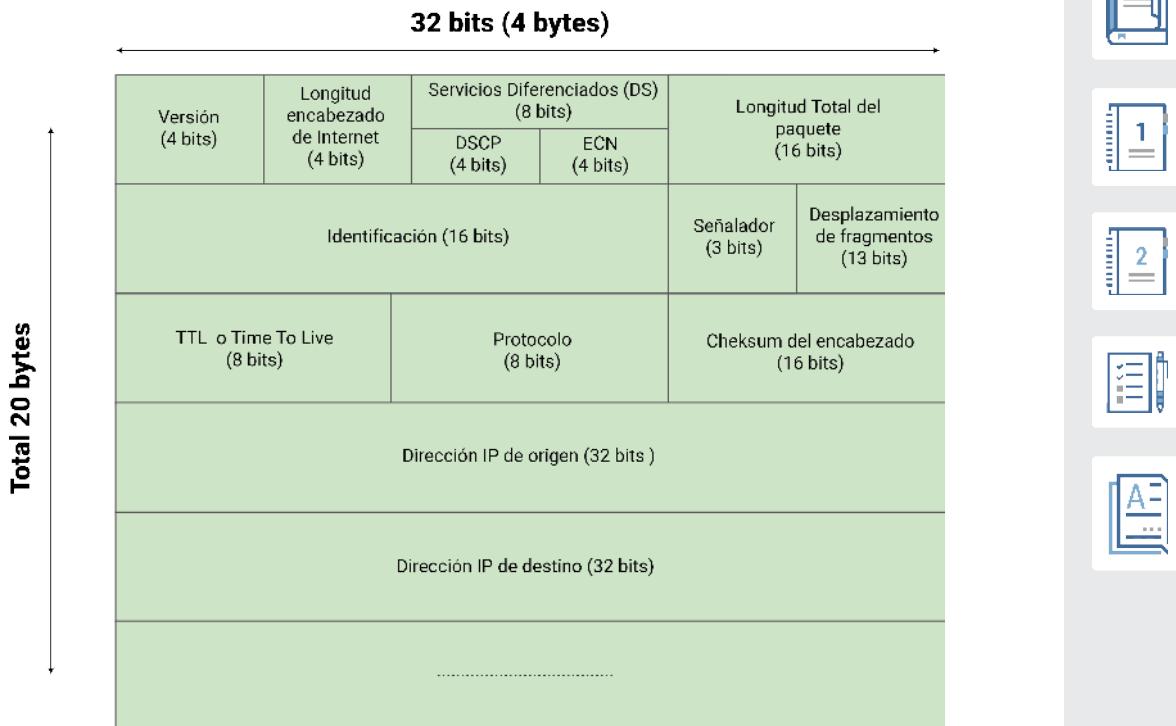
Le invito a continuar con el aprendizaje revisando el formato de los datagramas IP en las versiones 4 y 6 y los dispositivos red.

1.3. Datagrama IPv4

El datagrama IP o paquete permite establecer cómo se estructuran los encabezados de los protocolos IP y el significado de cada uno de los *bits* o grupo de *bits* que lo componen. El formato del encabezado IPv4 está representado por una matriz cuyas filas tienen una longitud de 32 *bits* (ver Figura 11), donde se delimitan los campos que forman el encabezado que tiene una longitud de 20 *bytes* en total, hay que recalcar el datagrama tiene una longitud variable y una longitud máxima de 1500 *bytes* incluido el encabezado y los datos si el protocolo usado en capa 2 es Ethernet.

Figura 11

Formato del encabezado de un datagrama IPv4



Nota. Adaptado de *REDES DE COMPUTADORAS: Un enfoque descendente* (p. 274) [Ilustración], por Kurose, J., y Ross, K., 2017, Pearson Education, CC BY 4.0.

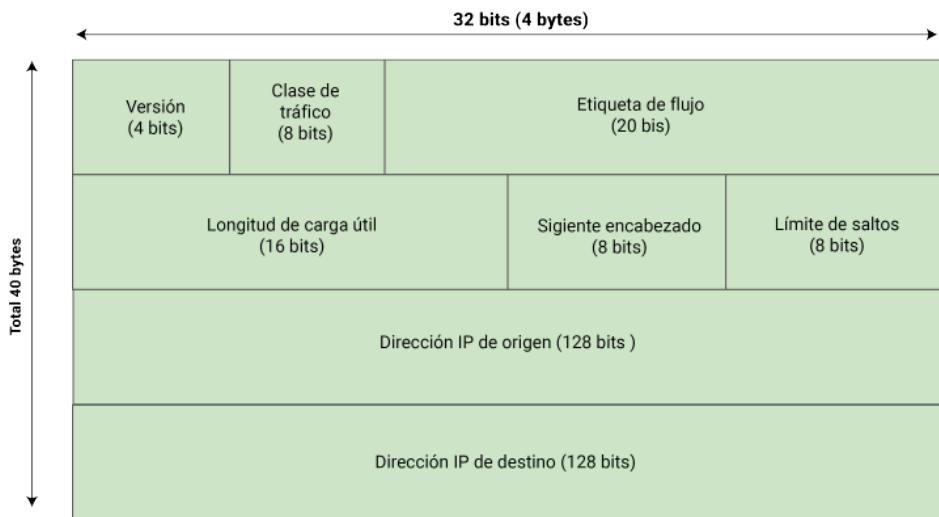
Si observamos la Figura 11 las direcciones IPv4 de origen y destino tienen 32 bits de longitud.

1.4. Datagrama IPv6

IPv6 fue creado para reemplazar a IPv6, dadas las dificultades presentadas por la escasez de direcciones IPv4 dado el incremento del número de dispositivos conectados a la red. Las direcciones IPv6 tienen una longitud de 128 bits, el encabezado del datagrama tiene una longitud de 40 bytes, que es mayor al de IPv4. Se han eliminado algunos campos en el encabezado y se han añadido otros, el formato del encabezado del datagrama IPV6 se puede observar en la Figura 12.

Figura 12

Formato del encabezado de un datagrama IPv6



Nota. Adaptado de *REDES DE COMPUTADORAS: Un enfoque descendente* (p. 274) [Ilustración], por Kurose, J., y Ross, K., 2017, Pearson Education, CC BY 4.0.

Si observamos el encabezado del datagrama IPv6 es mucho más sencillo comparado con IPv4, pero tiene mayor longitud debido a que las direcciones IPv6 tienen mayor número de bits.

1.5. Dispositivos de red

Antes de comenzar el aprendizaje de los conceptos es necesario conocer los distintos dispositivos que forman las redes y sus funciones básicas.

1.5.1. Host o terminal

Son todos los dispositivos que tengan una interfaz de red y puedan conectarse a la red por cualquier medio alámbrico o inalámbrico. Por ejemplo, computadoras, consolas de juegos, celulares, tablets, laptops, TV, entre otros.

1.5.2. Interfaz de Red o NIC

Es el punto que permite conectar un dispositivo a una red de datos, por medio de cualquier medio como cable UTP, fibra óptica o medio inalámbrico. Para conexiones con cable UTP usamos el puerto del tipo RJ45 que podemos encontrar en la mayoría de los dispositivos como *laptops*, TV, consolas de juegos, entre otros (ver Figura 13).

Figura 13

Interfaz de red cableada del tipo RJ45



Nota. Tomado de *Man plugs internet cable into the router. Ethernet connection concept* [Fotografía], por Proxima Studio, 2019, [Shutterstock](#), CC BY 4.0.

Para una red inalámbrica, esta interfaz se conoce como adaptador wifi, que puede ser interno o externo, y permite comunicarse al dispositivo con el punto de acceso inalámbrico AP.

1.5.3. Hubs o concentradores

Son dispositivos que trabajan en la capa física que son utilizados para regenerar la señal y dividir la señal proveniente de un enlace principal, estos dispositivos pueden producir varios errores debido a que propagaban las

colisiones que se dan en las señales de red, por lo que no es recomendable su uso en redes de datos. Actualmente, están en desuso en las redes de datos, pero podemos encontrarlos para aplicaciones como USB.

1.5.4. Switches o conmutadores

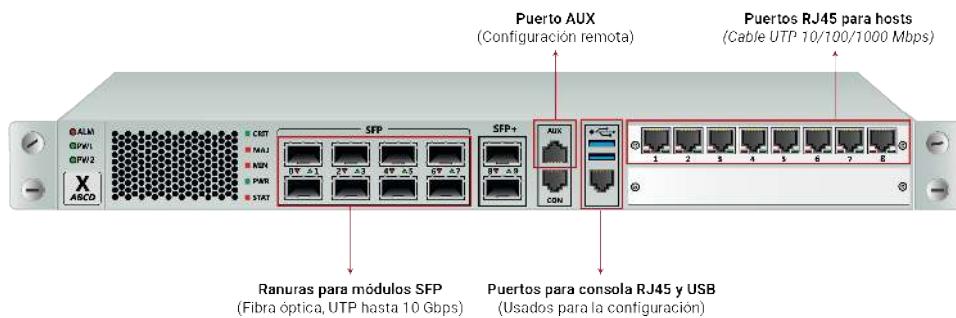
Son dispositivos de capa de enlace o capa 2 que usan las direcciones físicas para realizar la conmutación de las tramas hacia los destinos. Solo procesan la información existente en el encabezado de la trama de *Ethernet*, es transparente a la información de las otras capas. A diferencia de los hubs, pueden tomar decisiones con base en una tabla de direcciones MAC donde tienen asociadas las direcciones físicas con la interfaz de red a la que están conectadas. Estos dispositivos poseen varias interfaces de red 4, 8, 16, 24 o 48 puertos RJ45 con velocidades de hasta 1000 Mbps, los cuales permiten segmentar el dominio de colisión, lo que evita que estas se propaguen por la red.

Si un *switch* desconoce la interfaz a la que está conectada, una dirección física de destino envía la trama a todos sus puertos, excepto por el que recibió la trama, y al recibir una respuesta del destino guarda esa información en la tabla de direcciones MAC. Estos dispositivos pueden ser instalados en escritorios y racks de telecomunicaciones, permite interconectar varios dispositivos que estén en la misma subred. También existen un tipo de *switch* de capa 2/3 que puede procesar cierta información del encabezado IP, para permitir la comunicación entre subredes.

Estos dispositivos poseen algunos puertos que se los puede observar en la Figura 14.

Figura 14

Puertos del switch o comutador capa 2, modelo Cisco2960 de 24 puertos



Nota. Adaptado de enrutador 10G para montaje en rack de 19" con módulos SFP a SFP+, panel para conectores de control, panel adicional con 8 conectores RG-45 y panel redundante adicional. [Ilustración], por vs_vadim, 2022, [Shutterstock](#), CC BY 4.0.

Los puertos RJ45 se usan para la conexión de *hosts* o terminales, por medio de cable UTP, las ranuras para módulos SFP (*Small Form-factor Pluggable*) que permiten conectar enlaces principales a otras redes u otros dispositivos como *routers* o *switches*, por medio de fibra óptica o UTP hasta velocidades de 10 gbps. Los puertos de consola permiten configurar el *switch* mediante un cable de consola conectado a un puerto USB de una PC, donde se encuentra instalado un programa de terminal que permite acceder al *switch* y configurarlo. El puerto AUX o auxiliar se usa para conectar a líneas que permitan la configuración de manera remota mediante los protocolos de comunicación Telnet o SSH. **Recuerde que en las interfaces de un switch no se configura direcciones IP.**

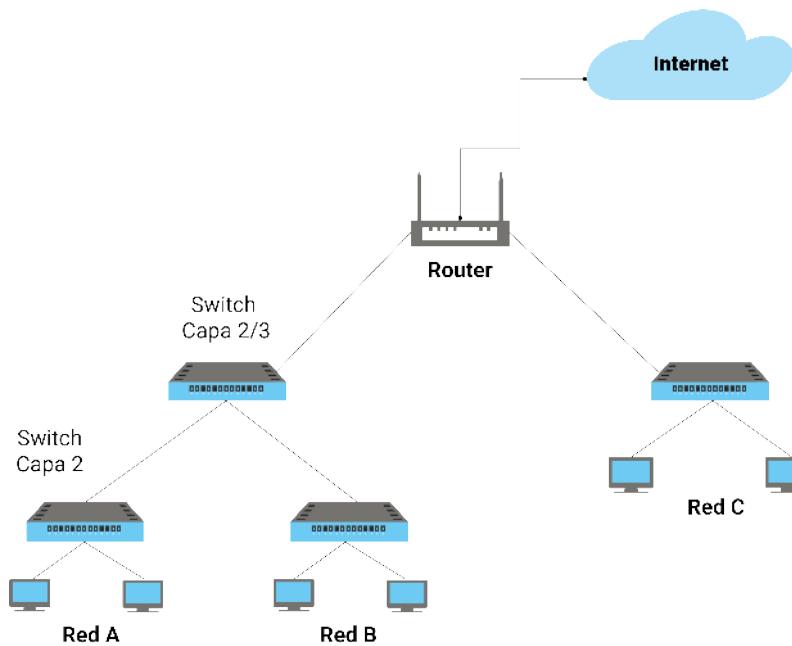
1.5.5. Routers o enrutadores

Son dispositivos de capa de red o capa 3, estos tienen una CPU, memoria y sistema operativo, es decir, una computadora dedicada a los servicios de red.

Este dispositivo permite conectar la red de una empresa a otras redes externas como por ejemplo la del proveedor de *Internet*, también permiten intercomunicar subredes de la empresa. En otras palabras, el enrutador permite aislar el tráfico interno de la red de otras redes e *Internet*, conecta una red LAN con una WAN (ver Figura 15).

Figura 15

Ejemplo de red de una empresa con varias redes interconectadas por un router

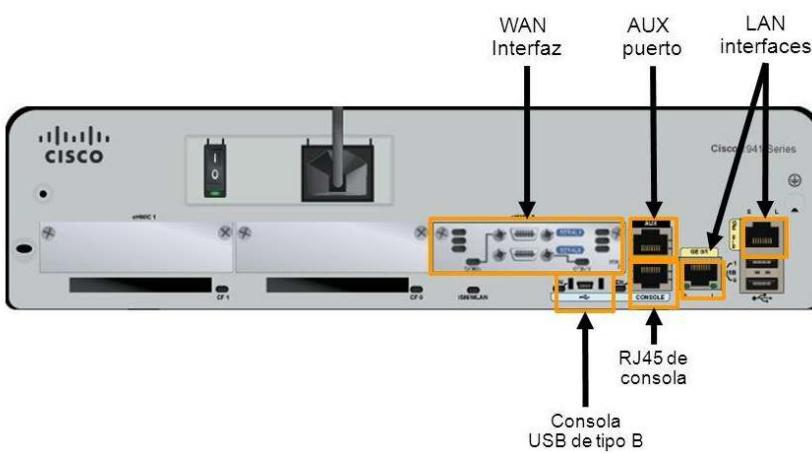


Nota. Rohoden, K., 2024.

Para realizar las conexiones al router se le puede añadir módulos que permitan conectar redes WAN o LAN mediante cable UTP, fibra óptica y conexiones seriales, por cada interfaz se podrá conectar una red diferente. Estas interfaces se pueden observar en la Figura 16. Las *interfaces del router* que se conecten deberán tener configurada una dirección IP.

Figura 16

Interfaces de un enrutador, en este caso marca Cisco modelo 1941

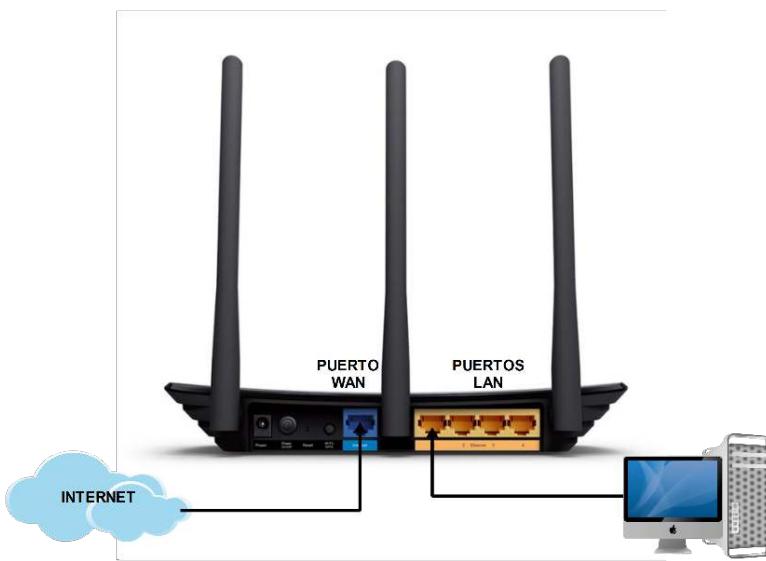


Nota. Adaptado de *Temel Router Yapılandırması* [Ilustración], por Mustafa İkbal Yaşar, 2024, [Medium](#), CC BY 4.0.

Algunos routers como es el caso de los domésticos o para pequeñas empresas, poseen un switch que permite conectar los hosts o terminales directamente al router (ver Figura 17).

Figura 17

Interfaces de un enrutador doméstico, modelo TP-Link TL-WR940N



Nota. Adaptado de *Router inalámbrico N 450Mbps* [Ilustración], por tp-link, s.f., [tp-link](#), CC BY 4.0.



Actividades de aprendizaje recomendadas

Con el objetivo de profundizar los conocimientos adquiridos, le invito a desarrollar las siguientes actividades:

1. Revise el vídeo titulado [Proceso de encapsulamiento de datos en modelo OSI y TCP/IP](#), donde podrá comprender de mejor manera el proceso de encapsulamiento en las redes de telecomunicaciones.

Tenga en cuenta que la capa de red transporta varios tipos de comunicación e información, ya que solo analiza la información de capa 3 y encapsula la información de capas superiores. En la capa de red se añade el encabezado que contiene las direcciones lógicas de la capa de red. Este proceso se denomina direccionamiento lógico, pero antes tenemos que revisar el direccionamiento físico que se realiza en la capa 2 del modelo OSI.

2. Es importante que comprenda la función de cada uno de los campos de la trama *Ethernet*, por ello le recomiendo revisar el artículo titulado [Trama Ethernet](#), donde se muestra la función de cada uno de estos campos.

3. Para complementar la teoría con la práctica, vamos a averiguar cuál es la dirección IP y MAC de nuestra PC que deberá estar conectada a una red inalámbrica o cableada. Para lo cual seguiremos los siguientes pasos:

- Estando en el escritorio de Windows, presionar las teclas:



- Escribimos en el cuadro de diálogo el comando: cmd y presionamos la tecla enter.



- Se abrirá la consola de Windows, donde ingresaremos el comando: ipconfig /all y presionamos la tecla enter.



- Aquí se desplegará toda la información sobre las interfaces de red conectadas y desconectadas que posee su PC, únicamente la que está conectada a la red mostrará información como la dirección IP asignada y dirección física MAC. Un ejemplo se puede observar en la Figura 18.



Figura 18

Ejemplo de información desplegada por el comando ipconfig /all de Windows

```
Adaptador de Ethernet Ethernet:  
  Sufijo DNS específico para la conexión. . . : utpl.edu.ec  
  Descripción . . . . . : Intel(R) Ethernet Connection (4) I219-V  
  Dirección física. . . . . : 54-E1-AD-EC-77-25  
  DHCP habilitado . . . . . : sí  
  Configuración automática habilitada . . . . . : sí  
  Vínculo: dirección IPv6 local. . . . . : fe80::3809:2594:e460:73d5%15(Preferido)  
  Dirección IPv4. . . . . : 172.18.4.166(Preferido)  
  Máscara de subred . . . . . : 255.255.255.0
```

Nota. Rohoden, K., 2024.

- Las interfaces no conectadas solo mostrarán la dirección física de fábrica, observe como todas tienen distinta dirección MAC. La dirección IP se asigna al momento de ser conectada.

4. Ahora vamos a averiguar la dirección IP de la puerta de enlace a la que su PC envía la información para conectarse a *Internet*. Para lo cual seguiremos los siguientes pasos:

- Estando en el escritorio de Windows, presionar las teclas:



- Escribimos en el cuadro de diálogo el comando: cmd y presionamos la tecla Enter.



- Se abrirá la consola de Windows, donde ingresaremos el comando: ipconfig y presionamos la tecla enter.



- Aquí se desplegará información básica sobre las interfaces de red conectadas y desconectadas que posee su PC, únicamente.

- La que esté conectada a la red mostrará información como la dirección IP asignada, dirección física MAC, y la puerta de enlace predeterminada, esta última sería la dirección de su *gateway*. Un ejemplo se puede observar en la Figura 19.



Figura 19

Ejemplo de información desplegada por el comando ipconfig, donde se puede observar la puerta de enlace o gateway

Adaptador de Ethernet Ethernet:

```
Sufijo DNS específico para la conexión. . . : utpl.edu.ec  
Vínculo: dirección IPv6 local. . . : fe80::3809:2594:e460:73d5%15  
Dirección IPv4. . . . . : 172.18.4.166  
Máscara de subred . . . . . : 255.255.255.0  
Puerta de enlace predeterminada . . . . . : 172.18.4.1
```

Nota. Rohoden, K., 2024.

- Usando esta dirección podríamos acceder al gateway, por ejemplo, para configurar la contraseña de WiFi, usando un navegador ingresamos en la barra de direcciones la dirección IP obtenida y presionamos la tecla Enter . Con esto podremos acceder a la pantalla de login del router inalámbrico. Está claro que debemos saber el usuario y contraseña del mismo.

5. Revise la siguiente presentación sobre el [Protocolo IPv4](#), especialmente encontrará los tipos de direcciones disponibles para IPv4

Debido a las exigencias actuales de las redes mundiales, las direcciones IPv4 se están agotando por lo que es necesario migrar a una nueva versión con mayor cantidad de direcciones disponibles como lo es IPv6 que vamos a revisar a continuación.

6. Revise el material disponible en el enlace [Protocolo IPv6: direccionamiento](#) donde encontrará la función de cada uno de los campos del datagrama IPv6.

7. De lectura de la información sobre [Mecanismos de reenvío de paquetes en un router](#), donde podrá conocer cómo el router trata los

paquetes para llevarlos desde la interfaz de entrada a la interfaz de salida.

8. Revise el video del canal de YouTube, Mastering IT, titulado [¿Cómo funcionan los routers y los switches dentro de una red?](#) Donde podrá complementar la lectura para conocer el funcionamiento y partes de un switch.
9. Posteriormente, lo invito a revisar, y a realizar la siguiente autoevaluación, donde podrá aplicar sus conocimientos adquiridos. Si su nota es baja, por favor, vuelva a leer y revisar los contenidos.



Autoevaluación 1

Dado los siguientes enunciados, escoja la respuesta correcta:

1. Un paquete IP contiene a:
 - a. Los segmentos.
 - b. Las tramas.
 - c. Dirección MAC.
2. Un *router* es un dispositivo de:
 - a. Capa 1.
 - b. Capa 2.
 - c. Capa 3.
3. Un *host* para comunicarse con un *host* remoto debe enviar la información:
 - a. Directamente al *host* remoto.
 - b. A un *switch*.
 - c. A su puerta de enlace.
4. La longitud total del encabezado del paquete IPv4 es:
 - a. 10 bytes.
 - b. 20 bytes.





- c. 30 bytes.
- d. 40 bytes.

5. La longitud total del encabezado del paquete IPv6 es:

- a. 10 bytes.
- b. 20 bytes.
- c. 30 bytes.
- d. 40 bytes.

6. El campo del datagrama IPv4 que es un contador que se reduce en uno cada vez que pasa por un *router* es:

- a. TTL.
- b. Versión.
- c. Checksum.
- d. Longitud del paquete.

7. El tamaño máximo del paquete IP incluido el encabezado y los datos es de:

- a. 20 bytes.
- b. 100 bytes.
- c. 1000 bytes.
- d. 1500 bytes.

8. Una dirección MAC o física se compone de:

- a. 48 bits.
- b. 32 bits.
- c. 24 bits.
- d. 64 bits.

9. La dirección MAC puede ser cambiada en el dispositivo:

- a. Verdadero.
- b. Falso.

10. El PDU de la capa de red es:

- a. Tramas.
- b. Paquetes.
- c. Segmentos.
- d. Datos.

[Ir al solucionario](#)



Resultado de aprendizaje 2:

Diseñar y dimensionar escenarios de red.

Para lograr el resultado de aprendizaje en esta unidad aprenderá la estructura de las direcciones lógicas tanto del protocolo IPv4 e IPv6, así mismo aprenderá como configurar las direcciones IP en los dispositivos que le permitirá configurar una red para trabajar en distintos escenarios.

Contenidos, recursos y actividades de aprendizaje recomendadas

Recuerde revisar de manera paralela los contenidos con las actividades de aprendizaje recomendadas y actividades de aprendizaje evaluadas.



Semana 2

Unidad 2. Direccionamiento de capa de red

Esta semana revisaremos el formato y estructura de las direcciones lógicas tanto en su versión IPv4 e IPv6, los contenidos explicados están basados en (CISCO, 2019a; Sánchez et al., 2020).

2.1. Direccionamiento IPv4

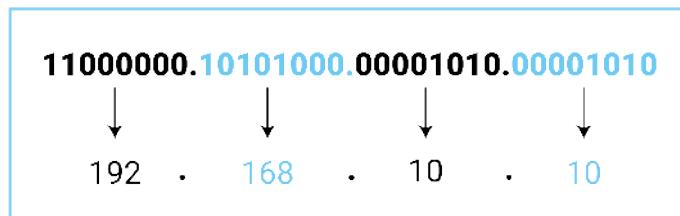
El direccionamiento IPv4 es un componente esencial en el funcionamiento de las redes de dispositivos, ya que permite identificar de manera única cada equipo conectado y facilitar la transmisión eficiente de datos. Este sistema, basado en direcciones numéricas de 32 bits, establece la estructura y organización de la red, definiendo tanto las direcciones de los hosts como la segmentación en subredes. Comprender su funcionamiento es fundamental para diseñar, configurar y administrar redes que optimicen el uso de recursos, garanticen la comunicación entre dispositivos y mantengan la integridad de la información en entornos locales y globales.

2.1.1. Estructura de la dirección IP

Las direcciones lógicas en IPv4 usan el sistema binario, ya que se representan mediante un conjunto de 1s y 0s. Para el caso de IPv4, se representan mediante 32 bits agrupados en cuatro octetos (8 bits) o bytes separados por un punto. También se usa la notación decimal, donde cada octeto se reemplaza por el número decimal equivalente (ver Figura 20).

Figura 20

Representación de dirección IPv4 de 32 bits en notación decimal punteada



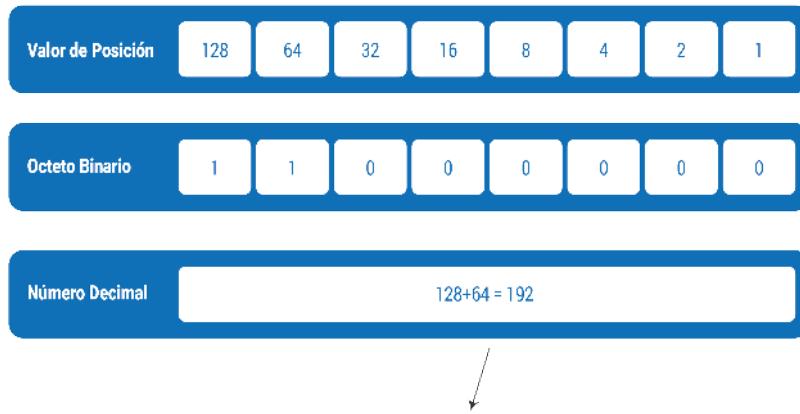
Nota. Rohoden, K., 2024.

Cada uno de los bits dentro del octeto representa a una potencia de 2 de acuerdo a su posición, para convertir el octeto a decimal solamente debemos sumar el valor de la posición de los bits que están en 1 (ver Figura 21).

Figura 21

Conversión del octeto en binario a número decimal

11000000.10101000.00001011.00001010



Nota. Rohoden, K., 2024.

Ejemplo: Convertir la dirección IP 11011000.10001000.00001010.10101000 a formato decimal.

Reemplazamos los 1s por el valor de posición en el octeto y los sumamos:

- Octeto 1: $128 + 64 + 16 + 8 = 216$
- Octeto 2: $128 + 8 = 136$
- Octeto 3: $8 + 2 = 10$
- Octeto 4: $128 + 32 + 8 = 168$

Luego la dirección IP sería: **216.136.10.168**

Recuerde que cada octeto puede tener un valor máximo de 255, ya que es la suma de $128 + 64 + 32 + 16 + 8 + 4 + 2 + 1 = 255$, cuando todos los bits del octeto están en 1.

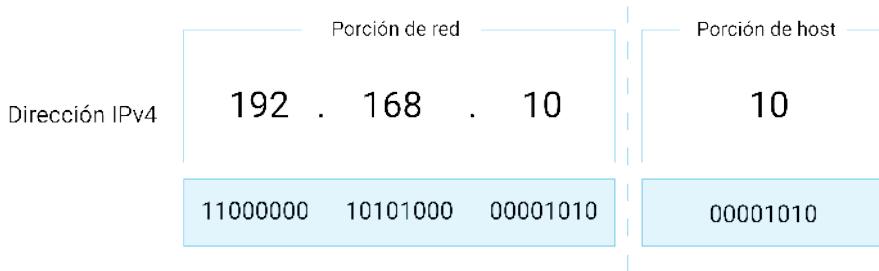
Para convertir la dirección de decimal a binario, es necesario convertir el octeto en decimal a su equivalente en binario.

Estas direcciones son asociadas a las interfaces de red de cada dispositivo conocidas como NIC (Network Interface Card), que tienen configurada una dirección física MAC de fábrica, y a la que debemos configurar una dirección IP exclusiva para que se pueda conectar a la red. Un dispositivo puede tener varias interfaces como en el caso de switches y routers, que permiten la conexión a la red por medio de varios medios como cobre, fibra y canales inalámbricos. Dado que IPv4 tiene una longitud de 32 bits, por lo que existen 2^{32} direcciones posibles, es decir, aproximadamente unos 4200 millones de direcciones.

Adicionalmente la dirección está estructurada con una porción de los bits para representar a la dirección de red y otra porción para asignar al host que pertenece a la red. Los bits que se usan para representar la porción de red se toman desde la izquierda, pueden tomarse 1 bit hasta 30 bits, y los bits restantes se usan para la porción de host (ver Figura 22).

Figura 22

Porción de red y porción de host en una dirección IPv4 (CISCO, 2019a)



Nota. Adaptado de *Qué es una máscara de subred y cómo descubrirla [Ilustración]*, por Adeva, R., 2025, [adslzone](#), CC BY 4.0.

En la Figura 22 se puede observar que se han tomado 24 bits para la porción de red y los restantes 8 bits son para la porción de host. Con estas porciones se podría representar hasta 2^{24} (16 777 216) redes, con 2^8 (256) dispositivos cada una de ellas. La dirección de red o también denominada subred sería 192.168.1.0, donde se colocan los bits de la porción de host en 0.

Para representar el número de bits que forman parte de la porción de red, se puede usar la siguiente notación 192.168.1.0/24 donde el prefijo /24 indica cuantos bits desde la izquierda de la dirección se usan para representar a la dirección de subred, en este caso indica que son 24 bits.

2.1.2. Tipos de direcciones IP

Ahora veamos qué tipos de direcciones IP existen, y cuáles son sus características:

- **Dirección de red:** es la dirección IP que tiene la porción de *host* en 0. Ejm: 192.168.10.0/24, el prefijo /24 indica que el último octeto es la parte de *host* y que está en 0. Esta dirección no puede asignarse a ningún *host* o terminal.
- **Dirección de difusión o broadcast:** es la dirección IP que tiene la porción de *host* en 1. Ejm: 192.168.10.255/24, el prefijo /24 indica que el último octeto es la parte de *host* y que está en 1. Esta dirección no puede asignarse a ningún *host* o terminal. Al usar esta dirección como destino se envían los paquetes a todos los dispositivos que pertenecen a la red.
- **Dirección de host:** son las direcciones que pueden ser configuradas en los terminales, y están comprendidas entre la dirección de red y Ejemplo: 192.168.10.1/24 a la dirección 192.168.10.254/24. Se usan para transmisión *unicast*.
- **Direcciones de localhost:** permiten probar la pila de protocolos TCP/IP en la misma terminal, se usan el rango de direcciones IP 127.0.0.0/8 al 127.255.255.255/8. Por lo general se usa la dirección 127.0.0.1.
- **Direcciones link-local:** son asignadas a un *host* cuando no se encuentra una dirección IP válida provista por un servidor DHCP que configura una dirección IP a un terminal de manera automática. El rango de direcciones IP es 169.254.1.0 hasta 169.254.254.255. Estas direcciones no pueden ser enrutadas por los routers. También son conocidas como APIPA (*Automatic Private IP Addressing*) o Auto-IP.
- **Direcciones privadas:** son direcciones IP que deben ser utilizadas en las redes internas de las empresas, estas direcciones no pueden ser enrutadas

por los routers, por lo cual deben ser traducidas a direcciones públicas mediante NAT(*Network Address Translation*). Los rangos disponibles para estas direcciones son:

- 10.0.0.0/**8** al 10.255.255.255/**8**
- 172.16.0.0/**16** al 172.31.255.255/**16**
- 192.168.0.0/**24** al 192.168.255.255/**24**

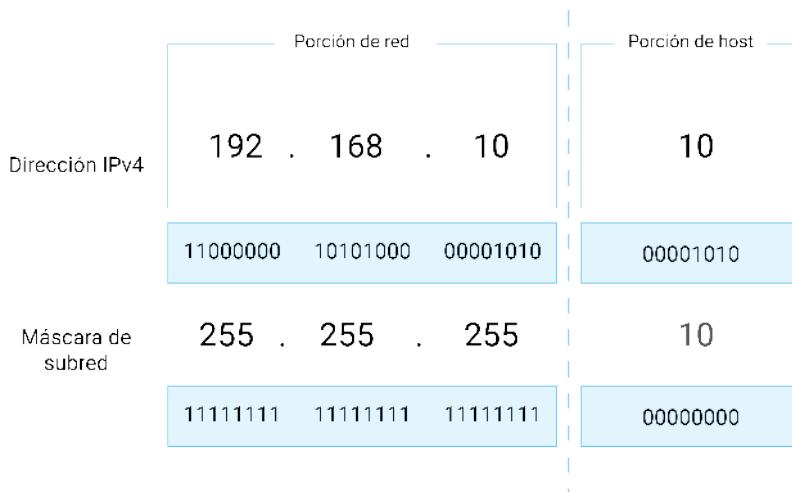
- **Direcciones públicas:** son las direcciones que son asignadas por IANA a dispositivos en las redes públicas o *Internet*, estas direcciones son enrutadas por los *routers* a sus destinos, y son asignadas a dispositivos de acceso público, como es el caso de servidores web. Las direcciones públicas son todas las disponibles, menos los rangos de las privadas y aplicaciones especiales vistas. Ejemplo: 8.8.8.8 (servidor DNS de Google)

2.1.3. Máscara de subred

Si por ejemplo conocemos la dirección IP de host, por ejemplo 192.168.1.2/24, debemos usar la denominada máscara de subred para obtener la dirección de subred. La máscara de subred se obtiene colocando los bits de la porción de red en 1 y los bits de la porción de host en 0, por ejemplo, si tenemos la dirección de *host* 192.168.10.10/24, la máscara de subred sería la que se observa en la Figura 23.

Figura 23

Máscara de subred de una dirección IP de host IPv4.(CISCO, 2019a)

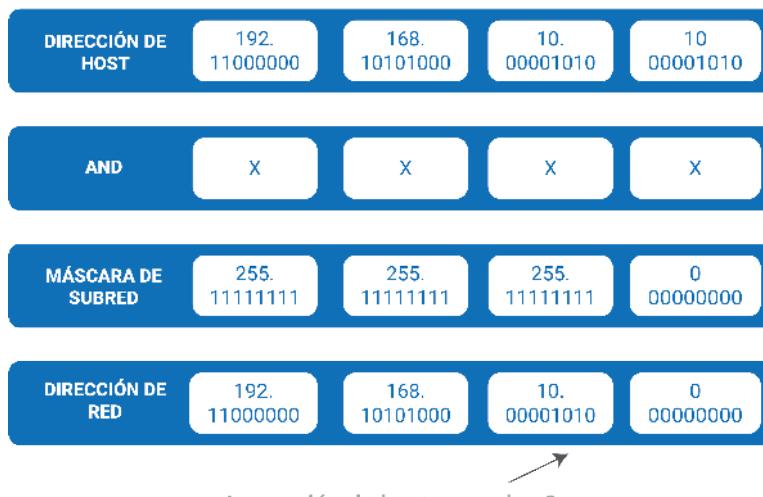


Nota. Adaptado de *Qué es una máscara de subred y cómo descubrirla [Ilustración]*, por Adeva, R., 2025, [adslzone](#), CC BY 4.0.

Para obtener la dirección de red se realiza la operación AND (multiplicación lógica) entre la dirección de host y la máscara de subred (ver Figura 24).

Figura 24

Obtención de la dirección de red mediante la operación AND con la máscara de subred



Nota. Adaptado de *Qué es una máscara de subred y cómo descubrirla [Ilustración]*, por Adeva, R., 2025, [adslzone](#), CC BY 4.0.

Así de esta manera los dispositivos pueden saber la red a la que pertenece un host o terminal, para la toma de decisiones.

2.1.4. Direccionamiento con clases y sin clases

Antiguamente, se asignaban las direcciones de acuerdo a tres clases principales, definidas en la RFC790, las cuales son:

- **Clase A:** para ser usadas en redes muy grandes, el rango de direcciones iba desde 0.0.0.0/8 a 127.0.0.0/8. Es decir, el primer octeto para la red y tres octetos para los hosts. Se puede asignar hasta 2^{24} terminales u hosts por red.
- **Clase B:** para ser usadas en redes medianas, el rango de direcciones iba desde 128.0.0.0/16 a 191.255.0.0/16. Es decir, dos primeros octetos para la red y dos octetos para los hosts. Se puede asignar hasta 2^{16} terminales u hosts por red.

- **Clase C:** para ser usadas en redes pequeñas o domésticas, el rango de direcciones iba desde 192.0.0.0/24 a 223.255.255.0/24. Es decir, los tres primeros octetos para la red y un octeto para los *hosts*. Se puede asignar hasta 254 terminales u *hosts* por red.

La desventaja principal que generaba este direccionamiento con clase es el desperdicio de direcciones, esto generó que las direcciones IPv4 públicas se agoten más rápidamente.

Para solucionar este problema surgió el Ruteo Entre Dominios sin Clase (CIDR-*Classless Inter-domain Routing*) definido en la RFC 4632, este permite asignar cualquier cantidad de *bits* a la porción de red y *hosts*, por ejemplo, podemos asignar 12 *bits* para la porción de red y 20 para los *hosts*, lo que no se podía con el direccionamiento antiguo. En la Tabla 1 podemos ver algunas máscaras de red y prefijos en CIDR.

Tabla 1

Algunos prefijos CIDR y máscaras de subred para direccionamiento sin clases

Prefijo CIDR	Máscara subred	de	Prefijo CIDR	Máscara subred	de	Prefijo CIDR	Máscara subred	de
/30	255.255.255.252		/23	255.255.254.0		/16	255.255.0.0	
/29	255.255.255.248		/22	255.255.252.0		/15	255.254.0.0	
/28	255.255.255.240		/21	255.255.248.0		/14	255.252.0.0	
/27	255.255.255.224		/20	255.255.240.0		/13	255.248.0.0	
/26	255.255.255.192		/19	255.255.224.0		/12	255.240.0.0	
/25	255.255.255.128		/18	255.255.192.0		/11	255.224.0.0	
/24	255.255.255.0		/17	255.255.128.0		/10	255.192.0.0	

Nota. Adaptado de *CIDR: what is classless inter-domain routing?*, por IONOS editorial team, 2019, [IONOS](#).

2.1.5. Asignación de direcciones IP

Para poder asignar las direcciones IP a las interfaces de los dispositivos existen dos formas que son:

- **Asignación estática o manual:** donde los dispositivos son configurados de manera manual con una dirección IP fija. Este direccionamiento es utilizado en empresas pequeñas, y es recomendable para dispositivos que requieren ser accedidos para configuración y mantenimiento como impresoras, centrales telefónicas, cámaras IP, servidores.
- **Asignación dinámica,** mediante esta asignación se arrienda de manera automática una dirección IP al momento de ser conectado el dispositivo, la cual tiene duración determinada. Para realizar esto se requiere de un servidor DHCP (Dynamic Host Configuration Protocol) que es un protocolo de la capa de aplicación que permite configurar las direcciones IP de manera dinámica. Es usado en redes grandes o medianas y de alta movilidad como las redes inalámbricas. La red WiFi en nuestras casas tiene asignación dinámica por medio de DHCP, donde el router inalámbrico es el servidor DHCP.

Le invito a continuar con el aprendizaje sobre Direccionamiento IPv6.

Direccionamiento IPv6

2.2. Direccionamiento IPv6

Ahora, vamos a ver el Protocolo de Internet versión 6 que surgió debido al agotamiento de direcciones IPv4, causado por el crecimiento exponencial de dispositivos en Internet. Esto provoca la escasez de direcciones IPv4 públicas. Una dirección IPv4 tiene una longitud de 32 bits, mientras que la dirección IPv6 tiene 128 bits, aproximadamente unas 340×10^{36} (2^{128}) direcciones IPv6 posibles, que si comparamos con 4.5×10^9 direcciones de IPv4 es mucho mayor.

IPv6 permite evitar las limitaciones de IPv4, además permite la configuración automática de direcciones, no requiere de traducción de direcciones NAT y brinda la suficiente holgura de direcciones para tecnologías como lo es *Internet de las Cosas* (IoT) donde casi todo deberá estar conectado a *Internet* y para ello requiere de una dirección IP.

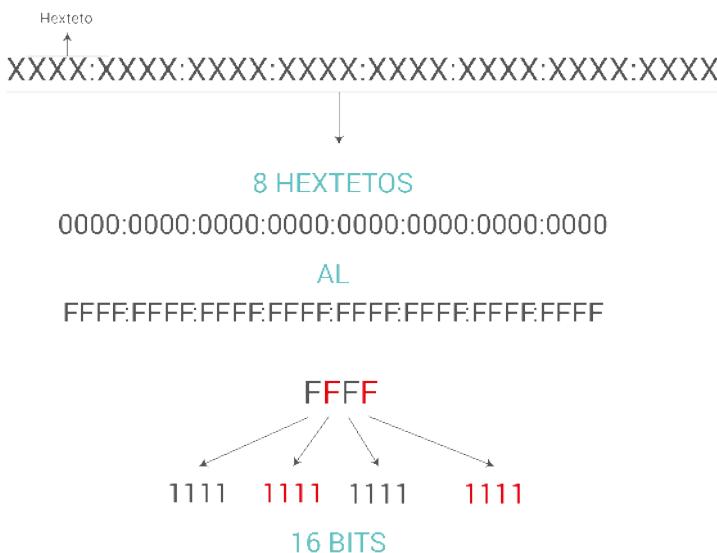
Ahora veamos cómo están estructuradas las direcciones IPv6.

2.2.1. Estructura de dirección IPv6

La dirección IPv6 tiene una longitud de 128 *bits*, donde cada 4 *bits* representa un carácter hexadecimal (0 a F), que se agrupan de cuatro para formar la dirección IPv6, a estos cuatro caracteres hexadecimales se les conoce como hexteto (16 *bits*). En total, la dirección IPv6 está compuesta por ocho hextetos (ver Figura 25).

Figura 25

Estructura de una dirección IPv6



Nota. Rohoden, K., 2024.

Un ejemplo de dirección IPv6 sería: 2001:0DB8:0000:1111:0000:0000:0:0000:0200, como vemos estas direcciones son muy largas, por lo cual se aplican algunas reglas para comprimir la escritura:

Regla 1: Se omiten los ceros iniciales de los hextetos. Por ejemplo, se tiene la dirección IPV6:

2001:**0**DB8:**0000**:1111:**0000**:**0000**:**0000**:**0**200

La dirección simplificada, considerando las secciones sombreadas, sería:

2001:DB8:0:1111:0:0:0:200

Regla 2: Se reemplaza uno o más hextetos en 0 seguidos por el símbolo ::, este símbolo solo puede ser utilizado una vez en la dirección. Por ejemplo:

2001:**0:0**:1111:ABCD:**0:0**:200

Se tienen las dos secciones sombreadas. La notación podría ser:

2001:0:0:1111:ABCD::200

O también:

2001::1111:ABCD:0:0:200

Revisemos otro ejemplo para que quede más claro. Si tenemos la dirección:

FE80:**0000:0000:0000:0000:0000:0000:0001**

Aplicando la primera regla obtendríamos:

FE80:**0:0:0:0:0:0:1**

Y luego de aplicar la segunda regla quedaría:

FE80::1

Las direcciones IPv6 están divididas en dos porciones, la porción de red o prefijo y la porción de interfaz (ver Figura 26). La longitud del prefijo comúnmente utilizada es de 64 bits, por ejemplo, FE80::1/64 indica que 64 bits son para el prefijo y los otros 64 restantes son para la interfaz.

Figura 26

Longitud del prefijo de una dirección IPv6

Prefijo (64 bits)	ID de la Interfaz (64 bits)
----------------------	--------------------------------

Ejemplo: FE80:100::/64

FE80:0100:0000:0000 | 0000:0000:0000:0000

Nota. Adaptado de *Direccionamiento IPv6 - Bases y Fundamentos* [Ilustración], por Salazar, G., 2016, [CiscoCommunity](#), CC BY 4.0.

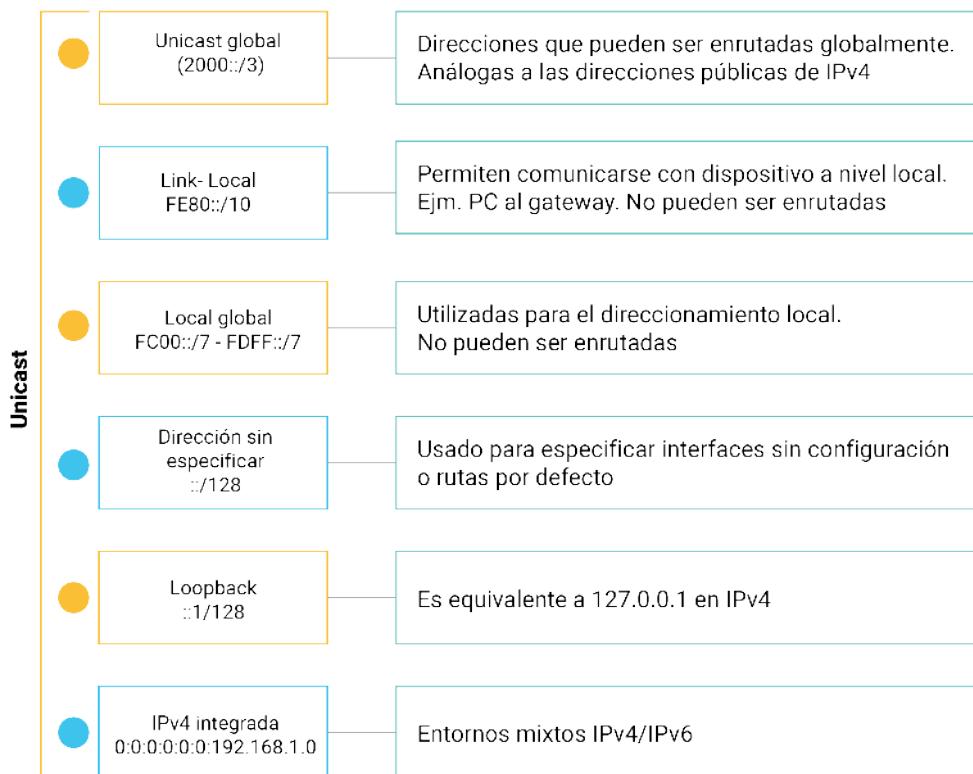
2.2.2. Tipo de direcciones IPv6

Existen tres tipos de direcciones IPv6, las cuales son:

- **Unidifusión:** o *unicast*, permiten la transmisión de un paquete IPv6 entre dos puntos. Estas se subdividen en otras que podemos observar en la Figura 27.

Figura 27

Tipos de direcciones unicast de IPv6 y su aplicación



Nota. Adaptado de *Direccionamiento IPv6 - Bases y Fundamentos* [Ilustración], por Salazar, G., 2016, [CiscoCommunity](#), CC BY 4.0.

- **Multidifusión:** o *multicast*, permite la transmisión de un paquete IPv6 de un punto a varios. Estas direcciones tienen el formato FF00::/8, es decir siempre empiezan en FF y el prefijo de red es de 8 bits.
- **Anycast:** identifica a varias interfaces del dispositivo, y es enviado a un solo dispositivo que sea el más cercano si se habla de enrutamiento. Son usadas solo en los routers, no en hosts.
- **Reservadas para documentación:** son usadas para los manuales y ejemplos. Los rangos son 3FFF:FFFF::/32 y 2001:0DB8::/32.

Analicemos un caso especial como lo son las direcciones globales de unidifusión, estas están estructuradas de acuerdo a la Figura 28. Estas son las direcciones que son enrutadas globalmente en *Internet*.

Figura 28

Formato de dirección global unicast, prefijo de ruteo global, id de subred y de interfaz

Prefijo Routing Global 48 bits	ID de la Subred	ID de la interfaz
-----------------------------------	-----------------	-------------------

Ejemplo: 2001:DB8:ACAD:1::10/64

Siempre debe comenzar con 001 en el primer carácter hexadecimal. Ejm: **0010** (2)

2001:0DB8:ACAD	001	0000:0000:0000:0000
----------------	-----	---------------------

Nota. Adaptado de *Direccionamiento IPv6 - Bases y Fundamentos [Ilustración]*, por Salazar, G., 2016, [CiscoCommunity](#), CC BY 4.0.

Recuerde que en una dirección global el prefijo de routing global siempre empieza con los bits 001 del primer carácter hexadecimal.

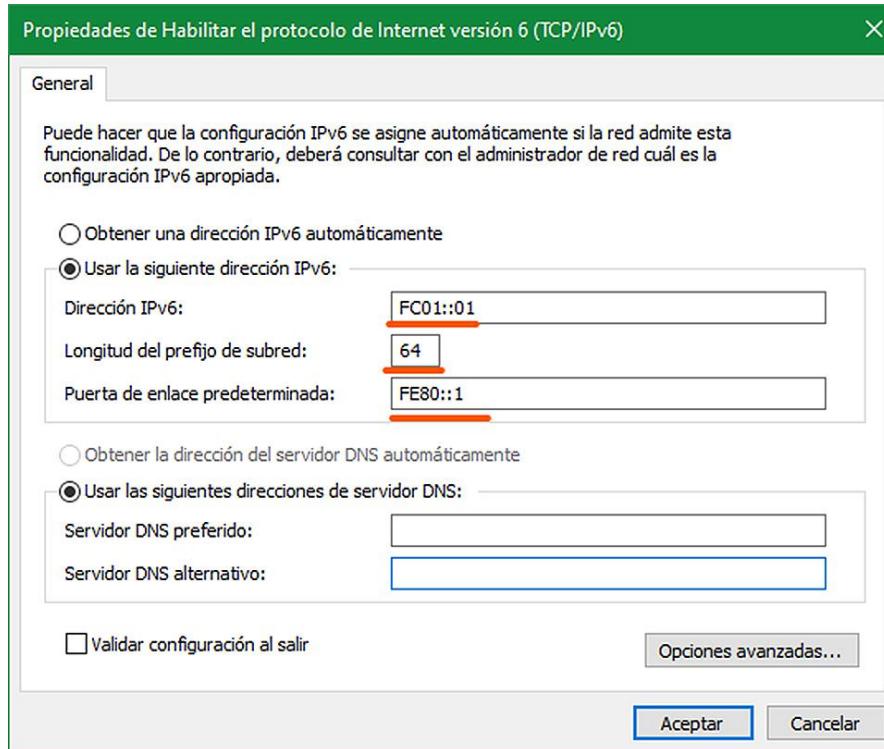
2.2.3. Asignación de direcciones IPv6

Para asignar direcciones IPv6 a una interfaz, existen algunos mecanismos como son:

Asignación estática: se asigna una dirección IPv6 de manera manual a la interfaz de un dispositivo. En la Figura 29 se muestra un ejemplo de configuración estática de una PC, donde se debe configurar la dirección IPv6, el prefijo de red y la puerta de enlace.

Figura 29

Asignación de dirección IPv6 en PC con Windows 10



Nota. Rohoden, K., 2024.

Hay que recalcar que, al momento de conectarse a Internet, la puerta de enlace debe tener una dirección IPv6 global, para poder enrutar tráfico. También se puede configurar una dirección IPv6 global a la interfaz del host.

Asignación dinámica: permite configurar las direcciones IPv6 de manera dinámica y automática. Para lo cual existen tres métodos para hacerlos que son:

- SLAAC o Configuración Automática de Direcciones Independiente de Estado, donde un *router* mediante un anuncio de *router RA* puede configurar la dirección IPv6 de un dispositivo como son la dirección IPv6 de interfaz, prefijo de red y *gateway*.

- DHCPv6 asignación con información de estado, donde un servidor DHCPv6 configura las interfaces de los dispositivos.

Usa direcciones *link-local* de los *routers* y DHCPv6 para los demás parámetros.

- Y un combinado con SLAAC con DHCPv6 sin información de estado, donde un *router* puede configurar la dirección IPv6, pero información adicional como la dirección del servidor DNS se la tiene que obtener de un servidor DHCPv6. Utiliza SLAAC para asignar la dirección *unicast* global y la dirección del *gateway*, y DHCPv6 para otros parámetros.

En SLAAC y SLAAC con DHCPv6 sin estado se genera la **ID de la interfaz**, utilizando el método EUI-64, que utiliza la dirección MAC de la misma, y se forma de la siguiente manera:

En primer lugar, se ubica la OUI de 24 *bits* de la MAC, y se invierte el 7.^º *bit* de la misma, luego se agrega el valor de 16 *bits* en formato hexadecimal FFFE, y por último los restantes 24 *bits* los forman los otros 24 *bits* de la dirección MAC que sobran. Veamos un ejemplo:

Si tenemos la dirección MAC o física en la interfaz: A8-99-B3- 77-B4-56, de la cual el OID es A8-99-B3, de este grupo debemos cambiar el 7.^º *bit* A8 = 1010 1000, invirtiendo este *bit* obtendríamos 1010 1010 = AA. Luego el primer grupo sería AA-99-B3. A este grupo le agregamos FFFE, entonces obtendríamos AA99:B3FF:FE, y bastaría con agregar los *bits* sobrantes de la MAC, con lo que el ID de la interfaz de 64 *bits* sería AA99:B3FF:FE77:B456.

Recuerde que a una dirección IPv6 está formada por el prefijo de red más el ID de la interfaz, también que una interfaz puede tener más de una dirección IPV6 asignada.

En el caso del sistema operativo Windows también se podría generar un ID de interfaz de manera aleatoria (ver Figura 30).

Figura 30

Ejemplo de ID de interfaz aleatoria generada por Windows

Nota. Rohoden, K., 2024.



2.2.4. Migración de IPv4 a IPv6

Para migración y coexistencia de IPV4 a IPv6 existen tres principales métodos, los cuales son:

- **Doble pila o dual stack:** donde las interfaces y dispositivos trabajan de manera simultánea en IPv4 e IPv6, es decir tienen configuradas, tanto direcciones IPv4 como IPv6.
 - **Tunelización:** se encapsula al paquete IPv6 dentro de un paquete IPv4 para poder ser enrutado por redes que trabajan con IPv4.
 - **Traducción o NAT64:** permite traducir direcciones IPv6 a IPv4, permitiendo que dispositivos con direcciones IPv6 se comuniquen con direcciones IPv4.



Actividades de aprendizaje recomendadas

Le invito a desarrollar las actividades que se presentan a continuación:

1. Revise el video [Direccionamiento IPv4 con y sin clases \(CIDR\)](#), tomado de la Universidad Politécnica de Valencia, que tiene por objetivo comprender cómo se asignan las direcciones IPv4.
 2. Revise los videos del canal enRedOS NET de YouTube titulados [Entendiendo IPv6 - direccionamiento y subredes- parte 1](#) donde

encontrará información acerca del direccionamiento IPv6 y [Entendiendo IPv6 - direccionamiento y subredes- parte 2](#) donde encontrará información sobre la estructura de las direcciones IPv6.

3. Con el propósito de reforzar su conocimiento, desarrolle la siguiente autoevaluación. Si su nota es baja, por favor, vuelva a leer y revisar los contenidos.



Autoevaluación 2

Dado los siguientes enunciados, escoja la respuesta correcta:

1. ¿Cuál de las siguientes direcciones IPv4 es una dirección de red?

- a. 192.168.10.4/24.
- b. 192.168.10.0/24.
- c. 192.168.10.0/16.
- d. 192.168.10.3/16.

2. ¿Cuál de las siguientes direcciones IPv4 es una dirección de host?

- a. 192.168.10.4/24.
- b. 192.168.10.0/24.
- c. 192.168.0.0/16.
- d. 10.0.0.0/8.

3. ¿Cuál de las siguientes direcciones IPv4 es una dirección de broadcast?

- a. 192.168.10.4/24.
- b. 192.168.10.255/24.
- c. 192.168.0.0/16.
- d. 10.0.0.0/8.

4. La máscara de subred que corresponde al prefijo /24 es:

- a. 255.0.0.0.
- b. 255.255.0.0.



- c. 255.255.255.0.
d. 255.255.240.0.
5. ¿Cuál de las siguientes direcciones IPv4 es una dirección privada?
- a. 16.168.10.4/24.
b. 192.168.10.255/24.
c. 205.168.0.0/16.
d. 1.1.1.1/8.
6. La longitud de una dirección IPv6 está formada por:
- a. 32 bits.
b. 8 hexátes.
c. 4 hexátes.
d. 4 octetos.
7. ¿Cuál de las siguientes direcciones IPv6 es una dirección *unicast* global?
- a. 2001:DCB::3/64.
b. FE80::3/64.
c. FC80::3/64.
d. ::1/64.
8. ¿Es posible enrutar una dirección IPv6 *link-local* fuera de la red local, por ejemplo, hacia *Internet*?
- a. Verdadero.
b. Falso.
9. La notación simplificada correcta de la siguiente dirección
- 2001:0DB8:0000:0000:ABCD:0000:0000:0001:
- a. 2001:0DB8:0:0:ABCD:0:0:1.
b. 2001:DB8::ABCD:0:0:1.
c. 2001:0DB8::ABCD:0:0:1.



d. 2001:0DB8::ABCD::1.

10. Protocolo usado por IPv4 para asignar direcciones dinámicamente:

- a. TCP.
- b. Ethernet.
- c. DHCP.
- d. SLAAC.

[Ir al solucionario](#)

Para alcanzar el resultado de aprendizaje, usted deberá realizar lectura de la guía, revisar y comprender los ejemplos de división de subredes, así como también revisar las herramientas complementarias como son los videos, que le permitirá diseñar redes en distintos escenarios y adaptar el direccionamiento lógico de la misma.

Contenidos, recursos y actividades de aprendizaje recomendadas



Semana 3

Unidad 3. Subredes

Una vez revisado el direccionamiento IP, en esta semana aprenderemos cómo se realiza el proceso de división en subredes y sus aplicaciones. Los contenidos explicados a continuación se basan en (CISCO, 2019a).

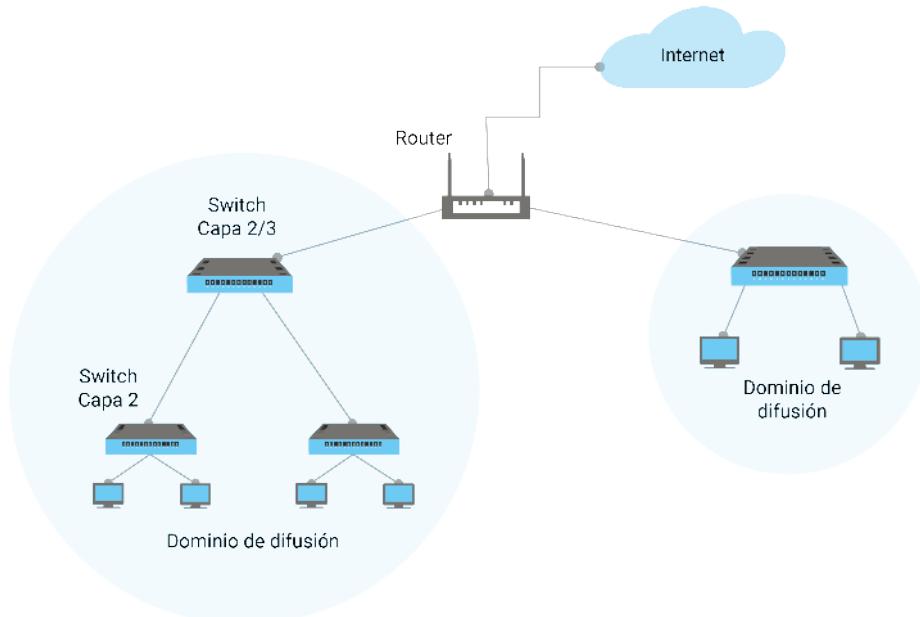
3.1. División en subredes

En las redes de dispositivos, los *hosts* requieren de cierta información para comunicarse con otros, como direcciones MAC e IP de los destinatarios, y al desconocerlas usa el *broadcast* (preguntar a todos) esa información, lo que genera mucho tráfico si son varios dispositivos, y esto a su vez genera

congestión en la red y caídas de los servicios disponibles en la red. Esto se da en los denominados dominios de difusión, que son los segmentos de la red donde se comparte información entre dispositivos (ver Figura 31).

Figura 31

Dominios difusión en una red de dispositivos



Nota. Rohoden, K., 2024.

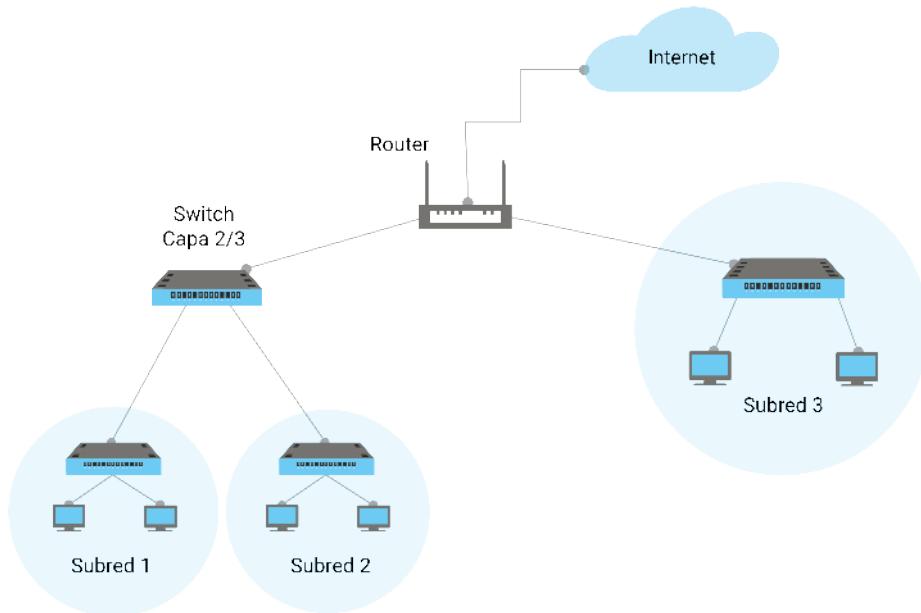
Por ejemplo, para averiguar una dirección MAC los hosts emplean el protocolo ARP (Address Resolution Protocol), por medio del cual se obtiene la dirección MAC de un dispositivo con una dirección IP conocida, mediante un broadcast a todos los hosts en el segmento de red, al incrementar el número de dispositivos estas solicitudes y respuestas generan congestión en el segmento de red.

Como se observa en la Figura 31, los switches pueden expandir los dominios de difusión, y esto lleva a tener mayor número de dispositivos que genera congestión. Una solución es dividir los dominios implementando las denominadas subredes, que son subconjuntos del dominio de difusión (ver Figura 32). De esta manera se reducen los dispositivos que comparten

información entre sí. Para comunicarse entre subredes es necesario realizarlo por medio de un dispositivo con funciones de capa 3 como una switch multicapa o router.

Figura 32

Subdivisión de dominios de difusión mediante subredes



Nota. Rohoden, K., 2024.

Ahora veamos cómo se realiza el proceso de división en subredes.

3.1.1. Subredes con máscara de subred de longitud fija

En este tipo de división todas las subredes tienen la misma máscara de subred, es decir, tienen la misma cantidad de bits para la porción de subred y la de host. El número de subredes requeridas dependerá por ejemplo del número de departamentos de la empresa por ejemplo una subred para gerencia, otra para ventas, otra para recursos humanos, por ubicación (una subred por cada piso) o por tipo de dispositivos (una subred para servidores, impresoras, cámaras IP); así como el número de dispositivos que debe tener cada subred.

Por ejemplo, si tenemos la siguiente dirección de red 192.168.1.0/24, a esta red se tiene que dividir en cinco (5) subredes para los Departamentos de Gerencia, TI, Recursos Humanos, Ventas y Contabilidad. Para lo cual seguiremos el siguiente proceso:

- Se debe tomar prestados **n bits** de la parte de *hosts* para poder obtener el número de subredes requerido, donde:

$$\text{Número de subredes} = 2^n$$

En este caso requerimos que el número de subredes sea cinco (5), por lo que necesitaríamos tomar tres (3) *bits* prestados:

$$\text{Número de subredes} = 2^3 = 8$$

Con esto el nuevo prefijo de subred sería /24+3 =/27 192.168.1.00000000/**27** o 192.168.1.0/27.

- Se calcula el número de *hosts* por subred, nos quedan **m bits** para la porción de *host*, que se calculan de la siguiente manera:

$$\text{Número de hosts} = 2^m - 2$$

Para este caso tenemos que $m=5$ *bits*, por lo que el número de *hosts* es:

$$\text{Número de hosts} = 2^5 - 2 = 30 \text{ hosts}$$

Se resta dos, ya que la primera dirección y última de cada subred son las direcciones de subred y *broadcast* respectivamente, las cuales no se asignan a ningún *host*. En este caso podemos tener hasta 30 terminales por cada subred, si se necesitara más *hosts* se debería subdividir una red con prefijo menor como por ejemplo 192.168.0.0/16.

- Luego obtenemos la máscara de subred que corresponde al prefijo / 27, la cual es:

$$255.255.255.11100000 = 255.255.255.(128+64+32) = 255.255.255.224$$

- d. Tomamos el número obtenido con los *bits* prestados, en este caso 224 y calculamos el número mágico, de la siguiente manera:

$$\text{Número Mágico} = 256 - 224 = 32$$

Este número nos permitirá calcular los rangos de direcciones de las subredes creadas. Por ejemplo, la subred 1 sería 192.168.1.**0**/27, la subred 2 sería 192.168.1.**32**/27, note que sumamos el número mágico en el octeto donde se tomó prestados los *bits*.

- e. Armamos la tabla de direcciones para el esquema de división en subredes planteado, de acuerdo a la Tabla 2.

Tabla 2

Esquema de direccionamiento para división de 5 subredes

Área	Dirección de subred	Rango para hosts	direcciones	Dirección Broadcast	Máscara de subred	Prefijo
Gerencia	192.168.1.0	192.168.1.1 a 192.168.1.30		192.168.1.31	255.255.255.224	/27
TI	192.168.1.32	192.168.1.33 a 192.168.1.62		192.168.1.63	255.255.255.224	/27
Recursos Humanos	192.168.1.64	192.168.1.65 a 192.168.1.94		192.168.1.95	255.255.255.224	/27
Ventas	192.168.1.96	192.168.1.97 a 192.168.1.126		192.168.1.127	255.255.255.224	/27
Contabilidad	192.168.1.128	192.168.1.129 192.168.1.158	a	192.168.1.159	255.255.255.224	/27

Nota. Rohoden, K., 2024.

Tenga en cuenta que sobran tres (3) subredes la cuales son 192.168.1.160, 192.168.1.192, 192.168.1.224, que podrán servir para posibles ampliaciones o para asignar a otras áreas.

3.1.2. Subredes con Máscara de Subred de Longitud Variable VLSM

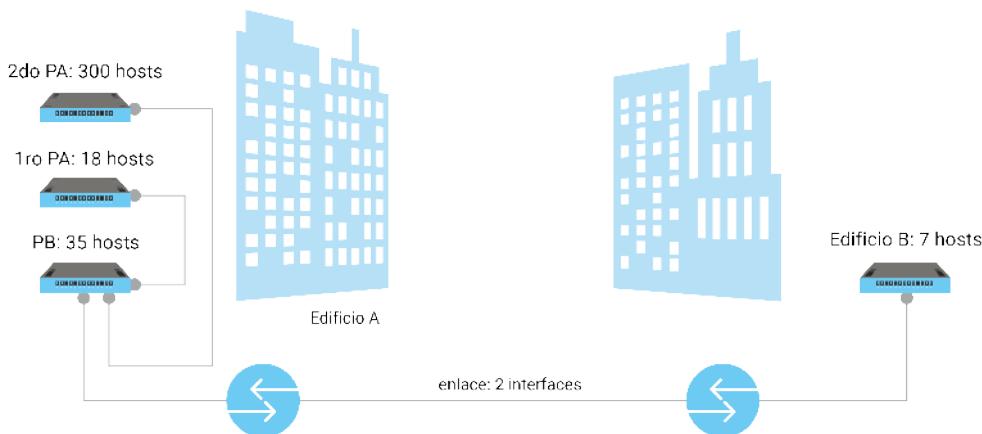
Ahora veamos otro tipo de división conocida como división en Subredes con Máscara de Subred de Longitud Variable o VLSM (*Variable Length Subnet Mask*), en la cual se toma en cuenta el número de dispositivos requeridos por cada subred, por lo que no existe tanto desperdicio de direcciones, pero para lograrlo es necesario que cada subred deba tener distinta máscara de subred.

En este caso calculamos el número de *bits* necesarios para la cantidad de hosts requerida, con la misma fórmula del método anterior. Veamos el ejemplo:

Si se tiene el escenario planteado en la Figura 33, se debe plantear un esquema de direccionamiento con VLSM, para la red 172.16.0.0/16, esto lo realizamos de la siguiente manera:

Figura 33

Requerimientos para ejemplo de VLSM



Nota. Rohoden, K., 2024.

1. En primer lugar, debemos ordenar las subredes de acuerdo al número de hosts de mayor a menor:

- 2do Planta Alta: 300 hosts
- Planta Baja: 35 hosts

- 1ra Planta Alta: 18 hosts
 - Edificio B: 7 hosts
 - Enlace: 2 interfaces
2. Debemos empezar a calcular el prefijo de red de la primera subred, de la siguiente manera:
- Para 300 hosts se requieren de nueve (9) bits, es decir un octeto y un bit adicional, por lo que tenemos la dirección 172.16.00000000.00000000, donde los bits en rojo son los que vamos a usar para la porción de hosts.
- $$\text{Número de hosts} = 2^9 - 2 = 51 \text{ hosts}$$
- Luego que el prefijo para esta subred sería: $32-9 = 23$ (/23), que le corresponde la máscara de subred 255.255.254.0, con esto calculamos el número mágico para saber el siguiente rango a dividir:
- $$\text{Número mágico} = 256 - 254 = 2$$
- Luego el rango iría de **172.16.0.0/23** a **172.16.1.255/23** para la primera subred, ya que la primera dirección de la siguiente subred sería 192.168.2.0 por lo que se resta 1. Siendo 192.168.0.0 la dirección de subred y 192.168.1.255 la dirección de broadcast.
3. Para 35 hosts se requieren de seis (6) bits:
- $$\text{Número de hosts} = 2^6 - 2 = 62 \text{ hosts}$$
- Por lo que el prefijo de subred sería /26 y la máscara 255.255.255.192, y el rango de subred o número mágico es 64. Entonces el rango iría desde 172.16.2.0 a 172.16.2.63, observe como se suma el número en último octeto.
4. Para 18 hosts se requieren de cinco (5) bits:
- $$\text{Número de hosts} = 2^5 - 2 = 30 \text{ hosts}$$



Luego el prefijo para esta subred sería: $32-5 = 27$ (**/27**), que le corresponde la máscara de subred 255.255.255.224, con esto calculamos el número mágico para saber el siguiente rango a dividir:

$$\text{Número mágico} = 256 - 224 = 32$$

Por lo que el rango iría de **172.16.2.64** a **172.16.2.95** para la tercera subred.

5. Para siete (7) hosts se requieren de cuatro (4) bits:

$$\text{Número de hosts} = 2^4 - 2 = 14 \text{ hosts}$$

Luego el prefijo para esta subred sería: $32-4 = 28$ (**/28**), que le corresponde la máscara de subred 255.255.255.240, con esto calculamos el número mágico para saber el siguiente rango a dividir:

$$\text{Número mágico} = 256 - 240 = 16$$

Por lo que el rango iría de **172.16.2.96** a **172.16.2.111** para la cuarta subred.

6. Para dos (2) interfaces de los routers se requieren de dos (2) bits:

$$\text{Número de hosts} = 2^2 - 2 = 2 \text{ hosts}$$

Luego el prefijo para esta subred sería: $32-2 = 30$ (**/30**), que le corresponde la máscara de subred 255.255.255.252, con esto calculamos el número mágico para saber el siguiente rango a dividir:

$$\text{Número mágico} = 256 - 252 = 4$$

Por lo que el rango iría de **172.16.2.112/30** a **172.16.2.115/30** para la quinta subred. Con esto el esquema de división de subredes con VLSM a usar, se resume en la Tabla 3.

Tabla 3*Ejemplo de división en subredes con VLSM*

Área	Dirección de subred	Rango direcciones para hosts	Dirección Broadcast	Máscara Subred	de	Prefijo
2da Planta Alta (300 hosts)	172.16.0.0	172.16.0.1 a 172.16.1.254	172.16.1.255	255.255.254.0	/23	
Planta Baja (35 hosts)	172.16.2.0	172.16.2.1 a 172.16.2.62	172.16.2.63	255.255.255.192	/26	
1ra Planta Alta (18 hosts)	172.16.2.64	172.16.2.65 a 172.16.2.94	172.16.2.95	255.255.255.224	/27	
Edificio B (7 hosts)	172.16.2.96	172.16.2.97 a 172.16.2.110	172.16.2.111	255.255.255.240	/28	
Enlace (2 hosts)	172.16.2.112	172.16.2.113 y 172.16.2.114	172.16.2.115	255.255.255.252	/30	

Nota. Rohoden, K., 2024.



Actividades de aprendizaje recomendadas

Desarrolle las siguientes actividades:

1. Visualice el video del canal de Gabriel Marcano de YouTube, titulado [Direccionamiento IPv4 y subredes](#), en el cual, podrá conocer sobre el proceso y ejemplos de división en subredes usando direcciones IPv4.

2. Realice el direccionamiento de la red 172.16.0.0/16, para un total de 12 subredes, y llene la tabla que se presenta a continuación con las cinco primeras subredes.

Completar

Área	Dirección de subred	Rango direcciones para hosts	Dirección broadcast	Máscara de Subred	Prefijo
Subred 1					
Subred 2					
Subred 3					
Subred 4					
Subred 5					

Nota: copie la tabla en un Word o cuaderno para llenar.

3. Visualizar el video del canal de Gabriel Marcano de YouTube, titulado [VLSM explicado en un ejemplo](#), donde podrá revisar la resolución de un ejemplo usando VLSM para la división de subredes.
4. Realice la división en subredes de la red 10.0.0.0/8 con VLSM, para un total de 5 subredes, que son:

1. Ventas: 600 hosts.
2. Recursos humanos: 300 hosts.
3. TI: 150 hosts.
4. Contabilidad: 80 hosts.
5. Enlace 1: 2 interfaces.
6. Enlace 2: 2 interfaces.



Completar

Área	Dirección de subred	Rango direcciones para hosts	Dirección broadcast	Máscara de Subred	Prefijo
Subred 1					
Subred 2					
Subred 3					
Subred 4					
Subred 5					

Nota: copie la tabla en un Word o cuaderno para llenar.

5. Le invito a reforzar sus conocimientos, participando en la siguiente autoevaluación.



Autoevaluación 3

Dado los siguientes ítems, seleccionar la respuesta correcta:

1. En la división de subredes con máscara de subred fija se tiene menos desperdicio de direcciones:
 - a. Verdadero.
 - b. Falso.

2. En VLSM todas las subredes tienen el mismo número de hosts:
 - a. Verdadero.
 - b. Falso.

3. Si una subred debe tener 60 hosts. ¿Cuántos bits debemos usar para la porción de hosts?

- a. 4 bits.
- b. 5 bits.
- c. 6 bits.
- d. 8 bits.

4. Si se requiere dividir en 10 subredes, la red 192.168.1.0/24. ¿Cuántos bits debemos pedir prestados a la porción de host?

- a. 4 bits.
- b. 5 bits.
- c. 6 bits.
- d. 8 bits.

5. Si se tiene la subred 10.1.1.0/28. ¿Cuál es la máscara de subred?

- a. 255.255.255.240.
- b. 255.255.240.0.
- c. 255.255.255.252.
- d. 255.255.255.248.

6. La red 10.0.0.0/16 ha sido dividida con una máscara de subred 255.255.255.224 para todas las subredes. ¿Cuántos hosts posibles hay en cada subred?

- a. 30 hosts.
- b. 62 hosts.
- c. 14 hosts.
- d. 126 hosts.

7. Si se ha dividido la red 172.16.0.0 usando una máscara de 255.255.240.0. ¿Cuál es la dirección de la 3.^a subred?

- a. 172.16.8.0.
- b. 172.16.16.0.



- c. 172.16.32.0.
d. 172.16.24.0.
8. Si se usa VLSM para dividir la red 192.168.1.0/24. ¿Cuál es la máscara de subred si se requieren conectar 4 hosts?
- a. 255.255.255.248.
b. 255.255.248.0.
c. 255.255.255.252.
d. 255.255.252.0.
9. Si una red tiene prefijo /26, ¿cuál es el valor del “número mágico” o rango de subred?
- a. 64.
b. 48.
c. 32.
d. 16.
10. Si se ha dividido la red 172.16.0.0/16 usando una máscara de 255.255.240.0. ¿Cuál es la dirección de broadcast de la 4.^a subred?
- a. 172.16.48.255.
b. 172.16.31.255.
c. 172.16.32.255.
d. 172.16.47.255.

[Ir al solucionario](#)

Resultado de aprendizaje 3:

Comparar el funcionamiento de los protocolos de enrutamiento interior con los protocolos de enrutamiento exterior.

Para alcanzar el resultado de aprendizaje usted identificará los conceptos básicos de los protocolos de enrutamiento, su funcionamiento y los diferentes tipos de protocolo usados en las redes de telecomunicaciones para enrutar la información desde su origen a su destino.

Contenidos, recursos y actividades de aprendizaje recomendadas

Recuerde revisar de manera paralela los contenidos con las actividades de aprendizaje recomendadas y actividades de aprendizaje evaluadas.



Semana 4

Unidad 4. Generalidades de protocolos de enrutamiento

En esta semana revisaremos la función de enrutamiento de la capa de red, que permite transmitir la información a través de *Internet*, veremos los distintos algoritmos y protocolos que se usan para que los *routers* intercambien información y puedan determinar la mejor ruta por la que viajará la información en las redes locales y globales. Los contenidos explicados están basados en (CISCO, 2019b; Kurose & Ross, 2017; Sánchez et al., 2020).

4.1. Reenvío y enrutamiento

La función de reenvío y enrutamiento es muy sencilla, ya que el dispositivo despacha los paquetes recibidos y los commuta a un destino. En la tarea de enviar los paquetes debemos distinguir dos procesos:

- **Reenvío o *forwarding*** se da cuando un paquete llega a la interfaz de un *router*. Este paquete es commutado a una interfaz de salida, ya que el

paquete está dirigido a una red remota conectada a una de las interfaces del *router*.

- **Enrutamiento o routing** este proceso consiste en determinar la ruta de salida de un paquete que es recibido, para realizar esto se emplean los algoritmos de enrutamiento, que mediante el análisis de algunas métricas determinan la mejor ruta a seguir para llegar al destino, al cual el paquete va a ser.

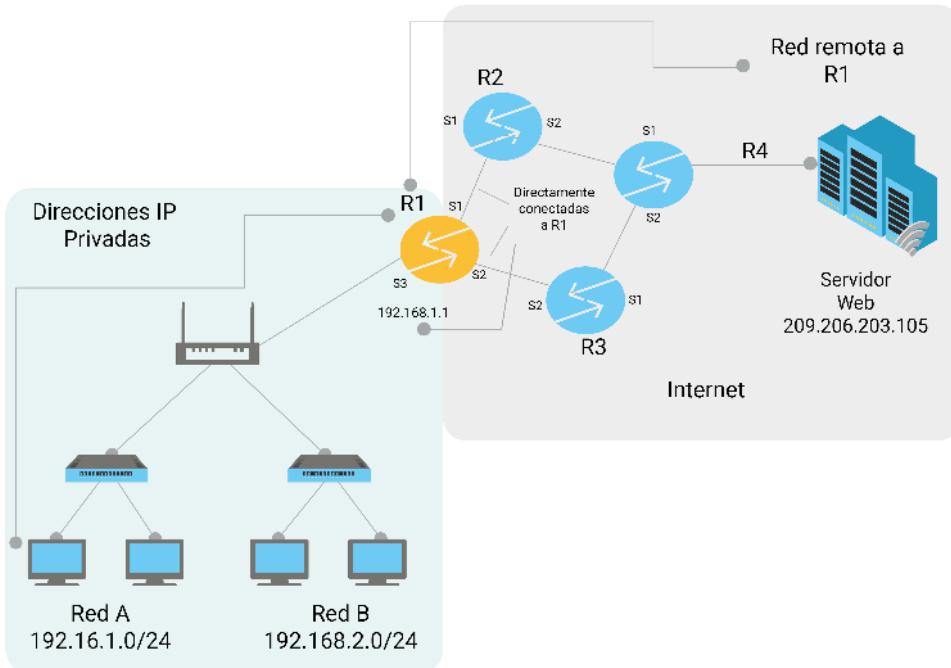
Cuando el *router* recibe un paquete que está dirigido hacia una red remota, este consulta la denominada tabla de ruteo o reenvío, donde se enlaza una red remota con una interfaz de salida del *router* que se conocen como rutas y donde existen algunos tipos de rutas, como son:

- **Rutas conectadas directamente** son las que están conectadas a las interfaces del *router*, que está realizando los procesos de reenvío y enrutamiento.
- **Rutas remotas** son las rutas donde el *router* debe enviar los paquetes por medio de otros *routers* para llegar al destino. Estas rutas pueden ser configuradas manualmente o aprendidas de manera dinámica mediante un protocolo de enrutamiento.
- **Ruta predeterminada**, esta ruta es utilizada para rutas que el *router* desconoce y no tiene registrada en la tabla de ruteo. Esta se representa con la dirección IP **0.0.0.0/0** para IPv4 y **::/0** para IPv6. Esta ruta, por lo general, es configurada de manera manual con una ruta estática o mediante propagación de la misma.

Los distintos tipos de rutas y redes se pueden observar en la Figura 34, con respecto al *router* R1.

Figura 34

Tipos de rutas y redes con respecto al router R1



Nota. Rohoden, K., 2024.

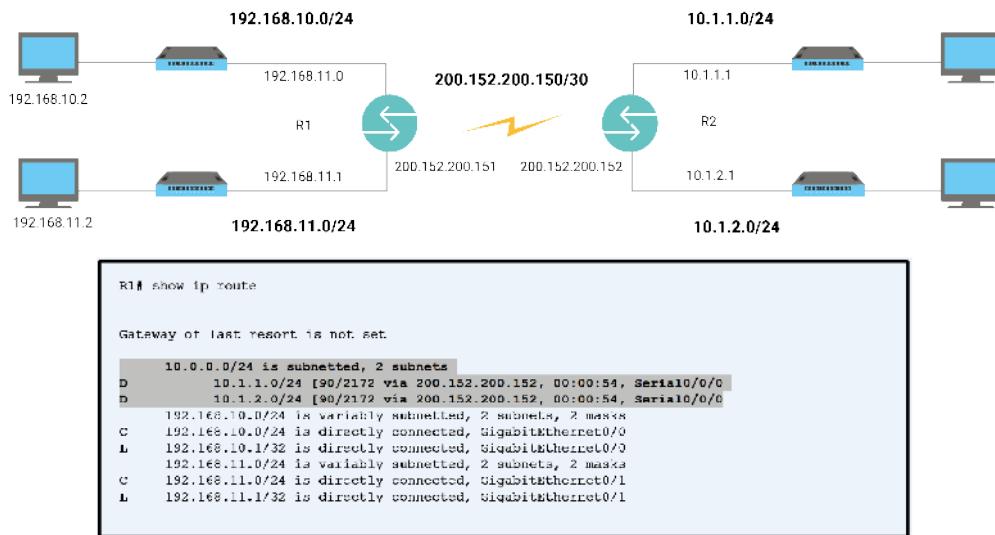
En la Figura 34, se observa los diferentes tipos de redes que almacena un router en su tabla de ruteo, tenemos las redes directamente conectadas que son todas las redes que están conectadas a sus interfaces, y las redes remotas que son aquellas que para alcanzarlas debe hacerlo a través de otros routers. En este caso un host quiere comunicarse con el servidor web con dirección 209.206.203.105, que es una red que el host desconoce, por lo cual envía los paquetes hacia la interfaz S3 de su gateway que en este caso es R1.

Luego R1 toma la decisión mediante su tabla de ruteo y los envía por la interfaz S1 hacia la interfaz S1 del router R2, R2 realiza el mismo procedimiento y envía por medio de la interfaz S2 a la interfaz S1 de R4. Luego R4 al revisar su tabla verifica que es una red que está conectada directamente a una de sus interfaces y envía la información hacia el servidor WEB.

En la tabla de ruteo se especifica la dirección de red, la interfaz de salida y el tipo de ruta. En la Figura 35, se observa los distintos detalles que se almacenan en esta, las direcciones de destino son obtenidas mediante los encabezados de los datagramas IP. Cada dispositivo de capa de red como routers y hosts tienen dos tablas una para IPv4 y otra para IPv6.

Figura 35

Tabla de ruteo de un router marca CISCO



Nota. Rohoden, K., 2024.

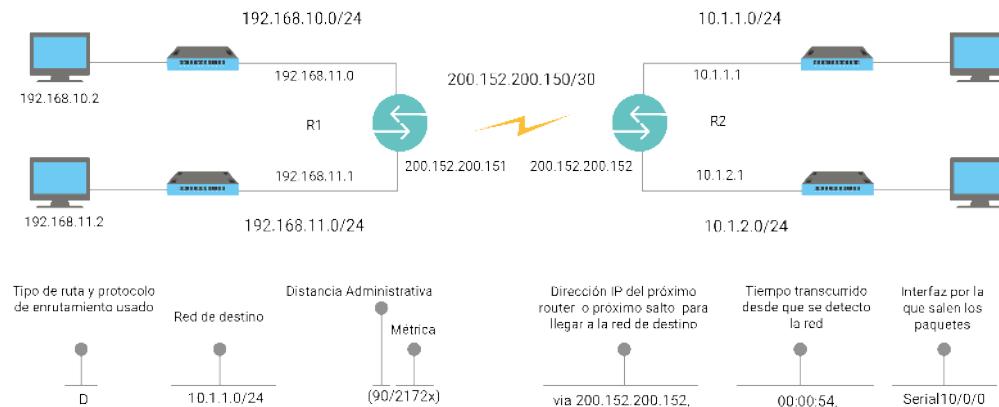
En el escenario de la Figura 35, se han resaltado las redes remotas aprendidas mediante un algoritmo de enrutamiento, etiquetadas con la letra D que corresponde al algoritmo de enrutamiento EIGRP que es propietario de CISCO. Aquí podemos distinguir dos tipos de rutas remotas:

- **Ruta de primer nivel** que es la ruta que tiene mayor máscara de subred, o la dirección de red sin dividir, en este caso 10.0.0.0/24.
- **Rutas de segundo nivel** que son las subredes de la ruta principal que están configuradas en las interfaces, en este caso 10.1.1.0/24 y 10.1.2.0/24.

Aquí se indica que para llegar a estas redes remotas se debe enviar hacia la dirección IP 200.152.200.152 que es la que tiene asignada la interfaz serial del router R2, y también indica que la interfaz de salida es Serial0/0/0 que pertenece a R1. Las filas etiquetadas con la letra C indica las redes directamente conectadas, y la letra L indica la dirección IP configurada en la interfaz respectiva.

Para interpretar todas estas rutas podemos usar la información provista en la Figura 36.

Figura 36
Interpretación de líneas de tablas de ruteo



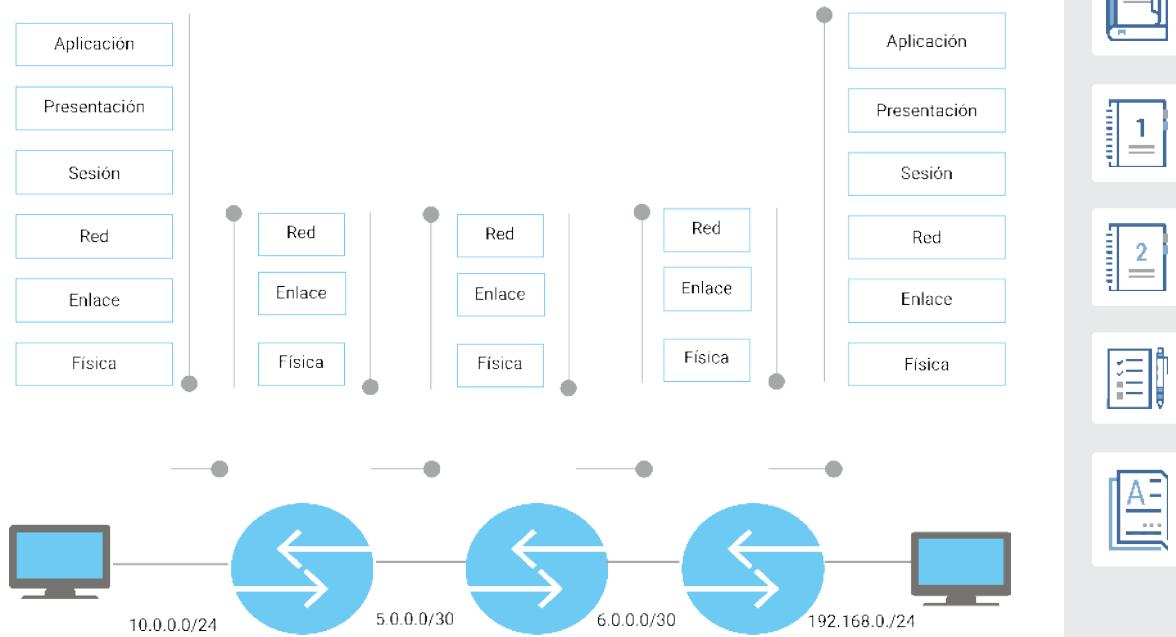
Nota. Adaptado de *Direccionamiento IPv6 - Bases y Fundamentos* [Ilustración], por Salazar, G., 2016, [CiscoCommunity](#), CC BY 4.0.

4.2. Funcionamiento de un router

Como habíamos dicho los routers o enrutadores son dispositivos de capa 3, es decir que trabajan desde la capa 1 hasta la capa 4, pueden procesar las PDU de esas capas, al recibir un nuevo paquete se realiza el desencapsulamiento de tramas y paquetes para poder agregar nuevos encabezados y poder reenviarlos o enrutarlos (ver Figura 37), ya que al pasar por cada router se agregan nuevas direcciones físicas y lógicas de origen y nuevas direcciones físicas de destino. Recuerde que la dirección lógica de destino final no se cambia.

Figura 37

Encapsulamiento y desencapsulamiento en routers

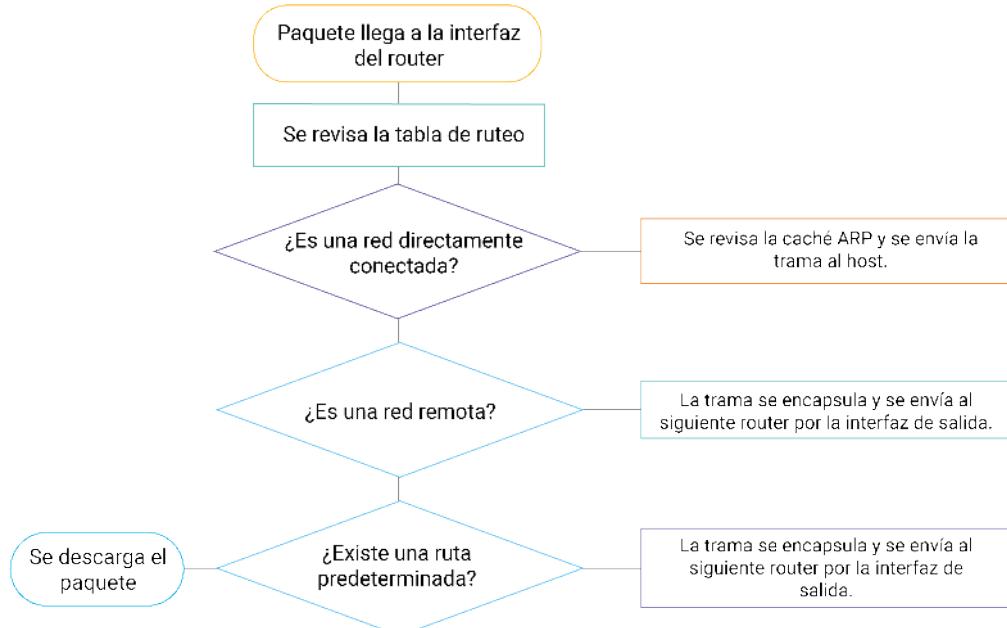


Nota. Adaptado de *Direccionamiento IPv6 - Bases y Fundamentos* [Ilustración], por Salazar, G., 2016, [CiscoCommunity](#), CC BY 4.0.

Ahora veamos cómo se realiza el proceso de enrutamiento, y cómo se realiza la toma de decisiones para reenviar y enrutar los paquetes recibidos (ver Figura 38). Note que el proceso es verificar si la red de destino es una red conectada directamente o una red remota y por último recurso si existe configurada una ruta predeterminada, de lo contrario el paquete será descartado.

Figura 38

Proceso de enrutamiento de paquetes en los routers



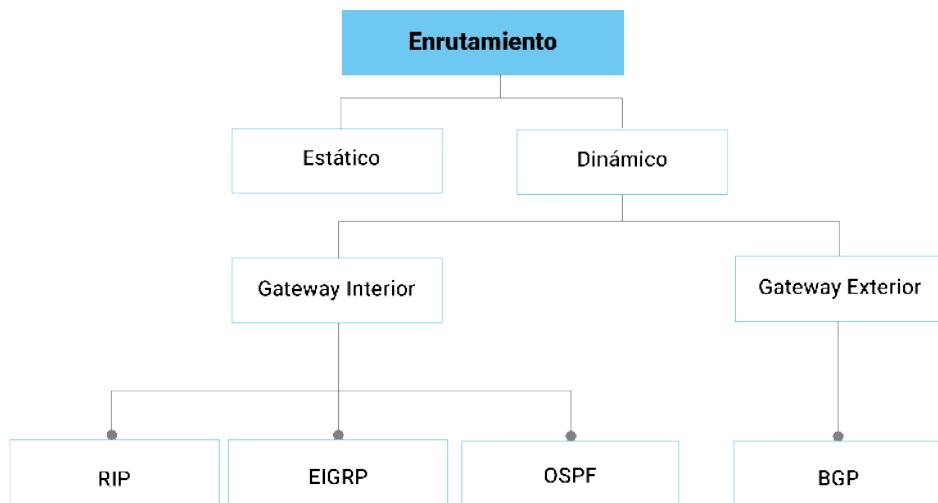
Nota. Adaptado de *Direccionamiento IPv6 - Bases y Fundamentos* [Ilustración], por Salazar, G., 2016, [CiscoCommunity](#), CC BY 4.0.

Pero ¿cómo se elige la mejor ruta?, aquí se toma en cuenta algunos factores como son las métricas de las rutas. Las métricas son valores numéricos que representan la “distancia” a seguir por una ruta, esta puede depender del ancho de banda, número de saltos, velocidad del canal, entre otros, luego la mejor ruta es aquella que tiene la métrica más baja.

Para escoger la mejor ruta se debe implementar algunos tipos de enrutamiento que se detallan en la Figura 39.

Figura 39

Tipos de enrutamiento en las redes de dispositivos



Nota. Rohoden, K., 2024.

En esta clasificación distinguimos el enrutamiento estático y el dinámico, en el dinámico se tiene una subclasiación de protocolos de enrutamiento de gateway interior y los de gateway exterior.

Los de gateway interior son aquellos que permiten comunicarse a routers que pertenecen a un mismo Sistema Autónomo AS, que son administrados bajo las mismas reglas, y los de gateway exterior que comunican entre AS.

A continuación, iremos desglosando cada uno de los tipos de enrutamiento, sus algoritmos y protocolos, los cuales son los siguientes:

- RIP (*Routing Information Protocol*).
- OSPF (*Open Shortest Path First*).
- EIGRP (*Enhanced Interior Gateway Routing Protocol*).
- BGP (*Border Gateway Protocol*).

4.3. Enrutamiento estático

El enrutamiento estático permite configurar en los *routers*, rutas estáticas de manera manual, para lo cual el administrador de red deberá conocer toda la topología de la red para realizarlo.

Estas rutas no se propagan por la red, lo cual brinda mayor seguridad, no consumen ancho de banda ni recursos como cálculos del CPU. Tienen algunas desventajas, ya que no se adapta a cambios en la red, y la configuración se complica a medida que crecen de tamaño las redes.

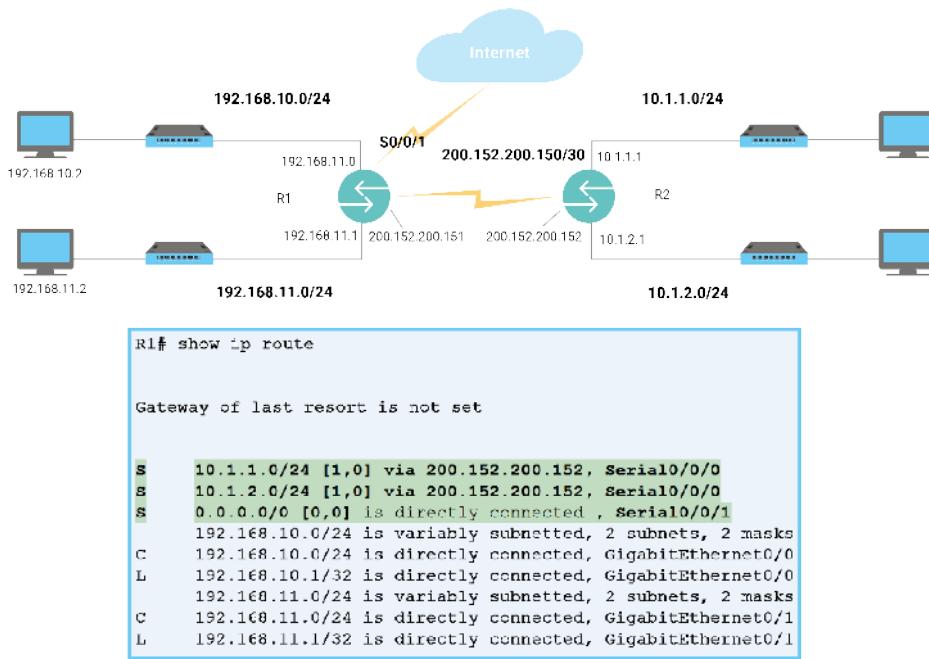
Las rutas estáticas son utilizadas para:

- Enrutar tráfico a una red especificada por el administrador.
- Ingresar rutas predeterminadas para tráfico dirigido a redes remotas desconocidas.
- Reducir el número de redes propagadas y anunciadas por los algoritmos dinámicos.
- Establecer rutas de respaldo para las rutas principales de la red.

Un ejemplo de tabla de ruteo con rutas estáticas es la que se muestra en la Figura 40.

Figura 40

Ejemplo de tabla de ruteo con rutas estáticas



Nota. Adaptado de *Direccionamiento IPv6 - Bases y Fundamentos* [Ilustración], por Salazar, G., 2016, [CiscoCommunity](#), CC BY 4.0.

Las rutas resaltadas en la Figura 40 y etiquetadas con la letra S se refieren a rutas estáticas, aquí vemos que se han configurado tres rutas estáticas en el router R1, dos de ellas son para dirigir el tráfico hacia las redes remotas 10.1.1.0/24 y 10.1.2.0/24, por medio del gateway R2 y por la interfaz serial S0/0/0, y la tercera que es la ruta predeterminada que especifica todo el tráfico dirigido a redes desconocidas se enrute a través de la interfaz serial S0/0/1. Las rutas estáticas tienen una distancia administrativa de 1 y métrica 0 que se representa como [1,0] cuando se trata de redes remotas, y cuando se trata de redes directamente conectadas la distancia administrativa es de 0 [0,0].



Actividades de aprendizaje recomendadas

Continuemos con el aprendizaje mediante su participación en las actividades que se describen a continuación:

1. Le invito a revisar el video [Introducción a la capa de red](#), tomado desde el sitio de URJC_RedesComputadores, donde podrá conocer sobre las funciones de reenvío y enrutamiento del *router*, que es el dispositivo que trabaja en la capa de red.
2. Realice los siguientes pasos orientados a obtener las tablas de ruteo que están almacenadas en su PC. Para lo cual debe seguir los siguientes pasos:

- Estando en el escritorio de Windows, presionar las teclas.



- Escribimos en el cuadro de diálogo el comando: cmd y presionamos la tecla enter.



- Se abrirá la consola de Windows, donde ingresaremos el comando: netstat -r y presionamos la tecla enter.



- Aquí se desplegará información de las interfaces de que dispone, y se mostrarán las tablas de ruteo para IPv4 e IPv6 (ver Figura 41).

Figura 41

Tabla de enrutamiento de un host de Windows, obtenida mediante el comando netstat -r

La figura muestra una captura de pantalla de la tabla de enrutamiento IPv4 en Windows. La tabla tiene las siguientes columnas: Rutas activas, Dirección de red, Máscara de red, Puerta de enlace, Tolerancia, Métrica. Los datos son:

Rutas activas	Dirección de red	Máscara de red	Puerta de enlace	Tolerancia	Métrica
	0.0.0.0	0.0.0.0	192.168.1.1	192.168.1.1/	15
	127.0.0.0	255.0.0.0	En vínculo	127.0.0.1	331
	127.0.0.1	255.255.255.255	En vínculo	127.0.0.1	331

Explicación de los campos:

- Red de destino de los paquetes: Dirección de red.
- Máscara de red de la red de destino: Máscara de red.
- Dirección IP de la interfaz por la que salen los paquetes hacia la red de destino: Puerta de enlace.
- Valor usado para determinar la mejor ruta: Tolerancia.
- Dirección IP del gateway a la que se deben enviar los paquetes de la red de destino: Dirección de red.

Nota. Rohoden, K., 2024.

- Con la información desplegada de su computador, identifique la ruta predeterminada (0.0.0.0), a qué dirección IP son enviados los paquetes. Esta dirección pertenece al ¿Qué máscara de subred tiene la ruta por defecto? _____.
- Esto nos indica que toda red que no conozca su computadora la enviará por su ruta por defecto que en este caso es el *gateway*, por medio de su interfaz de red.

Nota: por favor, complete la actividad en un cuaderno o documento Word.

- Observe el video titulado "[Enrutamiento estático, funcionamiento detallado](#)".
- Realice la autoevaluación para comprobar sus conocimientos. Si su nota es baja, por favor, vuelva a leer y revisar los contenidos.



[Autoevaluación 4](#)

Dado los siguientes ítems, seleccionar la respuesta correcta:

- Un *router* para poder reenviar o enrutar un paquete debe revisar:
 - Tabla de ruteo.



b. Tabla MAC.

c. Caché ARP.

d. Máscara de subred.

2. El reenvío hace referencia a transferir paquetes desde las interfaces de entrada a las de salida:

a. Verdadero.

b. Falso.

3. El enrutamiento se realiza en un tiempo de nanosegundos:

a. Verdadero.

b. Falso.

4. El enrutamiento es:

a. Desechar los paquetes que no pertenecen a las redes del *router*.

b. Analizar métricas que permitan determinar la ruta de salida.

c. Colocar una ruta en la trama.

5. El reenvío se implementa en el plano de:

a. Control.

b. De datos.

6. Una ruta remota es aquella que:

a. Está conectada directamente a una interfaz del *router*.

b. Es accesible a través de otros *routers*.

c. No requiere de otros *routers* para llegar a ella.

d. No se requiere de un *gateway* para llegar a ella.

7. Ruta que es representada en la tabla de ruteo con 0.0.0.0/0 en IPv4:

a. Ruta predeterminada.

b. Ruta directamente conectada.

c. Ruta en red remota.

- d. Conexión *localhost*.
8. Si la red de destino no se encuentra en la tabla de ruteo por donde se envían los paquetes:
- Ruta predeterminada.
 - Ruta en red remota.
 - Se descarta el paquete.
9. ¿Qué le sucede a un paquete cuya red de destino no se encuentra en la tabla de ruteo y en el *router* no está configurada una ruta predeterminada?
- Se devuelve al emisor.
 - Se envía por todas las interfaces.
 - Se descarta el paquete.
 - Se da una red remota de manera aleatoria.
10. Si llega un paquete al *router* que tiene la tabla de ruteo de la imagen, con la dirección de destino 180.172.12.0/24. ¿Por cuál interfaz saldrá el paquete?



```
R1# show ip route | begin Gateway
Gateway of last resort is 209.165.200.234 to network 0.0.0.0

S* 0.0.0.0/0 [1/0] via 209.165.200.234, Serial0/0/1
    is directly connected, Serial0/0/1
    172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
C   172.16.1.0/24 is directly connected, GigabitEthernet0/0
L   172.16.1.1/32 is directly connected, GigabitEthernet0/0
R   172.16.2.0/24 [120/1] via 209.165.200.226, 00:00:12, Serial0/0/0
R   172.16.3.0/24 [120/2] via 209.165.200.226, 00:00:12, Serial0/0/0
R   172.16.4.0/28 [120/2] via 209.165.200.226, 00:00:12, Serial0/0/0
R   192.168.0.0/16 [120/2] via 209.165.200.226, 00:00:03, Serial0/0/0
    209.165.200.0/24 is variably subnetted, 5 subnets, 2 masks
C   209.165.200.224/30 is directly connected, Serial0/0/0
L   209.165.200.225/32 is directly connected, Serial0/0/0
R   209.165.200.228/30 [120/1] via 209.165.200.226, 00:00:12, Serial0/0/0
C   209.165.200.232/30 is directly connected, Serial0/0/1
L   209.165.200.233/32 is directly connected, Serial0/0/1
R1#
```

- a. Serial 0/0/1.
- b. Serial 0/0/0.
- c. GigabitEthernet0/0.
- d. GigabitEthernet0/1.

[Ir al solucionario](#)

Resultado de aprendizaje 4:

Describir las estrategias para garantizar la disponibilidad de acceso a la red en redes comutadas y enrutadas.

Para alcanzar el resultado de aprendizaje se revisará el funcionamiento de los distintos algoritmos usados por los protocolos de enrutamiento para determinar el mejor camino, esto le permitirá conocer más a fondo como un router decide que ruta escoger.

Contenidos, recursos y actividades de aprendizaje recomendadas

Recuerde revisar de manera paralela los contenidos con las actividades de aprendizaje recomendadas y actividades de aprendizaje evaluadas.



Semana 5

Unidad 5. Algoritmos de enrutamiento

En esta semana revisaremos más a fondo el plano de control, que permite definir la manera en que se selecciona la mejor ruta de extremo a extremo, para que los paquetes lleguen desde el *host emisor* hasta su destino, pero este proceso sea de manera dinámica, mediante el uso de protocolos de enrutamiento dinámicos. Los contenidos explicados están basados en (Kurose & Ross, 2017; Sánchez et al., 2020).

5.1. Introducción

Un *router*, una vez que recibe un paquete, tiene que buscar en su tabla de enrutamiento para saber por cuál ruta debe reenviarlo. Para ello podemos usar el enrutamiento estático, pero a medida que las redes crecen o cambian se vuelve muy complicado y tedioso llevar a cabo estos cambios, por lo que es

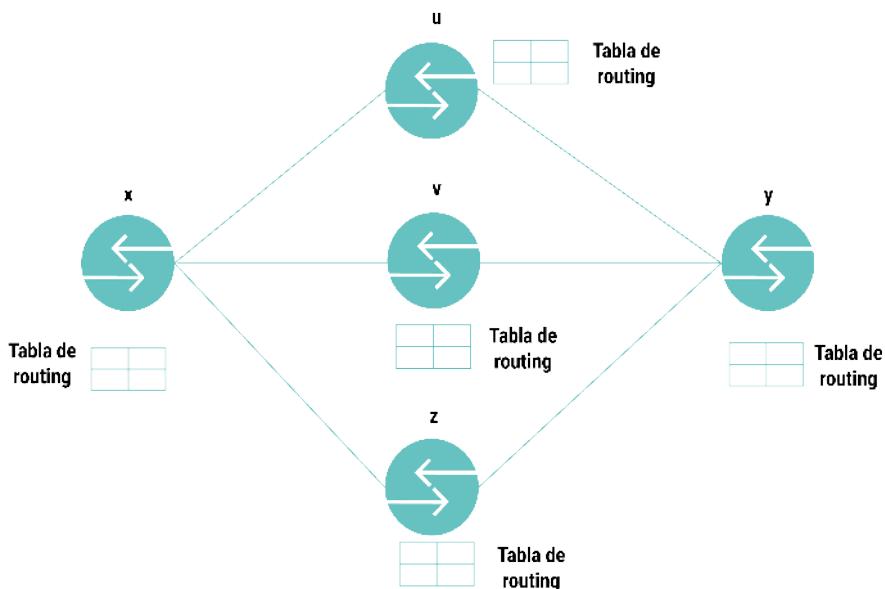
más conveniente realizarlo de manera dinámica para que se adapte a los cambios de la red y que los *routers* se intercomuniquen entre ellos para intercambiar información de rutas.

Para construir las tablas de reenvío o enrutamiento existen dos maneras de control, que son:

Control por router: donde en cada uno de estos dispositivos se ejecuta un protocolo de enrutamiento, mediante el cual intercambian información para poder elaborar las tablas de ruteo, cada *router* tiene funciones de reenvío y enrutamiento, y mantiene cada uno sus tablas de enrutamiento (ver Figura 42).

Figura 42

Enrutamiento con control por router



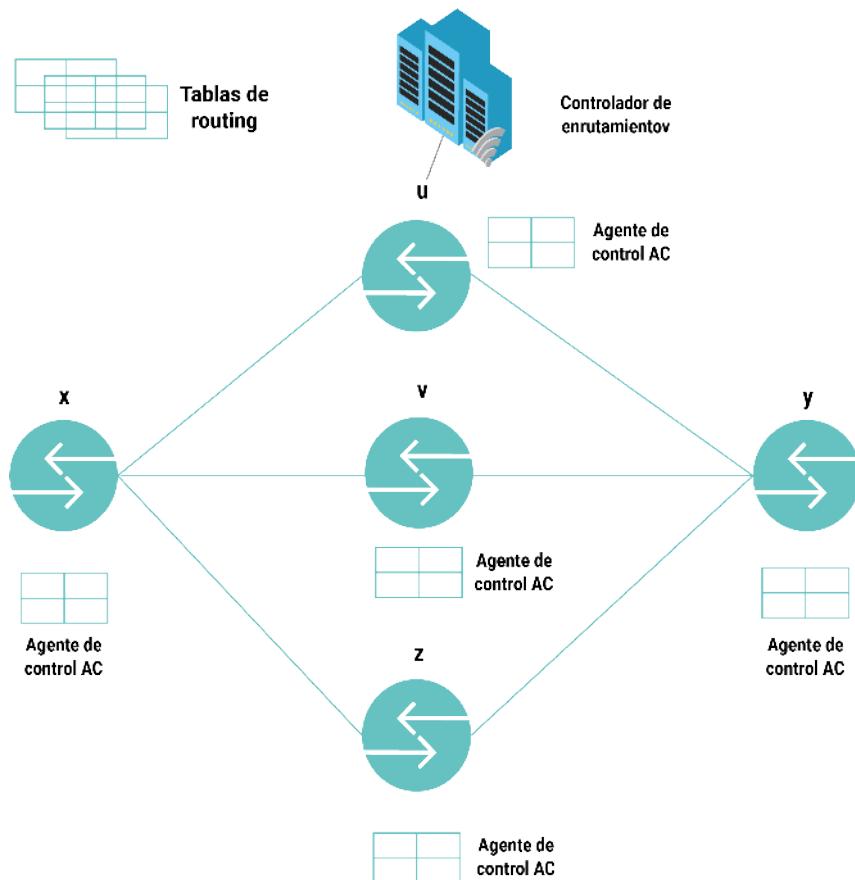
Nota. Adaptado de *REDES DE COMPUTADORAS: Un enfoque descendente* (p. 256) [Ilustración], por Kurose, J., y Ross, K., 2017, Pearson Education, CC BY 4.0.

Control lógicamente centralizado: en este caso un controlador centralizado calcula, y distribuye las tablas de enrutamiento que tienen que usar los *routers*. El controlador debe interactuar con un agente de control instalado en cada *router*, que solo tiene la función de comunicarse con el controlador, lo que

quita carga y la latencia de procesamiento de paquetes (ver Figura 43). El control centralizado se implementa mediante la técnica SDN (Software Defined Network) o redes definidas por software.

Figura 43

Enrutamiento con control lógicamente centralizado



Nota. Adaptado de *REDES DE COMPUTADORAS: Un enfoque descendente* (p. 257) [Ilustración], por Kurose, J., y Ross, K., 2017, Pearson Education, CC BY 4.0.

5.2. Algoritmos de enrutamiento

El objetivo de un algoritmo de enrutamiento es determinar las mejores rutas que son las que tienen el menor costo, por ejemplo, este costo depende del ancho de banda, número de saltos, retardo, entre otros. Entre los algoritmos de enrutamientos tenemos dos tipos:

- **Algoritmo de enrutamiento centralizado:** calcula la ruta usando la topología completa de la red, es decir, conoce todos los nodos y sus enlaces. Cada nodo conoce el estado de los enlaces de todos los nodos de la red y el coste de los mismos. El cálculo del costo puede ser realizado en un nodo centralizado o por todos los *routers* en la red. También es conocido como algoritmos de Estado Enlace (*link-state*, LS).
- **Algoritmo de enrutamiento descentralizado:** se calcula la mejor ruta por cada uno de los nodos de la red (*routers*), donde ningún nodo conoce toda la topología de la red, sino solo a sus vecinos, sus redes conectadas directamente y el coste de los enlaces. Un algoritmo descentralizado se denomina algoritmo de Vector Distancia (Distance Vector, DV).

Otra manera de clasificar los algoritmos de enrutamientos es en la forma en que se adaptan a la red, como el algoritmo de enrutamiento estático que ya vimos, y que muchas veces requiere de intervención humana; y los algoritmos de enrutamiento dinámico donde con cualquier cambio en la red estos son actualizados en las tablas sin necesidad de intervención humana.

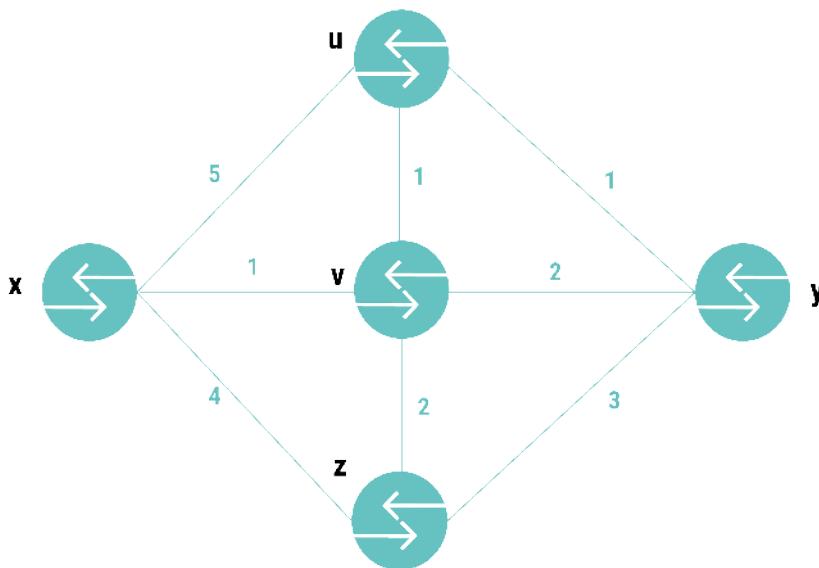
5.2.1. Algoritmo de Estado Enlace o Link-State LS

En un algoritmo de Estado Enlace es necesario conocer toda la topología de la red y los enlaces de entre los nodos. Aquí se intercambian los paquetes de estado de los enlaces que cada uno de los *routers* informa que tiene conocimiento, pero de tal manera que todos los nodos en la red conocen toda la topología, incluso de nodos remotos.

Un algoritmo conocido de estado enlace, es el algoritmo de Dijkstra o de caminos mínimos en honor a su creador, basada en la teoría de grafos, este calcula la ruta más corta desde un nodo origen hacia otros nodos que componen una red. Veamos un ejemplo de cómo funciona el algoritmo Dijkstra, del diagrama de nodos de la Figura 44.

Figura 44

Grafo para ejemplo de funcionamiento del algoritmo Dijkstra



Nota. Rohoden, K., 2024.

Para implementar el algoritmo tenemos que formar pares donde es el costo del enlace desde el nodo origen al destino, es el nodo origen. Entonces el proceso para hallar la mejor ruta entre el nodo x y el nodo y, es:

Paso 0: Armamos el par de origen en este caso sería (0,x), el coste es cero ya que es el nodo origen, y armamos la Tabla 4.

Tabla 4

Paso 0 de la resolución de ejercicio planteado sobre algoritmo Dijkstra

Nodo	Paso 0	Paso 1	Paso 2	Paso 3
X	(0, X)			
U				
V				
Z				
Y				

Nota. Rohoden, K., 2024.

Paso 1: Armamos los pares de los vecinos de X , que en este caso son los nodos U, V y Z, recorriendo el trayecto desde el nodo X hasta cada vecino (ver Tabla 5).

Tabla 5

Paso 1 de la resolución de ejercicio planteado sobre algoritmo Dijkstra

NODO	PASO 0	PASO 1	PASO 2	PASO 3
X	(0, X)			
U		(5 , X)		
V		(1 , X) → (1 , X)		
Z		(4 , X)		
Y				

Nota. Rohoden, K., 2024.



Se selecciona el nodo que tiene el menor costo acumulado, que este caso es el nodo V. Por lo que el camino parcial sería **X-V**.

Paso 2: Armamos los pares de los vecinos de V , que en este caso son los nodos U y Z, recuerde que el coste debe ser acumulado desde el nodo X, para lo cual se suma el coste del nodo seleccionado anterior con el costo del enlace al vecino (ver Tabla 6).

Tabla 6

Paso 2 de la resolución de ejercicio planteado sobre algoritmo Dijkstra

NODO	PASO 0	PASO 1	PASO 2	PASO 3
X	(0, X)			
U		(5 , X)	(1 + 1 , X) →	(2, V)
V		(1 , X) →	(1 , X)	
Z		(4 , X)	(1 + 2, V)	
Y				

Nota. Rohoden, K., 2024.

Igualmente se escoge el de menor coste acumulado, en este caso el nodo U, por lo que el camino parcial es **X-V-U**.

Paso 3: Armamos los pares de los vecinos de U, que en este caso es el nodo Y, descartamos el nodo X ya que es el origen y forma parte del camino parcial, recuerde que el coste debe ser acumulado desde el nodo X (ver Tabla 7).

Tabla 7

Paso 3 de la resolución de ejercicio planteado sobre algoritmo Dijkstra

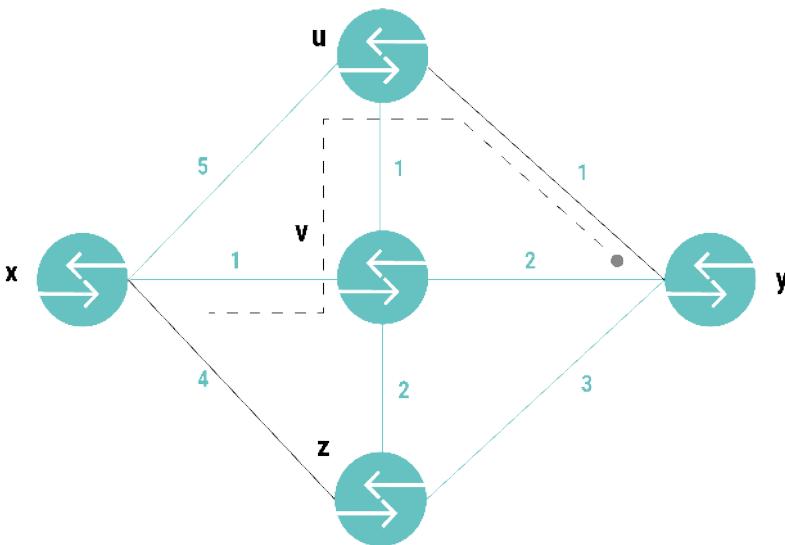
NODO	PASO 0	PASO 1	PASO 2	PASO 3
X	(0, X)			
U		(5, X)	(1 + 1, X) →	(2, V)
V		(1, X) →	(1, X)	
Z		(4, X)	(1 + 2, V)	
Y				(2 + 1, U) = (3, U)

Nota. Rohoden, K., 2024.

Igualmente seleccionamos el de menor coste acumulado, ya que en este caso solo hay un solo vecino este nodo es Y, que a su vez es el nodo destino, por lo que el mejor camino es X-V-U-Y, con un coste total de tres (3) (ver Figura 45). Si en alguna iteración hay dos nodos con el mismo coste acumulado, eso significa que haya más de un mejor camino al destino.

Figura 45

Mejor camino entre X e Y obtenido por el algoritmo Dijkstra



Nota. Rohoden, K., 2024.

5.2.2. Algoritmo de Vector Distancia o Distance Vector DV

Ahora veamos otro algoritmo conocido como algoritmo Vector Distancia DV, que a diferencia del algoritmo LS, este algoritmo es distribuido, es decir, que los nodos solo conocen a sus vecinos directamente conectados, y no a toda la red. Es asíncrono ya que no requiere que los nodos actúen sincronizados para intercambiar información. Es iterativo, ya que los nodos comparten la información de sus vecinos hasta que no hay información que compartir. También es conocido como algoritmo Bellman-Ford, ya que está basado en la ecuación del mismo nombre, la cual es:

$$d_x(y) = \min_v \{c(x, v) + d_v(y)\}$$

Donde:

$d_x(y)$: el coste mínimo de la ruta mínimo entre x e y.

\min_v : se calcula el mínimo de los costes entre todos los vecinos del nodo conectados directamente.

$c(x, v)$: costo del enlace entre x y v .

$d_v(y)$: el coste mínimo de ruta entre v a y .

Esta fórmula nos dice que, si tomamos la ruta de menor coste entre v e y denominada $d_v(y)$, el coste de la ruta entre x e y , será $c(x, v) + d_v(y)$, esto se realiza para todos los vecinos de x y luego la ruta que tenga el menor valor esa será la ruta escogida.



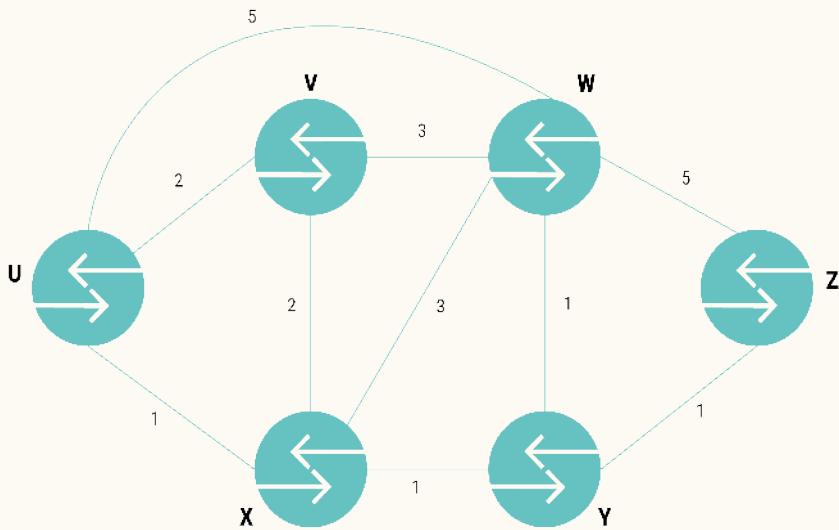
Actividades de aprendizaje recomendadas

Es hora de reforzar los conocimientos adquiridos resolviendo las siguientes actividades:

1. Le invito a revisar el video [Algoritmos de encaminamiento](#), para profundizar sobre las propiedades deseables en los algoritmos para que sean altamente eficientes.
2. Revise el vídeo del canal de YouTube Studios CAT, titulado [Algoritmo de Dijkstra](#), donde podrá encontrar un ejemplo del mismo, y el video de la Universidad Rey Juan Carlos, titulado [Algoritmos de enrutamiento: estado de enlaces](#), donde se explican los conceptos sobre este tipo de enrutamiento.
3. Revise el video del canal de YouTube de la Universidad Rey Juan Carlos titulado [Algoritmos de enrutamiento: vector de distancia](#), donde se exponen los conceptos sobre este tipo de enrutamiento.
4. Calcule la mejor ruta usando los algoritmos de Estado Enlace LS y Vector Distancia DV del diagrama de la Figura 46.

Figura 46

Ejercicio planteado para resolución de algoritmo de enruteamiento



Nota. Rohoden, K., 2024.

5. Le invito a reforzar sus conocimientos, participando en la siguiente autoevaluación. Si su nota es baja, por favor, vuelva a leer y revisar los contenidos.



Autoevaluación 5

Dados los siguientes ítems, seleccionar la respuesta correcta:

1. El control donde cada *router* ejecuta un protocolo de enruteamiento es:
 - a. Control por *router*.
 - b. Control lógicamente centralizado.
2. El control lógicamente centralizado se implementa mediante:
 - a. Redes definidas por *hardware*.
 - b. Redes definidas por *software*.
 - c. Redes privadas virtuales.
 - d. Redes públicas encriptadas.

3. El algoritmo de enrutamiento centralizado es conocido también como:

- a. Algoritmo estado enlace.
- b. Algoritmo vector distancia.
- c. Algoritmo vector enlace.
- d. Algoritmo estado distancia.

4. El algoritmo de Dijkstra es un algoritmo:

- a. Vector distancia.
- b. Vector enlace.
- c. Estado enlace.
- d. Enlace vector.

5. Un algoritmo de enrutamiento dinámico requiere de intervención humana para reconfigurar cualquier cambio en la topología.

- a. Verdadero.
- b. Falso.

6. Permite reducir la latencia y carga del procesamiento de paquetes:

- a. Control lógicamente centralizado.
- b. Control por *router*.

7. Algoritmo que no requiere conocer toda la topología de red:

- a. Algoritmo estado enlace.
- b. Algoritmo Dijkstra.
- c. Algoritmo vector distancia.
- d. Todas las opciones.

8. Algoritmo en donde todos los nodos deben conocer toda la topología:

- a. Algoritmo estado enlace.
- b. Algoritmo Dijkstra.
- c. Todas las opciones.



9. El algoritmo vector distancia es también conocido como:

- a. Algoritmo estado enlace.
- b. Algoritmo Dijkstra.
- c. Algoritmo Bellman-Ford.
- d. Algoritmo Jhonson-Ford.

10. El algoritmo vector distancia es iterativo, ya que los nodos:

- a. Actúan sincronizadamente para compartir información.
- b. Actúan de manera asíncrona para compartir información.
- c. Comparten información hasta que no haya más información.
- d. Comparten la información una sola vez.

[Ir al solucionario](#)



Resultado de aprendizaje 3:

Comparar el funcionamiento de los protocolos de enrutamiento interior con los protocolos de enrutamiento exterior.

Para alcanzar el resultado de aprendizaje se revisará los conceptos básicos sobre el protocolo de enrutamiento dinámico RIP, cuáles son sus principales parámetros, configuraciones y funcionamiento.

Contenidos, recursos y actividades de aprendizaje recomendadas

Recuerde revisar de manera paralela los contenidos con las actividades de aprendizaje recomendadas y actividades de aprendizaje evaluadas.



Semana 6

Unidad 6. Protocolos de Enrutamiento Dinámico RIP

Estimado estudiante, ahora revisaremos unos de los Protocolos de Enrutamiento Dinámico usados en las redes de datos, como es el Protocolo de Información de Ruta RIP por sus siglas en inglés. Veremos sus conceptos básicos y su funcionamiento. Los contenidos explicados están basados en (CISCO, 2019b; Sánchez et al., 2020).

6.1. Protocolo RIP

El protocolo RIP (*Routing Information Protocol*) es uno de los protocolos más antiguos de enrutamiento creado en la década de los 80 en su primera versión RIPv1 (RFC 1058), que evolucionó de algunos algoritmos básicos de ARPANET (*Advanced Research Project Agency Network*) de los Estados Unidos de Norteamérica. Luego RIP se actualizó a su versión RIPv2 (RFC 2453) para ampliar su uso en redes de mayor tamaño, mejoras de seguridad y soporte de VLSM. Actualmente, este protocolo es recomendable para redes pequeñas o medianas. RIP usa un algoritmo de Vector Distancia para calcular las rutas.

Los Protocolos de Enrutamiento Dinámico abarcan un conjunto de procesos, algoritmos y mensajes que permiten construir las tablas de ruteo y elegir el mejor camino de forma dinámica con la mínima intervención humana y adaptarse a cualquier cambio que se genere en la red mediante actualizaciones automáticas. Estos protocolos están formados por los siguientes componentes:

- **Estructuras de datos:** formado por tablas de ruteo y bases de datos, información que es guardada en la memoria RAM del *router*.
- **Mensajes:** son paquetes de datos que se intercambian entre los *routers* para actualizar la información de ruteo, armar las tablas de ruteo y descubrir *routers* vecinos conectados.
- **Algoritmos:** son los pasos necesarios para calcular el mejor camino. En el caso de RIP usa el algoritmo Vector Distancia DV.

Un algoritmo de enrutamiento dinámico usa ancho de banda en los enlaces, CPU y RAM del *router*.

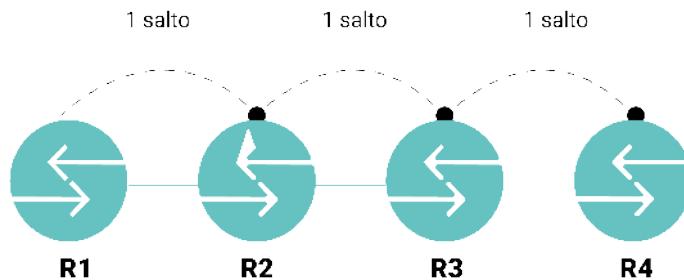
6.1.1. Especificaciones del protocolo RIP

Los enrutadores de una red deben anunciar las redes que tienen conectadas, y esta información es recibida por los demás *routers* en la red que tienen habilitado el protocolo RIP. Las actualizaciones se envían en intervalos de 30 segundos, se utiliza el protocolo de transporte UDP en el puerto 520. La métrica utilizada en este protocolo es el número de saltos. Un salto se define como el número de *routers* que existen en el camino seleccionado (ver Figura 47).



Figura 47

Ejemplo de definición de saltos en una ruta



Nota. Rohoden K., 2024.

La ruta seleccionada será la que tenga el menor número de saltos, donde el número máximo es de 15 saltos. Las métricas se actualizan cuando la métrica es menor a la almacenada. El tiempo de vida de las rutas es de 180 segundos.

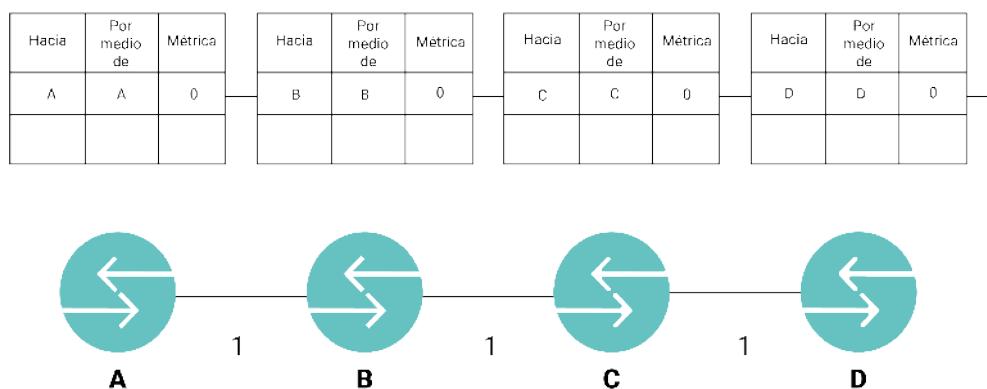
6.1.2. Funcionamiento del protocolo RIP

Ahora veamos cómo funciona el protocolo RIP, una vez que se inicia el *router* este envía difusiones por sus puertos para anunciar las redes conectadas mediante vectores de distancia. Existen dos tipos de nodos activos y pasivos, activos son aquellos que emiten las actualizaciones y los pasivos son las que las reciben.

En primera instancia, este *router* no conoce a los vecinos conectados. Otros *routers* en la red a su vez anuncian las redes que tienen conectadas, al recibir estas difusiones los *routers* deben recalcular sus tablas de ruteo (ver Figura 48).

Figura 48

Paso inicial del protocolo RIP con anuncios de rutas de redes directamente conectadas a los nodos

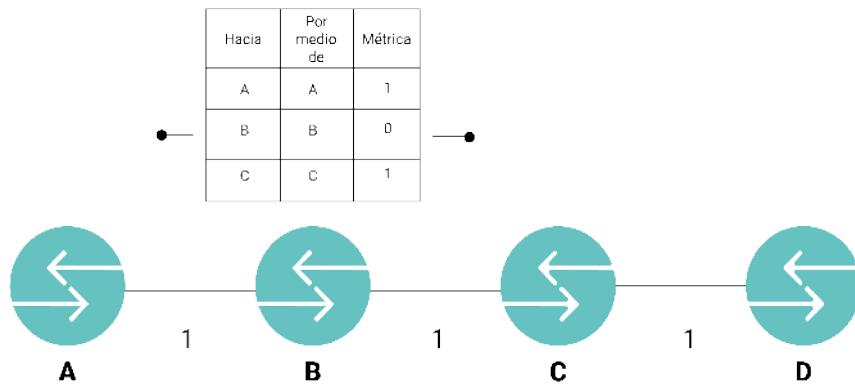


Nota. Rohoden, K., 2024.

Analicemos el nodo B, este nodo recibe los vectores distancia del nodo A y nodo C, si la red es desconocida se añade a la tabla de ruteo esta ruta, y la métrica será la suma de la métrica recibida más el coste del enlace por el que se recibió el anuncio o vector distancia. Por ejemplo, al recibir el anuncio del nodo A se pregunta si la red es desconocida, en este caso es desconocida, luego se suma la métrica recibida (0), con el coste del enlace por el que llegó (1), por lo que se obtiene de métrica uno (1). Este resultado le dice al router que la ruta para llegar al nodo A, el próximo salto es A y el número de saltos es uno (1) (ver Figura 49).

Figura 49

Tablas de ruteo del nodo B con las rutas anunciadas desde A y C agregadas

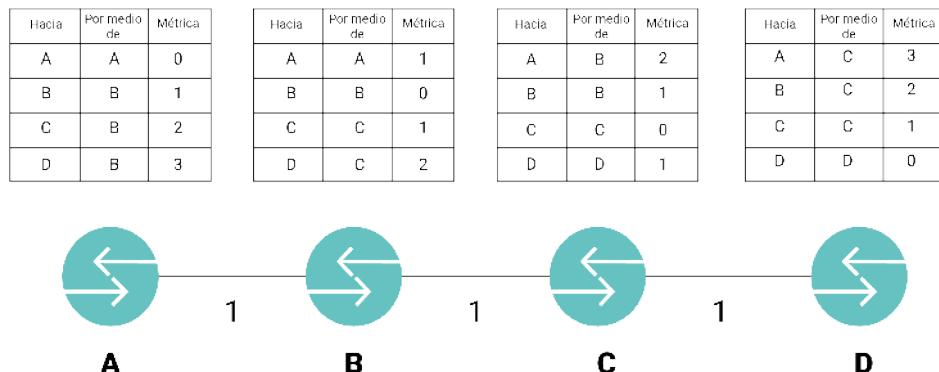


Nota. Rohoden, K., 2024.

En caso de que la ruta exista en la tabla se suma la métrica recibida más el coste del enlace recibido, si es mayor o igual se ignora la ruta, caso contrario se actualiza la ruta. Este proceso se realiza con todos los nodos, el proceso dura hasta que toda la red converge, es decir que ya no hay información que compartir entre los nodos, y todos ellos tienen las tablas de enrutamiento completas (ver Figura 50). A este tiempo se le conoce como **tiempo de convergencia**.

Figura 50

Tablas de ruteo actualizadas en todos los nodos



Nota. Rohoden, K., 2024.

Ahora revisemos el formato de las tablas de enrutamiento en el protocolo RIP.

6.1.3. Tablas de ruteo en RIP

Un *router* tiene muchas interfaces que deben tener configurada una dirección IP, la cual pertenece a una red específica, lo que es establecido mediante la máscara de subred. Estas interfaces son asociadas a las redes directamente conectadas y redes remotas, que son calculadas mediante el protocolo RIP o cualquier protocolo de enrutamiento. A continuación, vamos a revisar el formato con el que se presenta la tabla de enrutamiento en los *routers* de la marca CISCO®, un ejemplo de la misma podemos ver a continuación:

```
R2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

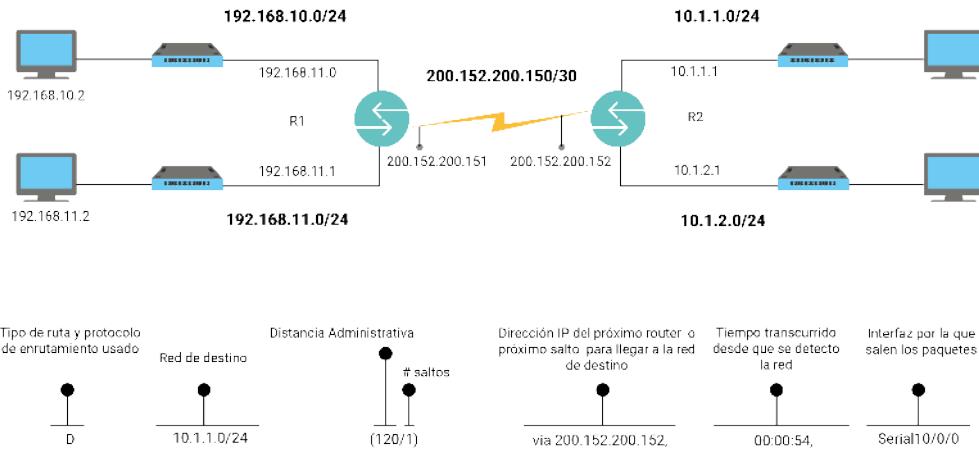
Gateway of last resort is 0.0.0.0 to network 0.0.0.0

  10.0.0.0/32 is subnetted, 1 subnets
C        10.10.10.10/32 is directly connected, Loopback0
  172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
C          172.16.1.0/30 is directly connected, Serial0/0/0
L          172.16.1.2/32 is directly connected, Serial0/0/0
C          172.16.2.0/30 is directly connected, Serial0/0/1
L          172.16.2.2/32 is directly connected, Serial0/0/1
R  192.168.99.0/24 [120/1] via 172.16.1.1, 00:00:01, Serial0/0/0
  209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.200.232/29 is directly connected, GigabitEthernet0/0
L        209.165.200.233/32 is directly connected, GigabitEthernet0/0
S*    0.0.0.0/0 is directly connected, GigabitEthernet0/0
```

En la tabla de ruteo anterior, podemos observar la ruta resaltada que es una ruta aprendida con el protocolo RIP ya que comienza con la letra R que indica que es una ruta aprendida mediante el protocolo RIP. Veamos cada uno de los componentes de la ruta especificada, que se muestran en la Figura 51.

Figura 51

Componentes de una ruta aprendida en una tabla de ruteo de un router CISCO®



Nota. Adaptado de *Enrutamiento Estático [Ilustración]*, por CCNA, 2016, [Cisco](#), CC BY 4.0.

Podemos observar en la Figura 51 que la distancia administrativa DA es 120 que permite especificar la prioridad que tiene la ruta en una tabla de ruteo, mientras menor sea la distancia administrativa mayor será su prioridad. Una ruta directamente conectada tiene una DA igual a cero (0) y una ruta estática tiene un DA igual a uno (1), por lo que siempre tienen la mayor prioridad dentro de una tabla de ruteo con respecto a otros protocolos, algunos valores de DA de varios protocolos podemos ver en la Tabla 8.

Tabla 8*Distancias administrativas de varios tipos de rutas*

Tipo de ruta	Distancia Administrativa DA
Directamente conectada	0
Estática	1
BGP externo	20
EIGRP externo	90
OSPF	110
IS-IS	115
RIP	120
BGP interno	200

Nota. Adaptado de *Enrutamiento Estático*, por CCNA, 2016, [Cisco](#).

6.1.4. Mensajes en el protocolo RIP

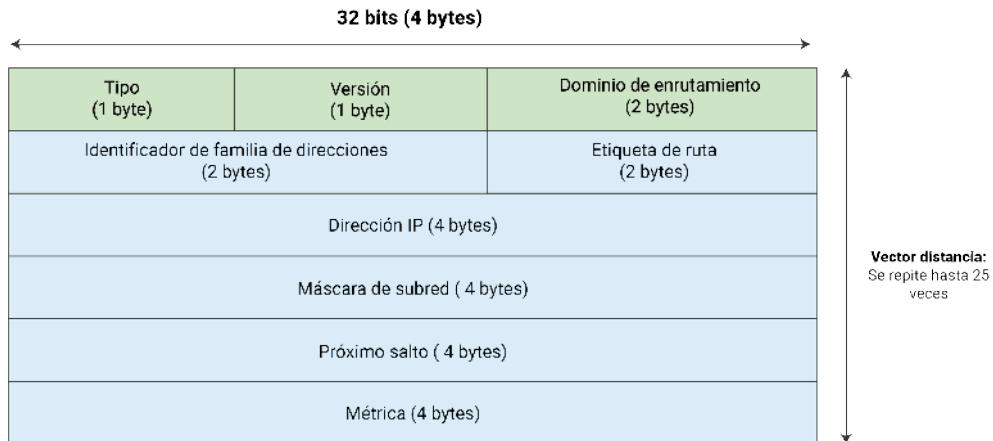
Ahora veamos cómo están estructurados los paquetes para difundir la información de ruteo mediante vectores de distancia, existen dos tipos de mensajes en el protocolo RIP, que son:

- **Request:** este tipo de mensaje son utilizados por los *routers* que, recién iniciados, se comunican para generar sus tablas de ruteo, o para actualizarlas.
- **Reply:** este tipo de mensajes son enviados cada 30 segundos en respuesta a un *request* o cuando cambia el coste de alguna ruta (actualizaciones disparadas por un evento).

Estos mensajes tienen los campos similares a un datagrama IP, estos campos se definen en la RFC 2453 para la versión 2, se pueden observar en la Figura 52.

Figura 52

Mensaje del protocolo RIPv2 de acuerdo al RFC 2453



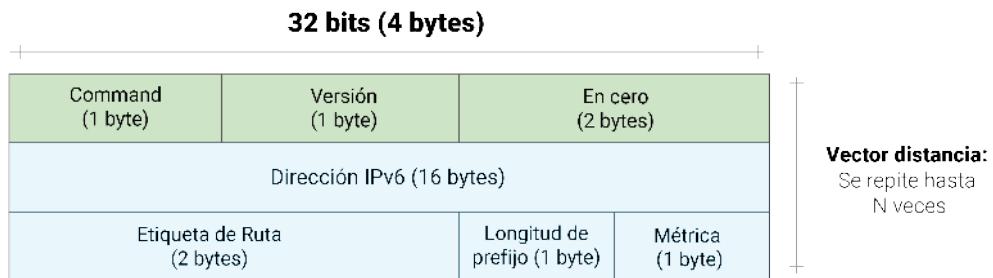
Nota. Adaptado de RFC2453 [Ilustración], por Malkin, G., 1998, RFC, CC BY 4.0.

6.1.5. RIP para IPv6

Ahora revisemos el protocolo de enrutamiento a usar en redes con IPv6 conocido como RIPng definido en la RFC2080, este protocolo trabaja con UDP en el puerto 521. El formato de los datagramas es similar a la versión de IPv4, donde se transmiten los paquetes con los Vectores Distancia (ver Figura 53), el tamaño máximo de los datagramas depende de la MTU de la tecnología de transmisión empleada (Salcedo et al., 2010).

Figura 53

Mensaje del protocolo RIPng de acuerdo a la RFC2080



Nota. Adaptado de RFC2453 [Ilustración], por Malkin, G., 1998, RFC, CC BY 4.0.

6.1.6. Horizonte partido (Split horizon)

Esta técnica permite evitar bucles de enrutamiento, que consiste en nunca difundir una ruta por la interfaz por la que se recibió la misma (Salcedo et al., 2010).

6.1.7. Actualizaciones provocadas (Triggered updates)

Permite anunciar cualquier falla en un enlace de la red antes de que caduque la vida de las rutas, esta falla es publicada con Vector Distancia con una métrica con valor infinito, es decir, la métrica toma un valor de 16 que está fuera del rango del máximo permitido en el protocolo RIP (Salcedo et al., 2010).

6.1.8. Autenticación

Como se había mencionado, la diferencia entre RIPv1 y RIPv2 es que en RIPv2 se ha agregado seguridad mediante autenticación, se usa una contraseña de 16 bytes, que se transmite en texto plano (no cifrada), también puede emplearse una autenticación cifrada como MD5.



Actividades de aprendizaje recomendadas

Le invito a realizar las siguientes actividades recomendadas:

1. Revise el vídeo del canal de YouTube de la Universidad Rey Juan Carlos denominado [*Router Information Protocol*](#), donde se exponen los conceptos sobre este tipo de enrutamiento.
2. Le invitamos a revisar la utilización de cada campo del mensaje del RIPv2 en el Protocolo [*RIPv2*](#).
3. De igual forma, revise la utilización de cada campo del mensaje del RIPng en el Protocolo [*RIPng*](#).
4. Realizar la lectura del artículo titulado [*RIP \(Routing Information Protocol\) Análisis y simulación*](#), donde se explican los conceptos y aspectos más importantes sobre el Protocolo RIP.
5. Ahora lo invito a realizar la autoevaluación que se presenta a continuación. Si su nota es baja, por favor, vuelva a leer y revisar los contenidos.



[Autoevaluación 6](#)

Dadas las siguientes preguntas, escoja la respuesta correcta:

1. Las siglas del nombre del protocolo de enrutamiento RIP significan:
 - a. Rest In Peace.
 - b. Router in Process.
 - c. Routing Information Protocol.
 - d. Routing In Protocol.
2. El protocolo de enrutamiento RIP usa algoritmo de estado enlace para encontrar la mejor ruta:
 - a. Verdadero.
 - b. Falso.



3. Versión de RIP que soporta VLSM:

- a. RIP V1.
- b. RIP V2.
- c. RIP V3.1.
- d. RIP V0.

4. El número máximo de saltos en el protocolo RIP es de:

- a. 10 saltos.
- b. 15 saltos.
- c. 20 saltos.
- d. 25 saltos.

5. Las actualizaciones de rutas en el protocolo RIP se envían en intervalos de:

- a. 10 segundos.
- b. 20 segundos.
- c. 30 segundos.
- d. 35 segundos.

6. En el protocolo RIP el tiempo de vida de las rutas es de:

- a. 60 minutos.
- b. 180 minutos.
- c. 60 segundos.
- d. 180 segundos.

7. La distancia administrativa de las rutas del protocolo RIP es de:

- a. 0.
- b. 1.
- c. 120.
- d. 90.



8. En el protocolo RIP la ruta escogida es la:

- a. Ruta con mayor número de saltos.
- b. Ruta con menor número de saltos.
- c. Ruta con el mayor ancho de banda.
- d. Ruta con la mayor velocidad.

9. Horizonte partido en el protocolo RIP significa que nunca se difunde una ruta por la interfaz por la que se recibió:

- a. Verdadero.
- b. Falso.

10. Una ruta estática tiene menos prioridad que una ruta aprendida mediante el protocolo RIP:

- a. Verdadero.
- b. Falso.

[Ir al solucionario](#)



Resultado de aprendizaje 5:

Configura los nodos de la red (ordenadores, routers, etc.).

Para alcanzar el resultado de aprendizaje en la configuración de nodos de red utilizando el protocolo OSPF, el estudiante deberá dominar los fundamentos del protocolo OSPF, comprender su función en el enrutamiento dinámico y aplicar esta comprensión para configurar adecuadamente routers y otros dispositivos de red. Esto implica configurar OSPF en los nodos, definir áreas y asignar identidades, realizar pruebas para verificar la correcta implementación y resolver problemas que surjan durante la configuración, asegurando así una red eficiente y bien gestionada.

Contenidos, recursos y actividades de aprendizaje recomendadas

Recuerde revisar de manera paralela los contenidos con las actividades de aprendizaje recomendadas y actividades de aprendizaje evaluadas.



Semana 7

Unidad 7. Protocolos de Enrutamiento Dinámico OSPF

Esta semana revisaremos otro Protocolo de Enrutamiento Dinámico conocido como Protocolo Abierto de preferencia para la Ruta más Corta u OSPF (*Open Shortest Path First*), donde veremos los conceptos básicos y su funcionamiento. Los contenidos explicados están basados en (CISCO, 2019c; Kurose & Ross, 2017; Sánchez et al., 2020).

7.1. Protocolo OSPF

Ahora revisaremos otro Protocolo de Enrutamiento Dinámico conocido como Protocolo Abierto de preferencia para la Ruta más Corta u OSPF (*Open Shortest Path First*), donde veremos los conceptos básicos y su funcionamiento. OSPF es un algoritmo de enrutamiento dinámico de gateway

interno, es decir, que se usa dentro de un mismo Sistema Autónomo AS. Un AS es un conjunto de *routers* y enlaces que están bajo la misma administración, por ejemplo, la red de *routers* de un ISP (*Internet Service Provider*) a nivel nacional. La versión 2 de OSPF se define en la RFC2328; hay que aclarar que OSPF es un Protocolo Abierto no propietario.

OSPF es un protocolo que usa algoritmos de Estado Enlace LS, es decir, usa la información del estado de los enlaces y el algoritmo Dijkstra para la selección de la mejor ruta. Cada *router* conoce la totalidad de la red, y construye un grafo con la topología del Sistema Autónomo al que pertenece. El coste de los enlaces puede ser establecido mediante las políticas del AS; en algunos casos, se puede usar como coste uno (1), para obtener el mejor camino basado en el número de saltos o usar el inverso del ancho de banda del enlace. Recuerde que la ruta seleccionada será la de coste mínimo, en *routers* que trabajan con varios Protocolos de Enrutamiento Dinámico, se escoge la de menor distancia administrativa.

7.1.1. Funcionalidades

Las funcionalidades del protocolo OSPF son:

- **Seguridad:** se usa autenticación para el intercambio de mensajes. En el intercambio de mensajes solo participan los *routers* que forman parte del Sistema Autónomo. Se puede usar una autenticación simple donde se configura una contraseña en todos los *routers*, o MD5 (*Message Digest 5*) donde se usa una función que permite verificar si los paquetes OSPF han sido cambiados.
- **Varias rutas de igual coste:** OSPF permite elegir o usar varias rutas cuando tienen igual coste.
- **Usa multidifusión y unidifusión:** permite el enrutamiento por multidifusión, usando direcciones IP *multicast*, es conocido como MOSPF (*Multicast OSPF*) definido en el RFC1584.
- **Jerarquía al interior de un Sistema Autónomo AS:** se configura un Sistema Autónomo en áreas, donde se difunde la información de enrutamiento entre

los *routers* que pertenecen al área, donde uno o más *routers* sirven de enlace entre áreas.

7.1.2. Componentes de OSPF

Los componentes del protocolo OSPF son:

- **Base de datos de adyacencia:** esta base de datos contiene información de cada vecino OSPF, que es un *router* que se encuentra en el mismo segmento de red y ejecuta el protocolo de enrutamiento OSPF. Estos deben ser descubiertos, mediante paquetes denominados *Hello*, que son generados cada 10 segundos, mediante direccionamiento *multicast* usando la dirección 224.0.0.5 como destino. Si un vecino deja de enviar paquetes *Hello*, se elimina de la tabla.
- **Base de Datos de Estado Enlace (LSDB – Link-State Database):** permite almacenar e intercambiar información de todos los *routers* que pertenecen a un área, aquí se representa la topología de la red. Cada *router* posee la misma LSDB que los demás *routers* que pertenecen al área.
- **Tabla de enrutamiento:** conformada por las listas de rutas generadas al ejecutar el algoritmo SPF, en la LSDB, estas tablas son generadas por cada *router*, donde cada uno de estos tendrá una tabla de ruteo distinta, y que le permite enrutar los paquetes hacia remotas.

7.1.3. Paquetes de OSPF

Los paquetes del protocolo OSPF que intercambian los *routers* son los siguientes:

- **Paquete Hello:** son enviados periódicamente con los listados de los vecinos OSPF, y que permiten descubrir nuevos vecinos.
- **Paquetes DBD (Description Database):** o descripción de la Base de Datos permiten intercambiar Bases de Datos.
- **Paquetes de Acuse de recibo de Estado Enlace LSA (Link-State Acknowledgement):** notifica el cambio de estado de los enlaces de los *routers*.

- **Paquete Petición de Estado Enlace LSR (Link-State Request):** Usados para solicitar Bases de Datos de Estado Enlace.
- **Paquete de Actualización de Estado Enlace LSU (Link-State Update):** Usados para responder a paquetes LSR.



7.1.4. Funcionamiento de OSPF



El funcionamiento de OSPF se realiza de acuerdo con lo especificado en la Figura 54.



Figura 54

Secuencia de funcionamiento de OSPF



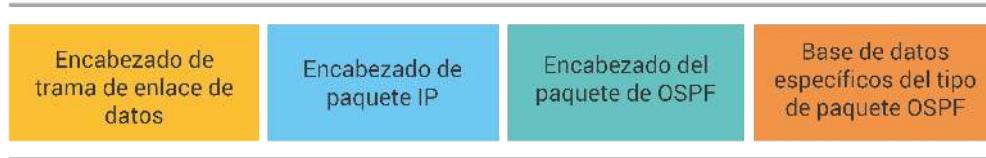
Nota. Adaptado de RFC23328 [Ilustración], por Moy, J., 1998, [IETF](#), CC BY 4.0.

7.1.5. Encapsulamiento de mensajes OSPF

OSPF tiene su propio encabezado que es agregado al encabezado IP en la payload del mismo (ver Figura 55). El encabezado del paquete de OSPF identifica el tipo de paquete OSPF, la identificación del router y el número de áreas. El encabezado tiene como dirección IP de destino una dirección de multidifusión como 224.0.0.5 o 224.0.0.6, en el campo de protocolo el valor de 89 que pertenece a OSPF. En el encabezado de la trama se usa una dirección física de multicast como es 01-00-5E-00-00-05.

Figura 55

Encapsulamiento en el protocolo OSPF

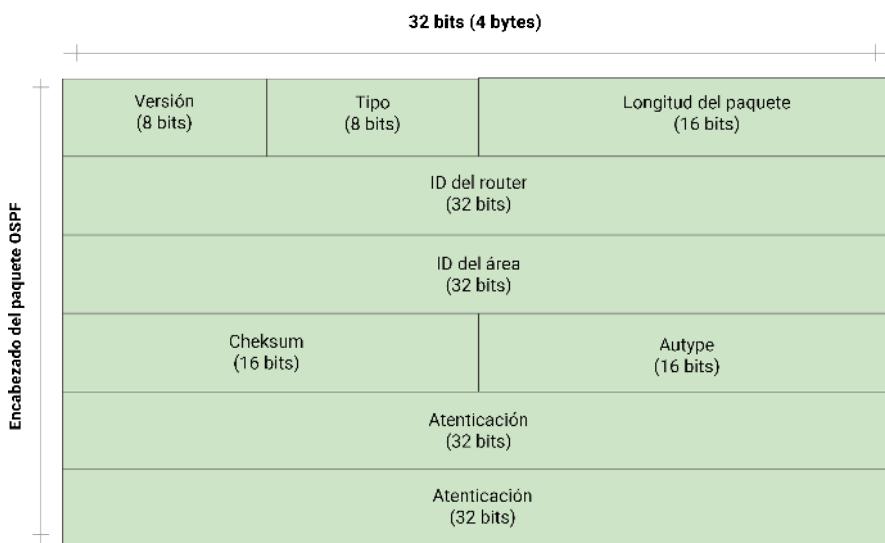


Nota. Adaptado de [RFC23328 \[Ilustración\]](#), por Moy, J., 1998, [IETF](#), CC BY 4.0.

El encabezado del paquete OSPF está estructurado según se especifica en la Figura 56.

Figura 56

Encabezado de paquete OSPF



Nota. Adaptado de [RFC23328 \[Ilustración\]](#), por Moy, J., 1998, [IETF](#), CC BY 4.0.

El campo Tipo del encabezado de OSPF se usa para indicar el tipo de paquete OSPF, y tiene los siguientes valores

Tipo de campo: 1 = saludo(hello); 2 = DBD; 3 = LSR; 4 = LSU; 5 = LSAck

7.1.6. Actualizaciones de estado enlace

Ahora veamos cómo se produce el proceso de actualizaciones de Estado Enlace en el protocolo OSPF, estas actualizaciones LSU contienen varios LSA, los mismos que poseen información de rutas y redes de destino. Este proceso se realiza de acuerdo a lo indicado a continuación:

1. Router envían paquetes DBD tipo 2, que son LSDB resumidas.
2. Routers que los reciben comparan con su LSDB.
3. Routers solicitan información más detallada de nueva ruta mediante un LSR de tipo 3.
4. Esta solicitud es respondida usando un LSU de tipo 4.

7.1.7. Estados operativos de OSPF

Para lograr la convergencia, es decir, que todos los routers tengan la topología completa de la red, se deben pasar varios estados, que están establecidos en la siguiente infografía titulada.

[Estados operativos OSPF.](#)

7.1.8. Router Designado DR y Router Designado de Respaldo BDR

Debido a que al aumentar el número de *routers* en la red, aumenta el número de adyacencias, esto puede ocasionar que al intercambiar paquetes OSPF se llegue a congestionar la red, es por ello que se elige un *Router Designado DR* (*Designated Router*) que es el único encargado de establecer las adyacencias con los otros *routers*. Este *router* se elige mediante paquetes *Hello* donde el que tenga la dirección IP más alta o la más alta prioridad configurada, conocida como RID (*Router ID*), es el elegido como DR. El DR es el único *router* que puede difundir LSA en la red.

Todos los *routers* deben tener adyacencia con el DR, adicionalmente se elige un DR de respaldo en caso de que falle el DR, conocido como BDR. La cantidad de adyacencias se calcula con la siguiente ecuación:

La cantidad de adyacencias es igual al número de routers por el mismo número menos uno para dos.



$$N = \frac{n(n-1)}{2}$$



Donde:



N: Cantidad de adyacencias.



n: Número de routers en el segmento.

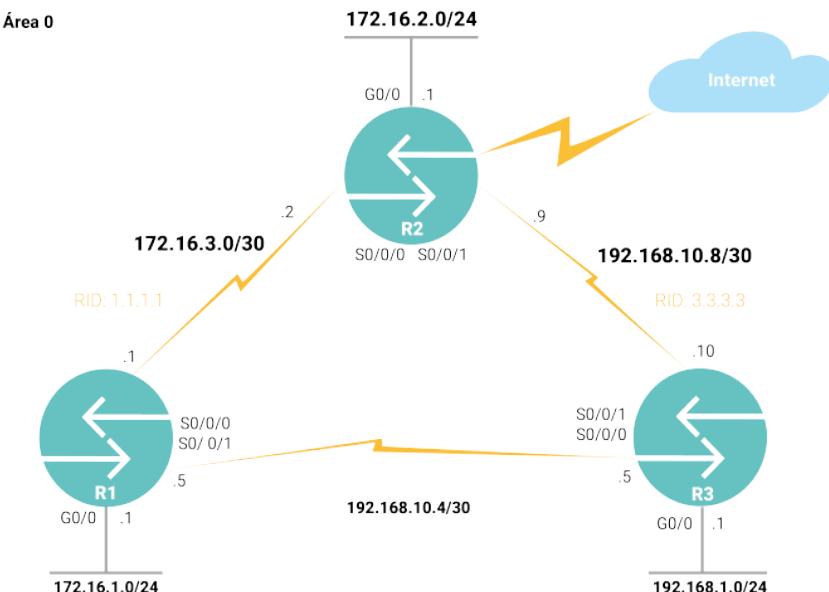


7.1.9. OSPF de área única

Se tiene un área única cuando todos los routers pertenecen al área 0 o backbone, se usa para redes pequeñas donde existen pocos routers (ver Figura 57).

Figura 57

Topología de OSPF para área única (CISCO, 2019c)



Nota. Adaptado de *Configuración de OSPF Multiárea* [Ilustración], por Cisco, 2019, [CCNA](#), CC BY 4.0.

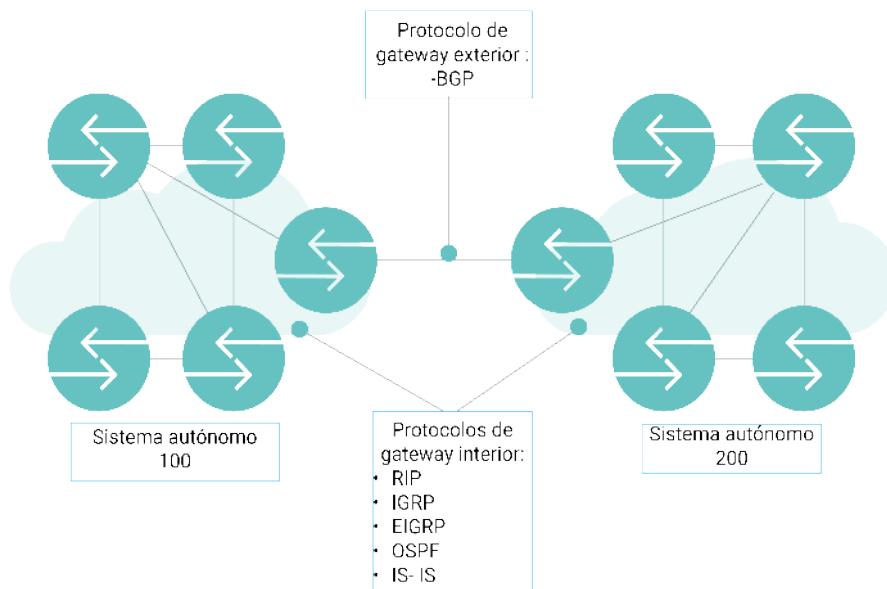
Como se observa en la Figura 57, en este tipo de topología toda el área troncal se comunica hacia otros sistemas autónomos mediante un router de la misma área troncal. Es importante configurar como pasivas las interfaces por las que no es necesario intercambiar información del protocolo OSPF, como por ejemplo del router R1, la interfaz G0/0.

7.1.10. OSPF multiárea

Ya se había dicho que un Sistema Autónomo es un conjunto de routers bajo las mismas reglas de administración o bajo el dominio de un mismo administrador, para comunicarse entre ellos utilizan los Protocolos de Enrutamiento de Gateway Interno, para comunicarse entre AS se utiliza Protocolos de Enrutamiento de puerta Externa. A estos Sistemas Autónomos se les asigna un número, que los representa. (ver Figura 58).

Figura 58

Sistemas autónomos y protocolos de Gateway interno y externo (CISCO, 2019c)

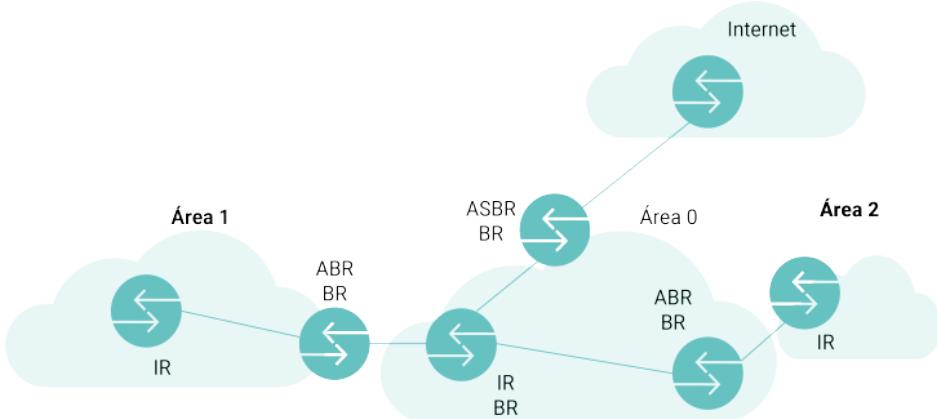


Nota. Adaptado de *Configuración de OSPF Multiárea* [Ilustración], por Cisco, 2019, [CCNA](#), CC BY 4.0.

En OSPF dentro de cada AS se divide en varias áreas, dentro de las cuales los routers intercambian información de enrutamiento, y para comunicarse con otras áreas se requieren de otros routers que sirven de enlaces (ver Figura 59).

Figura 59

Tipos de routers en el protocolo OSPF



Nota. Adaptado de *Configuración de OSPF Multiárea [Ilustración]*, por Cisco, 2019, [CCNA](#), CC BY 4.0.

En OSPF existe una jerarquía de *routers* conocidos como:

- **Internal Router (IR)**: o Router Interno que se encarga de mantener la tabla de datos de su área, y todos sus interfaces están conectadas dentro de una misma área.
- **Backbone Router (BR)**: o Router Troncal es aquel router que conecta otras áreas con el área backbone o troncal.
- **Area Border Router (ABR)**: o Router de Frontera de Área es el dispositivo que conecta varias áreas entre sí y mantiene información de enrutamiento de todas las áreas que conecta.
- **Autonomous System Border Router (ASBR)**: o Router de Frontera de Sistema Autónomo permite como enlace entre el AS con OSPF con otros Sistemas Autónomos.

Cada uno de estos *routers* intercambian mensajes conocidos como LSA (*Link State Acknowledgement*), estos mensajes pueden ser de los siguientes tipos:

- **Router Link LSA:** conocido como **LSA tipo 1** brindan información de los enlaces dentro del área a la que pertenece los *routers* y es difundido a todos los *routers* dentro del área.
- **Network Link LSA:** conocidos como **LSA tipo 2** son generados por los BR e injectados hacia un área específica.
- **Network Summary Link LSA:** conocidos como **LSA tipo 3** son generados por los ABR y enviados entre áreas con el resumen de redes IP.
- **AS external ASBR summary Link LSA:** conocidos como **LSA tipo 4**, es un LSA que se envía a un ASBR desde un ABR, contiene la métrica hacia el ASBR desde el ABR.
- **External Link LSA:** conocido como **LSA tipo 5**, es un LSA que contiene una ruta a redes fuera del AS y es generado por el ASBR.
- **NSSA External LSA:** similares a los LSA tipo 5, pero estos son generados por áreas NSSA y para ser propagados al AS, deben ser transformados en LSA de tipo 5.

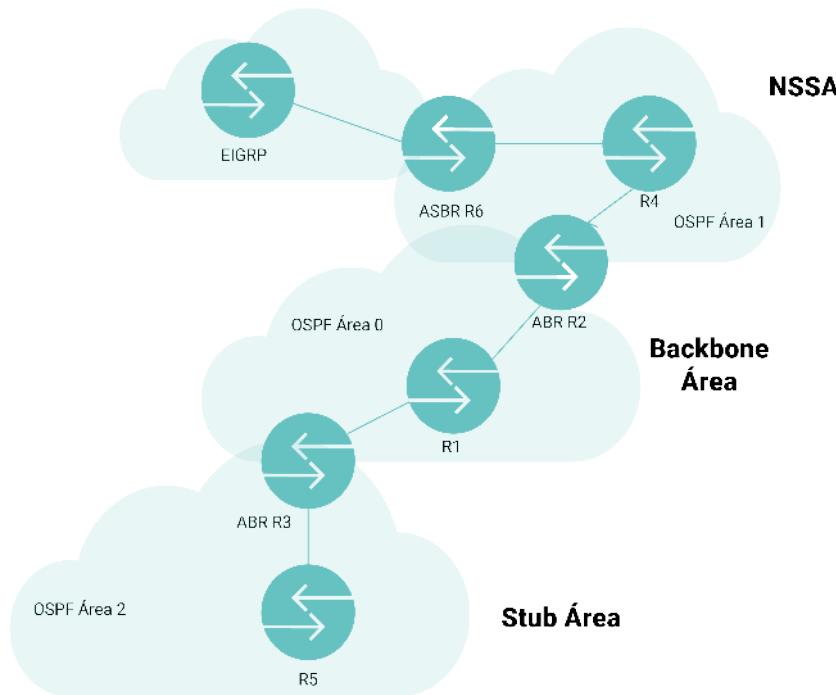
Los tipos de área en OSPF que albergan a los *routers* y donde se intercambian LSA, las cuales son las siguientes:

- **Área backbone o troncal:** conocida como **área 0**, interconecta todas las áreas dentro del AS, mediante los BR. No se pueden propagar paquetes LSA de tipo 7 en esta área, estos LSA deben ser traducidos a LSA de tipo 5.
- **Área estándar:** estas áreas se conectan al área 0, todos los *routers* del área conocen todos los *routers* internos y cada uno mantiene una tabla de ruteo diferente.
- **Área stub:** esta área, no pueden propagar LSA de tipo 5, solo pueden conectarse fuera del AS mediante una ruta por defecto.
- **Área totally stub:** no pueden propagar LSA de tipo 3,4 y 5, también requiere de una ruta por defecto para salir del AS hacia redes remotas de conectividad limitada hacia el AS.
- **Área NSSA:** estas áreas se usan para conectarse a un ISP, no admiten LSA de tipo 4 y 5. Pueden recibir rutas externas al igual que un área *Stub*, pero

no pueden propagar estas rutas hacia el área 0. Aquí se generan LSA de tipo 7 que deben transformarse a LSA tipo 5 para propagarse por el AS mediante los ABR.

Los diferentes tipos de áreas se pueden observar en la Figura 60.

Figura 60
Tipos de áreas en el protocolo OSPF



Nota. Adaptado de *Configuración de OSPF Multiárea* [Ilustración], por Cisco, 2019, [CCNA](#), CC BY 4.0.

7.1.11. Comparación entre OSPFv2 y OSPFv3

OSPF tiene dos versiones utilizadas más a menudo en el enrutamiento de datos, estas diferencias las podemos observar en la Tabla 9.

Tabla 9

Comparación entre protocolos OSPFv2 y OSPFv3

Característica	OSPFv2	OSPFv3
Protocolo soportado	IP IPv4	IPv6
Dirección IP origen	Dirección IPv4	Dirección IPv6 de link-local
Dirección destino usada	IP Dirección multidifusión 224.0.0.5 para todos los routers OSPF Dirección multidifusión 224.0.0.6 para el DR/BDR	Dirección IPv6 link-local de vecino Dirección de multidifusión FF02::5 de todos los routers OSPF Dirección de multidifusión FF02::6 del DR/BDR
Autenticación	Texto no cifrado y MD5	Autenticación de IP (IPsec)

Nota. Rohoden, K., 2024.

Una dirección IPv6 *link-local* permite que los dispositivos que se comunicuen con otros dispositivos que comparten la misma subred y los cuales no pueden ser enrutados más allá del segmento en que se originó. Estas direcciones se utilizan para intercambiar mensajes de OSPFv3.



Actividades de aprendizaje recomendadas

Con el propósito de reforzar sus conocimientos, le invito a desarrollar las siguientes actividades:

1. Le invito a revisar el video titulado: [Protocolo de routing de redes OSPF](#), donde se exponen los conceptos básicos sobre OSPF.
2. Con esta base, revise el video [OSPF Explicado en 5 Minutos](#), donde tiene disponible la explicación de cómo se implementa OSPF en Cisco Packet Tracer. Intente replicar la práctica.

3. Ahora lo invito a reforzar los conocimientos adquiridos mediante el desarrollo de la autoevaluación que se presenta a continuación. Si su nota es baja, por favor vuelva a leer y revisar los contenidos.



Autoevaluación 7

Dadas las siguientes preguntas, seleccionar la respuesta correcta:

1. OSPF es un protocolo de *gateway* interno, lo que significa:

- a. Se usa para comunicarse entre AS.
- b. Se usa para comunicarse solo con *routers* de la misma marca.
- c. Se usa para comunicarse al interior de un AS.
- d. Se usa para comunicarse solo con *switches* de la misma marca.

2. Las siglas del nombre del protocolo OSPF significan:

- a. *Open Shortest Path First*.
- b. *Open Short Path First*.
- c. *Open Setting Path Found*.
- d. *Off Shutdown Path First*.

3. OSPF usa el algoritmo:

- a. Vector distancia.
- b. Estado enlace.
- c. Vector estate.
- d. Bellman - Ford.

4. La base de datos de adyacencia:

- a. Contiene información de cada vecino OSPF.
- b. Representa la topología de la red.
- c. Contiene la lista de rutas generadas.



5. La base de datos de estado enlace LSDB:

- a. Contiene información de cada vecino OSPF.
- b. Representa la topología de la red.
- c. Contiene la lista de rutas generadas.

6. Paquete OSPF que permite descubrir nuevos vecinos:

- a. Paquete Hello.
- b. Paquete DBD.
- c. Paquete Link-State ACK.
- d. Paquete LSR.

7. Paquete OSPF que permite solicitar bases de datos de estado enlace:

- a. Paquete LSU.
- b. Paquete DBD.
- c. Paquete Link-State ACK.
- d. Paquete LSR.

8. No es un estado operativo de OSPF:

- a. Estado Up.
- b. Estado Init.
- c. Estado Exstart.
- d. Estado Exchange.

9. En OSPF de área única todos los routers pertenecen al área backbone o:

- a. Área 1.
- b. Área 2.
- c. Área 0.
- d. Área 3.



10. Tipo de router en OSPF multiárea que permite conectar el sistema autónomo con otro AS:

- a. Internal Router IR.
- b. Backbone Router BR.
- c. Area Border Router ABR.
- d. Autonomous System Border Router ASBR.

[Ir al solucionario](#)



Resultados de aprendizaje 1 a 5:

- Diseña y construye múltiples redes y las conecta entre sí.
- Diseñar y dimensionar escenarios de red.
- Comparar el funcionamiento de los protocolos de enrutamiento interior con los protocolos de enrutamiento exterior.
- Describir las estrategias para garantizar la disponibilidad de acceso a la red en redes conmutadas y enrutadas.
- Configura los nodos de la red (ordenadores, routers, etc.).

Para alcanzar los resultados de aprendizaje, los estudiantes se enfocarán en diseñar y conectar redes, comprendiendo la capa de red y su direccionamiento mediante lecturas y recursos interactivos. Aprenderán a configurar direcciones IPv4 e IPv6 y trabajarán en diversos escenarios de red. Además, compararon protocolos de enrutamiento interior y exterior para entender su funcionamiento en telecomunicaciones. También explorarán estrategias para garantizar la disponibilidad de la red, comprendiendo cómo los routers seleccionan las rutas óptimas. Finalmente, dominarán la configuración de nodos de red utilizando el protocolo OSPF para gestionar la red de manera eficiente.

Contenidos, recursos y actividades de aprendizaje recomendadas



Semana 8

Actividades finales del bimestre

Repaso de unidades 1-7

En esta semana lo invitamos a revisar los contenidos estudiados en el primer bimestre. Específicamente, deberá revisar los contenidos de las unidades 1 a la 7. Esta revisión le permitirá reforzar los conocimientos adquiridos, lo cual lo preparará para la evaluación bimestral.

También le recordamos que puede conectarse al *chat* de la tutoría para cualquier inquietud que tenga en el momento de verificar los contenidos del primer bimestre. Además, no olvide repasar las autoevaluaciones y ejercicios planteados en las unidades antes mencionadas.





Segundo bimestre



Resultado de aprendizaje 4:

Describir las estrategias para garantizar la disponibilidad de acceso a la red en redes conmutadas y enrutadas.

A través de este resultado de aprendizaje, usted identificará las principales diferencias entre la capa de red y la capa de transporte. Además, aprenderemos cuáles son las principales funciones de la capa de transporte, así como los servicios que ofrece esta capa, esto se deberá lograr realizando lectura comprensiva de la guía didáctica, revisión de los recursos complementarios como videos y realización de las actividades interactivas y recomendadas.

Contenidos, recursos y actividades de aprendizaje recomendadas

Recuerde revisar de manera paralela los contenidos con las actividades de aprendizaje recomendadas y actividades de aprendizaje evaluadas.



Semana 9

En el segundo bimestre nos centraremos en la revisión de la capa de transporte.

Le invitamos a revisar el video titulado [Servicios de transporte](#) de la Universidad Rey Juan Carlos, donde se explica de manera rápida y concisa la función de la capa de transporte.

Unidad 8. Servicios de la capa de transporte

En el segundo bimestre pondremos énfasis en los procesos que se llevan a cabo en la capa de transporte. La capa de transporte es la capa superior a la capa de red; por lo general, esta capa está implementada en los dispositivos finales de comunicación, emisor y receptor.

En esta unidad se estudia la relación que existe entre la capa de red y la capa de transporte; además, se revisan las principales tareas de la capa de transporte.

8.1. Conexión entre capa de red y capa de transporte

Antes de empezar con los contenidos de esta sección, es importante recalcar que en la pila de protocolos la capa de transporte se encuentra ubicada encima de la capa de red. De manera general, la principal diferencia entre estas dos capas se resume en lo siguiente:

- Un protocolo de capa de transporte facilita una comunicación lógica entre procesos que se ejecutan en *hosts*.
- Por otro lado, un protocolo de capa de red facilita la comunicación lógica entre *hosts*.

En la Tabla 10 se indican las principales diferencias entre la capa de red y la capa de transporte.



Tabla 10

Principales diferencias entre capa de red y capa de transporte

Capa de red	Capa de transporte
Entrega de paquetes de origen a destino a través de múltiples redes.	Responsable de la entrega del mensaje completo de origen a destino.
Brinda servicios de conexión, incluyendo control de flujo, control de errores y control de secuencias de paquete.	Puede ser sin conexión u orientada a la conexión.
Traduce direcciones de red lógicas a direcciones de máquina físicas.	Divide cada mensaje en paquetes en el origen y los vuelve a ensamblar en el destino.

Nota. Rohoden, K., 2024.

Tareas de la capa de transporte

Ahora vamos a revisar detenidamente las tareas de la capa de transporte, pero antes, vamos a indicar de forma resumida las funciones de dicha capa.

- La capa de transporte es responsable de establecer una comunicación de manera temporal entre dos aplicaciones y de transmitir datos entre ellas.
- Esta capa también es la encargada de enlazar entre las capas de aplicación y las capas inferiores.

A continuación, se indican las tareas de la capa de transporte.

a. Seguimiento de las conversaciones

Cuando una conversación fluye entre un origen y un destino, la capa de transporte hace un seguimiento de dicha conversación de forma individual por cada conversación que exista.

b. Segmentación

Esta capa divide los datos en segmentos, de tal manera, que sean más fáciles de administrar y transportar. Para poder hacer un seguimiento de dichos segmentos se agrega una cabecera.

c. Identificación de la aplicación

Esta tarea permite que todas las aplicaciones que se ejecutan en un dispositivo reciban de forma correcta los datos destinados a ellas, para esto se basa en los números de puerto.

8.2. La capa de transporte en internet

En este apartado vamos a identificar los protocolos de la capa de transporte para el modelo de referencia TCP/IP.

Los protocolos de la capa de transporte son UDP (Protocolo de Datagrama de Usuario) y TCP (Protocolo de Control de Transmisión). El protocolo UDP brinda un servicio sin conexión, mientras que el protocolo TCP proporciona un servicio orientado a la conexión.

A lo largo de esta guía, se denominará segmento a la unidad de datos de protocolo de la capa de transporte, ya sea que se esté hablando del protocolo TCP como UDP, es decir, no se usará el término datagrama para UDP para evitar confusión con la unidad de datos de la capa de red que se suele llamar o bien paquete o bien datagrama.

Con el fin de tener claras las características de los protocolos TCP y UDP, le invitamos a que llene la Tabla 11 con la comparativa entre TCP y UDP.

Tabla 11

Comparación entre TCP y UDP

Característica	TCP	UDP
Unidad de datos del protocolo		
Corrección de errores		
Control de flujo		
Principal uso		

Nota. Rohoden, K., 2024.

8.3. Multiplexación y demultiplexación

Para entender mejor el concepto de multiplexación y demultiplexación primero se debe tener claro los conceptos de números de puertos y *sockets*.

A manera de recordatorio, cada proceso que se comunica con otro proceso se identifica por uno o más puertos. Un puerto es un número que está conformado por 16 bits, lo que hace es identificar a qué protocolo o programa de aplicación debe entregar los mensajes de entrada.

Los *sockets* son puertas por donde pasan los datos de la red al proceso, y viceversa. También se los conoce como mecanismos de comunicación entre procesos que permiten que un proceso emita o reciba información con otro proceso (incluso si el otro proceso está en una máquina distinta).

Una vez que ha recordado los conceptos de puertos y *sockets* revisamos el concepto de multiplexación.

- **Multiplexación:** recolección de fragmentos de datos en el *host* de origen desde los diferentes *sockets*, encapsulando cada fragmento de datos con información de cabecera para la creación de segmentos y así pasarlo a la capa de red.

- **Demultiplexación:** se refiere a la entrega de datos contenidos en un segmento de la capa de transporte al socket correcto.

8.3.1. Multiplexación y demultiplexación sin conexión

Para tener una mejor comprensión de este tema, le invito a que revise el video [Multiplexación y Demultiplexación](#), tomado del sitio URJC_RedesComputadores, donde hay una explicación detallada.

De manera resumida, multiplexación y demultiplexación sin conexión se basan en sockets UDP. Un socket UDP está identificado por la dupla que consta de dirección IP de destino y número de puerto de destino. Dicho esto, es importante tener claro lo siguiente:

- Cuando el *host* recibe el segmento UDP.
 - Chequea el número del puerto de destino en el segmento.
 - Dirige el segmento UDP al socket con dicho número de puerto.
- Los segmentos UDP con diferentes direcciones IP origen y/o números de puerto origen dirigidos al mismo socket.

8.3.2. Multiplexación y demultiplexación orientadas a la conexión

Para la multiplexación y demultiplexación orientada a la conexión se deben considerar los sockets TCP y el establecimiento de conexiones TCP. Además, es conveniente en este punto recordar la principal diferencia entre un socket TCP y un socket UDP. Para lo cual, considerar que:

- Un socket TCP está determinado por una dupla de cuatro elementos: dirección IP de origen, número de puerto de origen, dirección IP de destino, número de puerto de destino.
- Cuando un segmento TCP llega a un *host*, el *host* emplea los cuatro valores para demultiplexar el segmento al socket apropiado.
- Dos segmentos TCP con direcciones IP de origen o número de puerto de origen diferentes serán dirigidos a dos sockets distintos.



Con el fin de reforzar los contenidos relacionados con esta unidad, le invito a revisar el siguiente video titulado: [Nmap tutorial for beginners - 1 - what is Nmap?](#), donde encontrará información relacionada con el programa Nmap. Nmap es un programa que le permitirá realizar un escáner de puertos.



Actividades de aprendizaje recomendadas

Es momento de aplicar sus conocimientos a través de las actividades que se plantean a continuación:

1. Revise el video [Protocolo UDP TCP](#), tomado del sitio Mastering IT, con el fin de establecer un primer acercamiento a estos protocolos que estudiaremos a lo largo de las próximas semanas.
2. Con el propósito de reforzar sus conocimientos, le invito a dar lectura sobre los puertos, en especial sobre los denominados puertos bien. Estos puertos son asignados por la Autoridad de Números Asignados de Internet (IANA), para lo cual diríjase a la [Página principal de asignación de puertos](#).
3. Usando el software Wireshark, ingrese a la [página web de UTPL](#) y obtenga los componentes del socket.
4. Descargue el programa [Nmap](#) de la página y realice un escaneo de puertos. A continuación, realice una tabla e indique los puertos encontrados (TCP y UDP). Además, indique si los puertos encontrados son puertos abiertos, cerrados o inalcanzables.
5. En esta unidad nos centramos en conocer la capa de transporte, los procesos de multiplexación y demultiplexación. A continuación, le invito a desarrollar la siguiente autoevaluación con el fin de reforzar los conocimientos adquiridos.





Autoevaluación 8

Dados los siguientes enunciados, seleccione la alternativa que corresponda a la respuesta correcta.

1. Seleccione las funciones principales de la capa de transporte:

- a. Establece una sesión de comunicación temporal entre dos aplicaciones.
- b. Enlaza la capa de aplicación con capas inferiores.
- c. Se encarga de la sintaxis y semántica de la información.

2. Elija los protocolos de la capa de transporte en relación con el modelo TCP/IP:

- a. UDP, HTTP.
- b. UDP, IP.
- c. TCP, UDP.
- d. TCP, HTTP.

3. ¿Cuál es el rango de los puertos "bien conocidos"?

- a. 0-1023.
- b. 1-1023.
- c. 0-1024.
- d. 1-1024.

4. Un socket UDP se representa mediante:

- a. Dirección IP de destino y número de puerto de origen.
- b. Dirección IP de destino y número de puerto de destino.
- c. Número de puerto de origen y número de puerto de destino.
- d. Dirección IP de origen y dirección IP de destino.

5. Un número de puerto se representa mediante:

- a. 8 bits.



- b. 12 bits.
- c. 16 bits.
- d. 32 bits.



6. ¿Qué número de puerto utiliza FTP?

- a. 20.
- b. 21.
- c. 22.
- d. 23.



7. ¿En la capa de transporte se manejan paquetes?

- a. Falso.
- b. Verdadero.

8. ¿Cómo se identifican de forma única las conexiones en un mismo equipo?

- a. Mediante las direcciones IP de origen y destino.
- b. Mediante sockets.
- c. Mediante la dirección de la tarjeta de la red del equipo.
- d. Mediante numeración de conexiones entrantes y salientes.

9. La multiplexación en TCP:

- a. Se realiza sobre la misma conexión de transporte, además, soporta transmisiones *full-duplex*.
- b. Se realiza sobre la misma conexión de transporte; además, no soporta transmisiones *full-duplex*.
- c. Se realiza sobre la misma conexión de transporte; además, es de tipo punto-multipunto.
- d. Soporta transmisiones *full-duplex*, además, es de tipo punto-multipunto.

10. TCP organiza los bytes en segmentos. Los segmentos también contienen un número de reconocimiento que identifica:

- a. El número de reconocimiento del octeto anterior recibido.
- b. El número de reconocimiento del *bit* anterior recibido.
- c. El número de reconocimiento del siguiente octeto que se espera recibir.
- d. El número de reconocimiento del siguiente *bit* que se espera recibir.

[Ir al solucionario](#)

Para alcanzar el resultado de aprendizaje, el estudiante debe conocer las principales características del protocolo UDP. Esto le permitirá discernir entre qué servicios funcionan mejor bajo el protocolo UDP en comparación con el protocolo TCP dependiendo del tipo de red que se use.

Contenidos, recursos y actividades de aprendizaje recomendadas



Semana 10

A partir de la unidad 9 de esta guía nos enfocaremos en las características del protocolo UDP, el cual es un protocolo de transporte sin conexión.

Lo invitamos a revisar las siguientes diapositivas sobre el [Protocolo UDP](#), que le permitirán revisar de manera simplificada las principales características del Protocolo UDP.

[Unidad 9. Transporte sin conexión - UDP](#)

En esta unidad veremos a detalle el transporte sin conexión, para lo cual se usa el Protocolo de Datagrama de Usuario (UDP, por sus siglas en inglés *User Datagram Protocol*).



9.1. Características de UDP

Antes de verificar las características del protocolo UDP, recordemos que este protocolo no está orientado a la conexión.

¿Qué significa que un protocolo no sea orientado a la conexión?

Un protocolo no orientado a la conexión es un protocolo que hace su mejor esfuerzo para entregar la información. Además, este protocolo es muy simple, ya que no proporciona detección de errores.

Las principales características de UDP son:

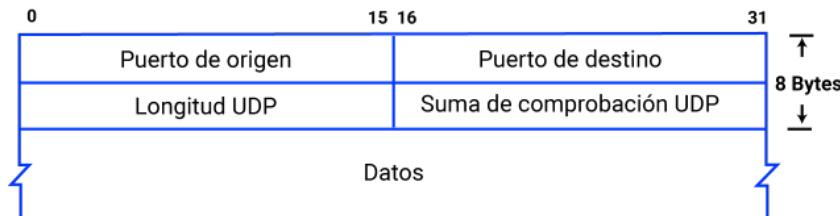
- Los datos se reconstruyen en el orden en que se recibieron.
- No se vuelven a enviar los segmentos perdidos.
- No hay establecimiento de sesión.
- No se informa al emisor sobre la disponibilidad o no de recursos.

9.2. Estructura de un segmento UDP

La estructura de un segmento UDP se indica en la Figura 61. Esta estructura se encuentra definida en el documento [RFC 768](#).

Figura 61

Estructura del segmento UDP.



Nota. Adaptado de *User Datagram Protocol* [Ilustración], por Postel, J., 1980, [datatracker](#), CC BY 4.0.

Ahora realicemos un pequeño recordatorio de cada campo del segmento UDP.

- a. **Puerto de origen.** Es el número de puerto relacionado con la aplicación del remitente del segmento UDP. Este campo es opcional, lo que significa que, si el puerto de origen no está especificado, los 16 bits de este campo se pondrán en cero.
- b. **Puerto de destino.** Este campo contiene el puerto correspondiente a la aplicación del equipo receptor al que se envía.
- c. **Longitud total.** Aquí se especifica la longitud total del segmento, con el encabezado incluido.
- d. **Suma de comprobación.** Es una suma de revisión realizada de manera tal que permita controlar la integridad del segmento. En la siguiente sección veremos más sobre la suma de comprobación.
- e. **Datos.** Se refiere a los datos de la aplicación. Por ejemplo, para una aplicación DNS, el campo de datos contiene un mensaje de consulta o un mensaje de respuesta.

9.2.1. Suma de comprobación

La suma de corrección es usada para la detección de errores. El proceso de suma, de verificación se realiza de la siguiente manera.

1. En el lado del emisor calcula el complemento a 1 de la suma de todas las palabras de 16 bits del segmento, acarreando cualquier desbordamiento.
2. El resultado se almacena en el campo de suma de revisión del segmento UDP.

Para un mejor entendimiento explicaremos un ejemplo adaptado de (Kurose & Ross, 2017) y que podrá seguir paso a paso en la Tabla 12. El mensaje tiene tres palabras de 16 bits, se suman las dos primeras y luego la tercera con la sumatoria de las primeras. Luego, se saca el complemento a 1 de la suma total y esa palabra de 16 bits se pone en el campo.

Tabla 12*Descripción del proceso de suma de comprobación*

Palabras	Proceso de suma de comprobación
	Se realiza la suma de las dos primeras palabras de 16 bits: 0110011001100000 0101010101010101 1011101110110101
Se tienen tres palabras de 16 bits 0110011001100000 0101010101010101 100011100001100	A continuación, se suma la tercera palabra a la suma anterior: 1011101110110101 100011100001100 0100101011000010
	Como paso final, se realiza el complemento a 1 de la suma resultante (0100101011000010), para lo cual se convierte todos los 0 en 1 y los 1 en 0. De esta manera, la suma de comprobación será igual a: 1011010100111101.

Nota. Adaptado de *REDES DE COMPUTADORAS: Un enfoque descendente* (7^a edición), por Kurose, J., y Ross, K., 2017, Pearson Education.

Una vez que llega al destino se suman las cuatro palabras de 16 bits, las tres que llegan en el mensaje y la palabra contenida en el campo de suma de comprobación. Si no hay error entonces la suma de comprobación debería ser 1111111111111111. Si existe algún cero en este valor entonces la información ha llegado con problemas.

9.3. Proceso de comunicación en UDP

Existen algunas propiedades que un protocolo requiere para su correcto funcionamiento. En UDP se pueden encontrar las siguientes propiedades:

- Que sea rápido.
- Que tenga baja sobrecarga.
- Que no requiera reconocimiento.
- Que no reenvíe los datos perdidos.
- Que entregue los datos a medida que van llegando.

9.3.1. Comparación de baja sobrecarga y confiabilidad de UDP

Recordemos que UDP es un protocolo no orientado a la conexión, el cual no ofrece retransmisión, secuenciación ni control de flujo. Entonces, todas las funciones que no son soportadas por UDP se deben implementar aparte.

UDP no establece ninguna conexión antes de enviar los datos

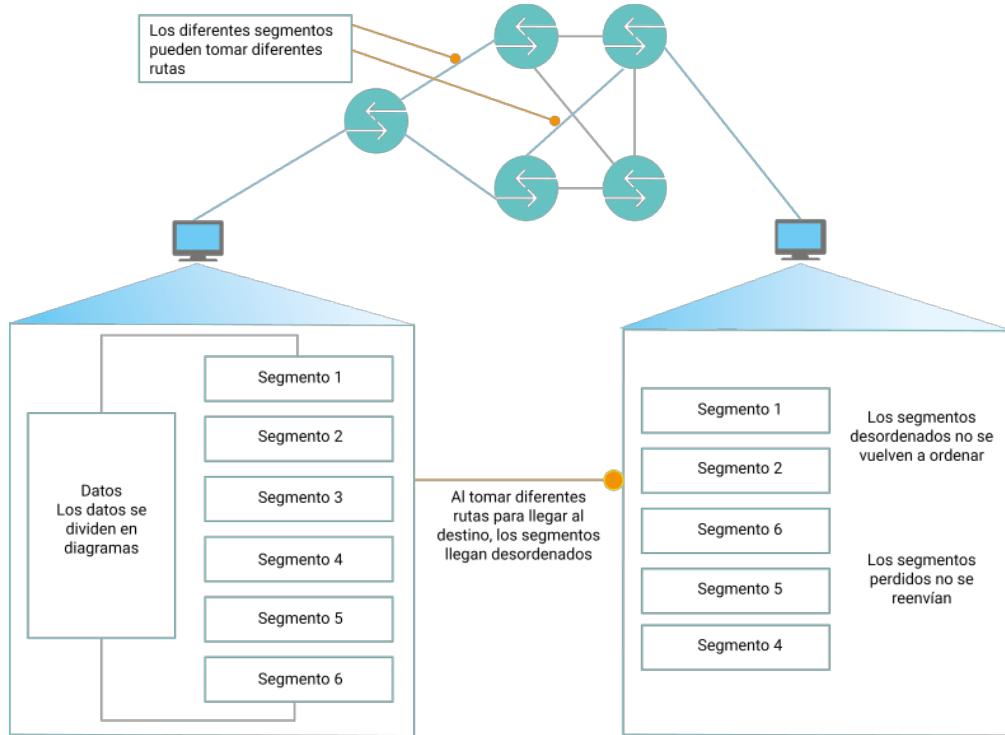
Debido a esto, la sobrecarga que UDP suministra al transporte de datos es baja. Esto se da porque UDP posee un encabezado de datagrama pequeño sin tráfico de administración de red.

Rearmado de segmentos UDP

Los datos se rearman en el orden recibido para luego ser enviados a la aplicación. Es la aplicación la que debe identificar la secuencia correcta. Sin embargo, los segmentos que están desordenados no se vuelven a ordenar, ver Figura 62.

Figura 62

Comunicación de Datos (CISCO, 2019a)



Nota. Adaptado de *Rearmado de datagramas UDP* [Ilustración], por CISCO, 2019, [Cisco](#), CC BY 4.0.

Procesos y solicitudes de servidores UDP

Las solicitudes de clientes a servidores usan número de puertos bien conocidos como puerto de destino. Por ejemplo, para el caso de solicitudes de DNS de clientes se recibirán en el puerto 53.



Actividades de aprendizaje recomendadas

Le invito a reforzar sus conocimientos mediante el desarrollo de las actividades que se presentan a continuación:

1. Con base en el ejemplo titulado “*Descripción del proceso de suma de comprobación*”, realice el cálculo del complemento a 1 en el lado del receptor.

Nota: por favor, complete la actividad en un cuaderno o documento Word.

2. Posteriormente, cambie algunos *bits* en las tres palabras iniciales simulando un error en el envío y realice nuevamente el cálculo en el lado del receptor.
3. Le invito a desarrollar la siguiente autoevaluación. Si su nota es baja, por favor, vuelva a leer y revisar los contenidos.



Autoevaluación 9

Dados los siguientes enunciados, seleccione la alternativa que corresponda a la respuesta correcta:

1. ¿La comunicación entre dos servidores DNS siempre utiliza el protocolo UDP?
 - a. Verdadero.
 - b. Falso.
2. Los puertos dinámicos o privados también se conocen como:
 - a. Puertos específicos.
 - b. Puertos registrados.
 - c. Puertos efímeros.
3. ¿En qué RFC está definido el protocolo UDP?
 - a. 1052.

- b. 768.
c. 2423.
4. ¿UDP es un protocolo de datos fiable porque utiliza la suma de comprobación para la corrección de errores?
- a. Verdadero.
b. Falso.
5. ¿Cuál es la longitud expresada en *bytes* del campo de suma de comprobación del datagrama UDP?
- a. 16.
b. 8.
c. 2.
6. La ausencia de un mecanismo de control de congestión en el UDP puede provocar:
- a. Altas tasas de pérdidas entre emisor y receptor.
b. Reducción de velocidades de transmisión.
c. Un servicio fiable de transferencia de datos.
7. ¿La aplicación DHCP trabaja con el protocolo UDP en el puerto 68?
- a. Verdadero.
b. Falso.
8. ¿A qué se debe la baja sobrecarga que proporciona UDP?
- a. A que el UDP establece una conexión antes de enviar los datos.
b. A que el UDP no establece una conexión antes de enviar los datos.
c. A que el UDP realiza la suma de comprobación.
d. A que el UDP es un protocolo de mejor esfuerzo.



9. Un paquete UDP está limitado a una máxima carga de:

- a. 65507 bits en IPv4, 65527 bits en IPv6.
- b. 65507 bits en IPv6, 65527 bits en IPv4.
- c. 65507 bytes en IPv6, 65527 bytes en IPv4.
- d. 65507 bytes en IPv4, 65527 bytes en IPv6.

10. El servicio de UDP:

- a. Protege contra la duplicación de datagramas.
- b. No protege contra la duplicación de datagramas.
- c. Provee fiabilidad.
- d. No provee fiabilidad.

[Ir al solucionario](#)

Para alcanzar el resultado de aprendizaje continuaremos con el estudio del protocolo UDP. Para lo cual usted aprenderá a reconocer un datagrama UDP. Además, mediante el software Wireshark podrá identificar los campos de cabecera UDP de un determinado servicio.

Contenidos, recursos y actividades de aprendizaje recomendadas



Semana 11

Unidad 9. Transporte sin conexión - UDP

A continuación, dentro del tema Protocolo UDP, veremos las aplicaciones que utilizan UDP.

9.4. Aplicaciones que utilizan UDP

Las aplicaciones que utilizan UDP se clasifican en 3 grupos:

1. Aplicaciones multimedia y video en vivo.



2. Solicitudes y respuestas simples.
3. Aplicaciones que manejan la confiabilidad por su cuenta.

Algunos ejemplos de estas aplicaciones son DHCP, DNS, SNMP, TFTP, VoIP e IPTV.

Estimado estudiante, con el fin de conocer los puertos de ciertas aplicaciones, en la Tabla 13 se indican los diferentes tipos de números de puerto.

Tabla 13

Tipos de números de puerto

Rango de números de puerto	Grupo de puertos
Entre 0 y 1023	Puertos bien conocidos
De 1024 a 49151	Puertos registrados
De 49152 a 65535	Puertos privados y/o dinámicos

Nota. Rohoden, K., 2024.

9.5. Diferencias entre UDP y TCP

En esta sección se presentan las principales diferencias entre UDP y TCP.

A continuación, se presenta una Tabla 14, con número de puerto, protocolo, aplicación y acrónimo para que sean llenadas por usted y así reforzar los conocimientos adquiridos hasta el momento.

Tabla 14*Aplicaciones con sus números de puerto conocidos*

Número de puerto	Protocolo	Aplicación	Acrónimo
20	TCP	Protocolo de transferencia de archivos (datos).	FTP
21	TCP	Protocolo de transferencia de archivos (control)	FTP
22	TCP	Secure shell	SSH
23	TCP	Telnet	-
25	TCP	Protocolo simple de transferencia de correo	SMTP
53	UDP; TCP	Servicio de nombres de dominios.	DNS
67	UDP	Protocolo de configuración dinámica de host (servidor).	DHCP
68	UDP	Protocolo de configuración dinámica de host (cliente).	DHCP
69	UDP	Protocolo de transferencia de archivos trivial.	TFTP
80	TCP	Protocolo de transferencia de hipertexto	HTTP
110	TCP	Protocolo de oficina de correos versión3	POP3
143	TCP	Protocolo de acceso a mensajes de internet	IMAP
443	TCP	Protocolo seguro de transferencia de hipertexto	HTTPS

Nota. Adaptado de *Número de puertos conocidos*, por CCNA, 2019, [Cisco](#).





Actividades de aprendizaje recomendadas

Con el propósito de profundizar y reforzar los conocimientos adquiridos sobre esta temática, le invito a desarrollar las siguientes actividades.

1. Para profundizar en el tema de aplicaciones que utilizan UDP, se recomienda realizar la siguiente práctica usando [Wireshark](#). Mediante el uso de Wireshark, identificar los campos de cabecera UDP usando una captura de sesión de TFTP.
2. Complete la tabla que se presenta a continuación, identificando en mayor detalle las diferencias entre protocolos UDP Y TCP.

Diferencias entre los protocolos UDP y TCP

Diferencias	
UDP	TCP

Nota: copie la tabla en un Word o cuaderno para llenar.

3. Hemos llegado al final de la unidad que estudia el Protocolo UDP. A continuación, desarrolle la siguiente autoevaluación para que así pueda profundizar en los conocimientos adquiridos de ser el caso o pueda corroborar lo ya aprendido. Si su nota es baja, por favor, vuelva a leer y revisar los contenidos.



Autoevaluación 10

Dados los siguientes enunciados, seleccione la alternativa que corresponda a la respuesta correcta.

1. UDP se multiplexa con base en los puertos, si el puerto asociado al datagrama no se encuentra:
 - a. El datagrama está encolado.



- b. El datagrama es encolado luego de generarse un comando ICMP.
- c. El datagrama está descartado.
- d. El datagrama es descartado luego de generarse un comando ICMP.
2. UDP se multiplexa con base en los puertos, si el puerto asociado al datagrama se encuentra:
- a. El datagrama está encolado.
- b. El datagrama es encolado luego de generarse un comando ICMP.
- c. El datagrama está descartado.
- d. El datagrama es descartado luego de generarse un comando ICMP.
3. UDP se multiplexa con base en los puertos, si el *buffer* se encuentra lleno:
- a. El datagrama está encolado.
- b. El datagrama es encolado luego de generarse un comando ICMP.
- c. El datagrama está descartado.
- d. El datagrama es descartado luego de generarse un comando ICMP.
4. ¿Cada puerto tiene asociada una cola?
- a. Verdadero.
- b. Falso.
5. En TCP, la memoria reservada para cada puerto (*socket*) es:
- a. Un único *buffer* de 8 kB.
- b. Dos *buffers* de 8 kB cada uno (envío y recepción).
- c. Un único *buffer* de 16 kB.
- d. Dos *buffers* de 4 kB cada uno.

6. En UDP, la memoria reservada para cada puerto (socket) es:

- a. Un único *buffer* de 8 kB.
- b. Dos *buffers* de 8 kB cada uno (envío y recepción).
- c. Un único *buffer* de 4 kB.
- d. Dos *buffers* de 16 kB cada uno.

7. En UDP, el tamaño máximo de un datagrama (incluyendo cabecera y datos) es de:

- a. 16 kB.
- b. 32 kB.
- c. 48 kB.
- d. 64 kB.

8. El tamaño de la cabecera de UDP es de:

- a. 20 bytes.
- b. 20 bits.
- c. 8 bytes.
- d. 8 bits.

9. ¿Tanto TCP como UDP pueden corregir errores?

- a. Verdadero.
- b. Falso.

10. ¿Tanto TCP como UDP pueden comprobar si hay errores?

- a. Verdadero.
- b. Falso.

[Ir al solucionario](#)

Resultado de aprendizaje 2:

Diseñar y dimensionar escenarios de red.

Para lograr alcanzar este resultado de aprendizaje, en esta unidad será capaz de identificar un protocolo de transferencia fiable de uno no fiable. Por lo tanto, usted determinará qué protocolo de capa de transporte se adapta de mejor manera a una red de datos.

Contenidos, recursos y actividades de aprendizaje recomendadas

Recuerde revisar de manera paralela los contenidos con las actividades de aprendizaje recomendadas y actividades de aprendizaje evaluadas.



Semana 12

Para poder realizar un buen dimensionamiento de una red es necesario trabajar con protocolos de transferencia de datos fiables. En la unidad 10 de esta guía nos centraremos en la construcción de este tipo de protocolos.

Lo invitamos a revisar la siguiente [Herramienta en línea](#), la cual le permite simular los protocolos GBN y SR.

Unidad 10. Principios de un servicio de transferencia de datos fiable

Una vez revisado el Protocolo UDP, en esta unidad revisaremos el Protocolo de Control de Transmisión (TCP, por sus siglas en inglés *Transmission Control Protocol*). Este protocolo fue creado con el fin de solventar las deficiencias del Protocolo UDP, como lo es una transmisión no fiable. Por lo tanto, usando TCP, la capa de transporte garantiza que la información llegue de un origen a un destino de forma fiable.

10.1. Construcción de un protocolo de transferencia de datos fiable

Para entender de mejor manera el funcionamiento del Protocolo TCP, como primera parte, vamos a revisar cómo se construye un protocolo de transferencia de datos fiable. Para esto iremos verificando algunos temas considerando un canal totalmente fiable, un canal con errores de *bit* y un canal con pérdidas y errores de *bit*.

10.1.1. Transferencia de datos fiable sobre un canal totalmente fiable

Este caso es uno de los más sencillos, ya que se considera que el canal es completamente fiable. Para explicar cómo funciona la transferencia de datos de forma fiable en este tipo de canales, usaremos el concepto de Máquinas de Estado Finitos (FSM, por sus siglas en inglés *Finite-State Machine*).

En la Figura 63 se observa la definición de emisor y receptor. Para la transferencia de datos fiable, el lado emisor simplemente acepta datos de la capa superior, crea un paquete el que contiene los datos y envía el paquete al canal. Por otro lado, en el lado del receptor, se recibe un paquete, se extraen los datos del paquete y se pasan los datos a la capa superior.

Figura 63

Protocolo para un canal fiable (Kurose & Ross, 2007)



Nota. Adaptado de *REDES DE COMPUTADORAS: Un enfoque descendente* (p. 171) [Ilustración], por Kurose, J., y Ross, K., 2017, Pearson Education, CC BY 4.0.

En este caso, con este protocolo, no existe diferencia entre unidad de datos y un paquete. Todo el flujo de paquetes va desde el emisor hasta el receptor, ya que considerando que el canal es fiable no es necesario que el receptor realice ninguna realimentación al emisor.

10.1.2. Transferencia de datos fiable sobre un canal con errores de bit

En esta sección, consideramos un caso más real en donde un canal puede estar corrompido, por ejemplo, errores de *bit*. En este caso se puede asumir lo siguiente:

- El canal podría modificar *bits* del paquete.
- ¿Cómo se resuelve el problema de los errores?
 - Mediante el uso de ACK, el emisor informa al receptor que el paquete llegó bien.
 - Mediante el uso de NAK, el receptor informa al emisor que el paquete tuvo errores, por lo tanto, el paquete se retransmite.
- Incorporar:
 - Detección de errores.
 - Retroalimentación por parte del receptor, mediante el uso de ACK y NAK.

10.1.3. Transferencia de datos fiable sobre un canal con pérdidas y errores de bit

En este caso se considera que en este canal los paquetes se pueden perder, ya sean datos o mensajes ACK. Para esto, se cuenta con suma de comprobación, número de secuencia, ACK. Se podría considerar que la retransmisión sirva en cierto grado en este tipo de canales. Por lo tanto, las estrategias que se deben considerar son:

- El emisor espera un tiempo razonable por el ACK. Si durante ese tiempo no se recibe un ACK se retransmite.

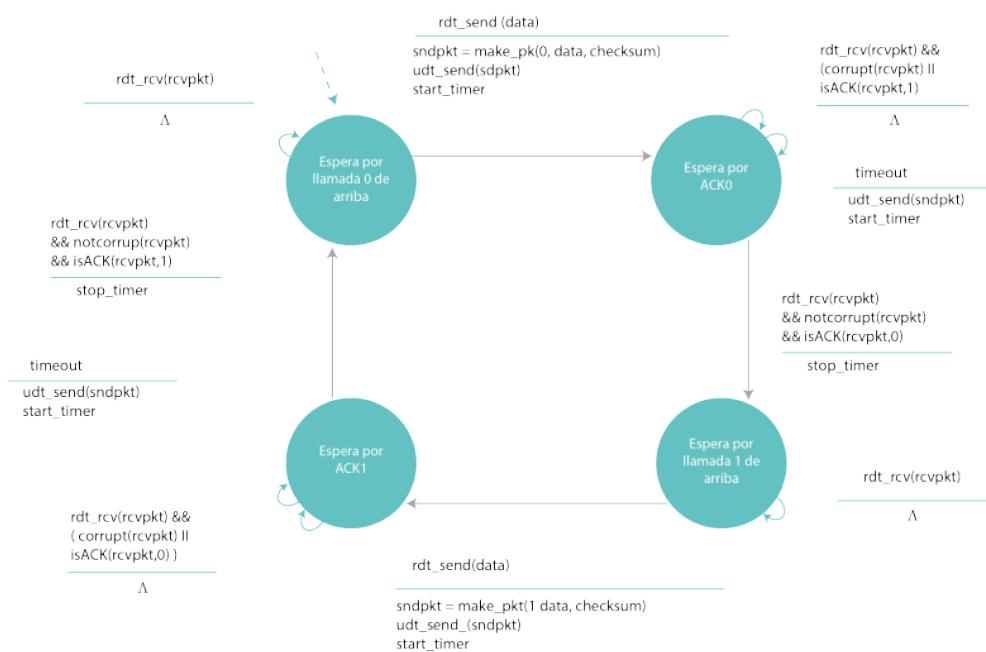
- Si, por el contrario, los datos o ACK se retrasaron, las consideraciones son:

- Números de secuencia ayudan a diferenciar en duplicado en la retransmisión.
- El receptor debe indicar el número de secuencia del paquete que es confirmado.
- Se requiere de un temporizador.

En la Figura 64 se muestra la Máquina de Estados Finitos para un protocolo que transfiere datos de forma fiable a través de un canal con pérdidas y errores de *bit*. Esta máquina de estados corresponde al emisor. Se recomienda al estudiante definir la máquina de estados para el receptor.

Figura 64

Máquina de estados en el lado del emisor (Kurose & Ross, 2007)



Nota. Adaptado de *REDES DE COMPUTADORAS: Un enfoque descendente* (p. 178) [Ilustración], por Kurose, J., y Ross, K., 2017, Pearson Education, CC BY 4.0.

10.2. Protocolo de transferencia de datos fiable con procesamiento en cadena

En las secciones anteriores, revisamos algunos protocolos, los cuales son considerados como protocolos de parada y espera. Este tipo de protocolos tienen un rendimiento muy bajo en comparación con un protocolo con procesamiento en cadena.

A continuación, llevaremos a cabo un análisis del comportamiento de parada y espera a través de un ejemplo. Las consideraciones de este ejemplo son:

- Canal con velocidad de transmisión $R = 1 \text{ Gbps}$.
- Retardo de propagación de ida y vuelta $RTT = 30 \text{ ms}$.
- Tamaño de paquete $L = 1000 \text{ bytes} (8000 \text{ bits})$.

Basándose en los datos antes dados, el tiempo necesario para transmitir el paquete por un enlace de 1 Gbps está dado por la ecuación siguiente:

$$d_{trans} = \frac{L}{R} = \frac{800 \text{ bits/paquete}}{10^9 \text{ bits/segundo}} = 8 \text{ microsegundos (us)}$$

En la Figura 65, se puede observar el funcionamiento del protocolo de parada y espera. Algunas consideraciones son:

- Tasa de utilización del emisor definida como la fracción de tiempo que el emisor está realmente ocupado enviando *bits* al canal.
- Se supone que el ACK es extremadamente pequeño y que el receptor envía el ACK tan pronto como recibe el último *bit* del paquete.
- El ACK estará de vuelta en el emisor en el tiempo calculado mediante la ecuación a continuación:

$$t = RTT + \frac{L}{R} = 30.008 \text{ ms}$$

Por lo tanto, la tasa de utilización estará dada por la ecuación que se indica:

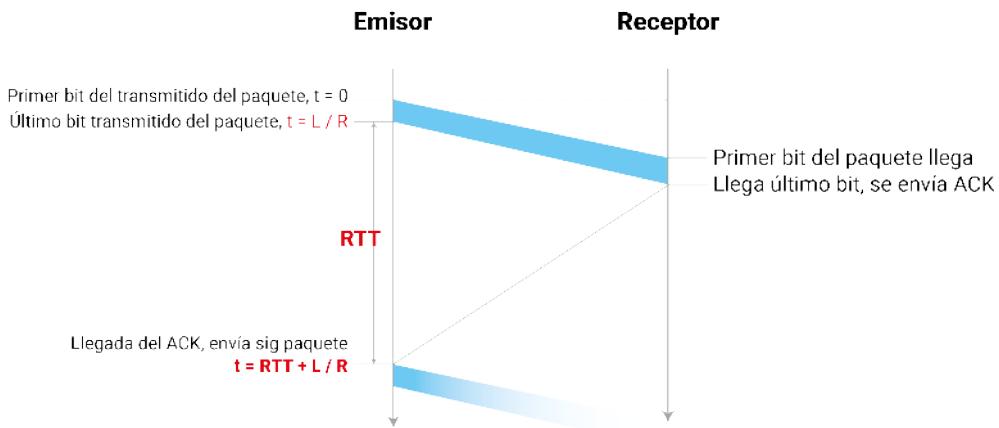
$$U_{emisor} = \frac{\frac{L}{R}}{RTT + \frac{L}{R}} = \frac{0.008}{30.008} = 0.00027$$

Como se puede observar, esta tasa de utilización del emisor del protocolo de para y espera es muy baja. Lo que significa que el emisor solo ha podido enviar 1000 bytes en 30,008 ms, una tasa de transferencia efectiva de solo 267 Kbps.



Figura 65

Protocolo de parada y espera (Kurose & Ross, 2007)

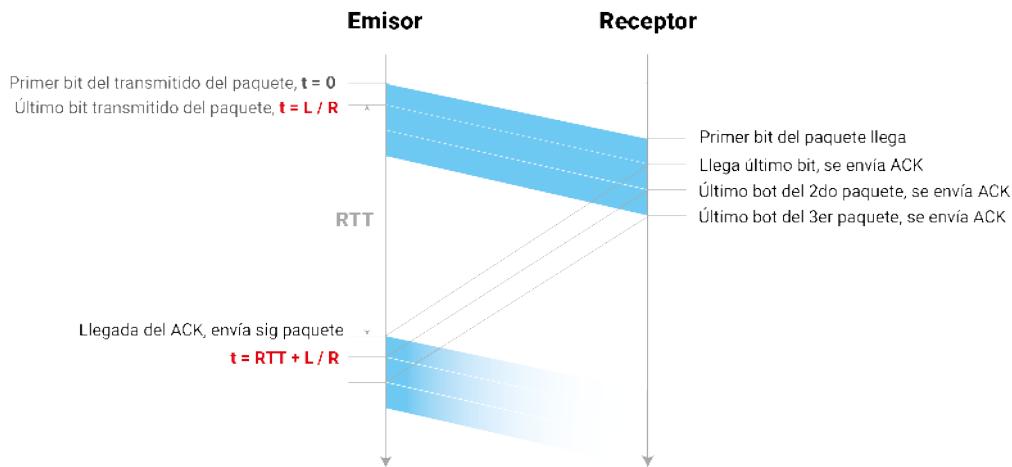


Nota. Adaptado de *REDES DE COMPUTADORAS: Un enfoque descendente* (p. 181) [Ilustración], por Kurose, J., y Ross, K., 2017, Pearson Education, CC BY 4.0.

Como solución al problema antes analizado, la solución propuesta son los protocolos con procesamiento en cadena, lo que significa que el emisor podría enviar varios paquetes sin esperar a los mensajes de reconocimiento, ver Figura 66.

Figura 66

Protocolos con procesamiento en cadena



Nota. Adaptado de *REDES DE COMPUTADORAS: Un enfoque descendente* (p. 181) [Ilustración], por Kurose, J., y Ross, K., 2017, Pearson Education, CC BY 4.0.

Observando la Figura 66, veremos que el emisor transmite tres paquetes antes de tener que esperar a los paquetes de reconocimiento. En este caso, la utilización del emisor se triplica, como se indica con la siguiente ecuación:

$$U_{emisor} = \frac{\frac{3*L}{R}}{RTT + \frac{L}{R}} = \frac{0.024}{30.008} = 0.0008$$

En conclusión, se puede decir que un protocolo de procesamiento en cadena debería manejar en forma más eficiente los números de secuencia.

Adicionalmente, tanto emisor como receptor deben contar con una memoria temporal con suficiente capacidad para el almacenamiento de paquetes.

10.3. Retroceder N (GBN)

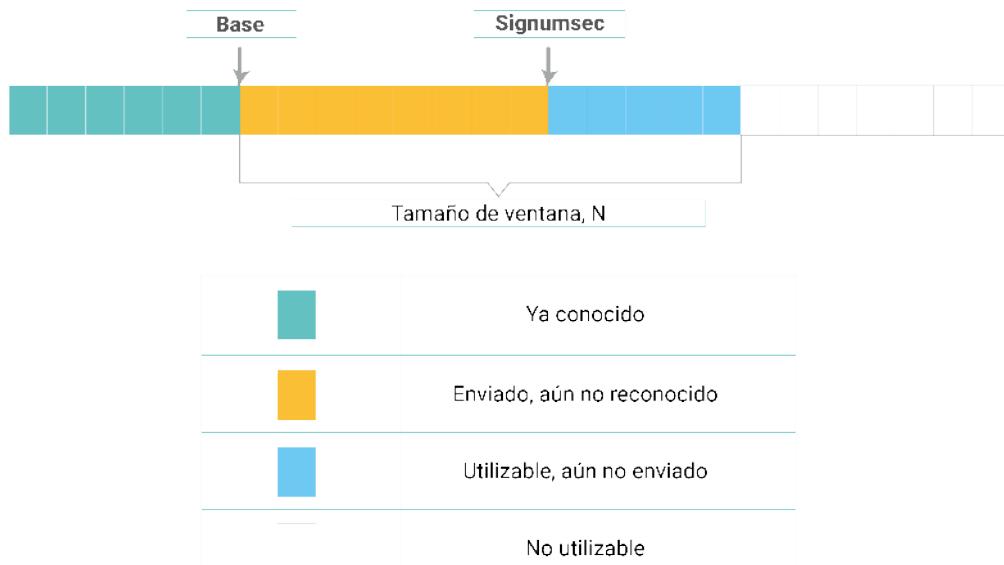
Le invitamos a revisar el video [GBN](#), tomado de URJC_RedesComputadores, en donde puede encontrar la descripción del protocolo GBN (Go-Back-N, Retroceder N). Las principales características del protocolo GBN son:

- Los paquetes pueden ser enviados por el emisor sin esperar reconocimiento.
- Es un protocolo para la transferencia fiable con procesamiento de cadena.
- Utiliza una variable, N , para determinar el tamaño de la ventana, la cual es igual al número de paquetes que pueden ser transmitidos al mismo tiempo.

El rango de los números de secuencia de un protocolo GBN se indica en la Figura 67. En donde, base es el número de secuencia del paquete no reconocido más antiguo y signumsec es el número de secuencia más pequeño no utilizado. Los paquetes de color verde son los paquetes transmitidos y reconocidos, los de color amarillo son paquetes enviados, pero todavía no se han reconocido, los de color azul corresponde a los paquetes que pueden ser enviados de forma inmediata. Los últimos, los números de secuencia mayores o iguales a $\text{base}+N$ no pueden ser utilizados hasta que un paquete no reconocido que se encuentra en el canal sea reconocido.

Figura 67

Números de secuencia, retroceder N



Nota. Rohoden, K., 2024.

10.4. Repetición Selectiva (SR)

El protocolo denominado Repetición Selectiva (SR) es un protocolo que mejora el rendimiento del protocolo Retroceder N. A continuación, veremos cómo realiza esto.

- Con el protocolo SR, el emisor solo retransmite paquetes que tienen errores o paquetes que se han perdido en el camino.
- Para esto, es necesario que tanto el emisor como el receptor cuenten con una memoria temporal. Esta memoria sirve para almacenar los paquetes antes de ser ordenados secuencialmente.
- Es importante considerar el tamaño de la memoria temporal. Si es demasiado pequeña, los paquetes se pueden perder, por otro lado, si es muy grande puede existir desperdicio de recursos.

En la Tabla 15 encontrará las principales características de SR.

Tabla 15
Características del protocolo SR

Característica	Descripción de la característica de protocolo SR
El receptor reconoce los paquetes de manera selectiva.	Los paquetes se almacenan en un buffer, y se envían de forma ordenada a la capa superior.
El emisor retransmite solo paquetes para los cuales no recibió confirmación, ACK.	El emisor maneja un temporizadores por cada paquete no confirmado.
La ventana del emisor cuenta con:	<ul style="list-style-type: none">• N números de secuencia consecutivos.• Los números de secuencia de paquetes de envío se limita a los paquetes no confirmados.

Nota. Rohoden, K., 2024.

Para profundizar en el funcionamiento de este protocolo, le invitamos a revisar el video [SR](#), tomado de URJC_RedesComputadores.

Hemos llegado a la parte final sobre los protocolos para la transferencia de datos fiable. Para sintetizar y consolidar los conocimientos adquiridos, le invitamos a revisar la siguiente infografía.

[Resumen mecanismos de transferencia de datos fiable.](#)



Actividades de aprendizaje recomendadas

Continuemos con el aprendizaje mediante su participación en las actividades que se describen a continuación:

1. Realice una revisión de los números de secuencia y cómo son usados en la versión del protocolo. Además, analice en la FSM de la versión del protocolo en qué estados se realizan los procesos de inicialización y finalización de los temporizadores.

2. Revise la herramienta en línea que le permitirá profundizar el conocimiento respecto al [Protocolo GBN](#), de manera que se familiarice con ella y aprenda el funcionamiento de la misma.
3. Revise la herramienta en línea que le permitirá mejorar el conocimiento del [Protocolo SR](#), de manera que se familiarice con ella y aprenda el funcionamiento de la misma.
4. Realice un mapa conceptual o una tabla resumen sobre los servicios que brindan los protocolos GBN y SR. Para esta actividad puede hacer uso de diversas herramientas como por ejemplo [Lucidchart](#).
5. Ahora lo invitamos a verificar los conocimientos adquiridos mediante el desarrollo de la autoevaluación que se presenta a continuación. Si su nota es baja, por favor, vuelva a leer y revisar los contenidos.



[Autoevaluación 11](#)

Dados los siguientes enunciados, seleccione la alternativa que corresponda a la respuesta correcta.

1. ¿Qué estrategia utilizan los protocolos de transferencia de datos fiable para determinar en el receptor que el mensaje ha llegado con errores?
 - a. El uso de números de secuencia.
 - b. El protocolo de repetición selectiva.
 - c. El uso de temporizadores.
 - d. El campo de suma de comprobación.
2. Se emplea para numerar secuencialmente los paquetes de datos que van desde el emisor al receptor.
 - a. Reconocimiento (ACK).
 - b. Reconocimiento negativo (NAK).
 - c. Temporizador.
 - d. Número de secuencia.



3. ¿Con SR, los paquetes no recibidos en orden se almacenan en el buffer hasta que se reciban los paquetes que faltan?

- a. Verdadero.
- b. Falso.

4. En la práctica, el número de secuencia de un paquete se incluye en:

- a. En un campo de longitud variable de la cabecera del paquete.
- b. En un campo de longitud fija de la cabecera del paquete.
- c. En el campo de suma de comprobación con longitud variable.
- d. En el campo de suma de comprobación con longitud fija.

5. ¿El emisor del protocolo GBN debe responder a 3 tipos de sucesos?

- a. Suceso de invocación, suceso de almacenamiento, suceso de fin de temporización.
- b. Suceso de invocación, suceso de recepción, suceso de inicio de temporización.
- c. Suceso de secuenciación, suceso de recepción, suceso de fin de temporización.
- d. Suceso de invocación, suceso de recepción, suceso de fin de temporización.

6. ¿Cuándo se considera a un canal totalmente fiable?

- a. Cuando no hay errores en los bits.
- b. Cuando se aplica la detección de errores.
- c. Cuando se realiza retroalimentación.
- d. Cuando se utiliza un temporizador.

7. ¿La técnica de pipeline se refiere al?

- a. Envío de paquetes con parada y espera.
- b. Envío de paquetes con procesamiento en cadena.
- c. Envío de varios paquetes.
- d. Envío de paquetes de datos duplicados.



8. ¿A qué se denomina protocolo de *bit* alternante?

- a. A la asignación de números de secuencia alternados entre 0 y 1.
- b. A la asignación de números de secuencia fijos entre 0 y 1.
- c. A la asignación de números de puerto alternados entre 0 y 1.
- d. A la asignación de números de puerto fijos entre 0 y 1.

9. La información de control y datos:

- a. Fluye de forma unidireccional.
- b. Fluye en ambas direcciones.
- c. Se envía dentro del canal subyacente.
- d. No se envía dentro del canal subyacente.

10. Si k es el número de bits contenido en el campo que especifica el número de secuencia del paquete, el rango de los números de secuencia será:

- a. $[0, 2k - 1]$.
- b. $[0, 2k-1 - 1]$.
- c. $[2k - 1, 0]$.
- d. $[2k-1 - 1, 0]$.

[Ir al solucionario](#)

A través del presente resultado de aprendizaje usted identificará las principales características de un Protocolo de Transporte orientado a la Conexión como lo es el protocolo TCP.

Contenidos, recursos y actividades de aprendizaje recomendadas



Semana 13

En esta unidad revisaremos el Protocolo orientado a la Conexión TCP.

Lo invito a revisar el siguiente video titulado [TCP](#), donde se presentan de manera resumida las principales características de TCP, del segmento TCP y la transferencia de datos fiable.

Unidad 11. Transporte orientado a la Conexión – TCP

En esta unidad vamos a revisar a detalle el Protocolo TCP, el cual es un Protocolo orientado a la Conexión. Con TCP se trabajan estrategias de entrega de datos fiables, realiza funciones de control y flujo y manejo de congestión. A continuación, vamos a entrar más a detalle en las características principales de TCP y en su funcionamiento.

11.1. Características de TCP

A modo de resumen, hemos puesto en la Tabla 16 las principales características de TCP.



Tabla 16
Características de TCP

Punto-a-punto	Un emisor, un receptor
Fiable, ordenamiento por bytes	Sin límites de mensajes.
Procesamiento en cadena	Esquemas de control de congestión y flujo inicializan la ventana.
Cuenta con buffers	Para envío y recepción.
Datos en full-dúplex	<ul style="list-style-type: none">Flujo de datos bidireccional en la misma conexión.MSS: Tamaño máximo de segmento.
Orientado a conexión	Intercambio de mensajes de control, inicializan el estado del emisor y el receptor antes de intercambiar datos.
Flujo controlado	El receptor no será saturado por el emisor.

Nota. Rohoden, K., 2024.

11.2. La conexión TCP

¿Qué significa que un protocolo sea orientado a la conexión?

Este concepto orientado a la conexión viene del hecho de que antes de que un proceso de la capa de aplicación pueda comenzar a enviar datos a otro proceso, entre los dos procesos primero se debe establecer una comunicación. Es importante recordar que TCP está definido en los documentos RFC 793, RFC 1122, RFC 1323, RFC 2018 y RFC 2581, le invitamos a revisarlos para profundizar los conocimientos de TCP.

Ahora sí, estamos listos para conocer sobre la conexión TCP. Es una conexión lógica que contiene un estado en común en los niveles TCP de los dos sistemas terminales que se comunican. Una conexión TCP se caracteriza por:

- Proporcionar un servicio *full-dúplex*.
- Ser casi siempre una conexión punto a punto.

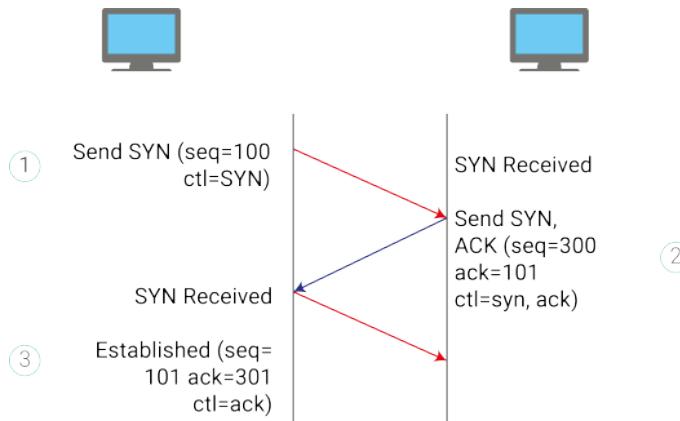
¿Cómo se establece una conexión TCP?

Para ilustrar cómo se realiza la conexión TCP vamos a referirnos a la Figura 68. Además, debemos recordar que una conexión TCP existe en un modelo cliente-servidor.

- **Primera fase.** El cliente genera la conexión hacia el puerto y la dirección del servidor utilizando un paquete conocido como SYN.
- **Segunda fase.** El paquete SYN envía también un número de secuencia del cliente. Si el servidor tiene el puerto abierto envía un paquete SYN/ ACK, este paquete contiene la confirmación con el siguiente número de secuencia del cliente. Por su parte, el servidor también envía su propio número de secuencia al cliente.
- **Tercera fase.** El cliente envía un ACK al servidor y finaliza el establecimiento de conexión. Luego de este establecimiento de conexión se empieza con el envío de información.

Figura 68

Enlace de tres vías TCP



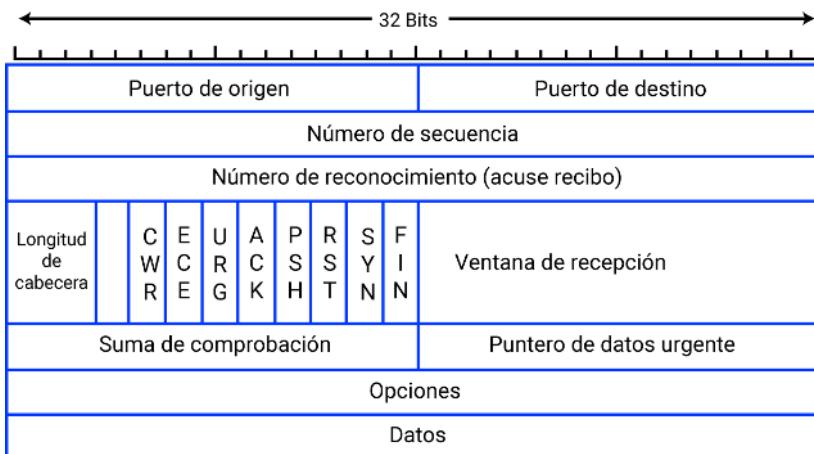
Nota. Adaptado de *Enrutamiento Estático [Ilustración]*, por CCNA, 2016, [Cisco](#), CC BY 4.0.

11.3. Estructura del segmento TCP

La estructura del segmento TCP se indica en la Figura 69. Dicho segmento está formado por campos de cabecera y campos de datos. El campo de datos contiene un fragmento de los datos de aplicación. El tamaño máximo de este campo de datos es limitado por el MSS.

Figura 69

Estructura del segmento TCP



Nota. Rohoden, K., 2024.

11.3.1. Números de secuencia y números de reconocimiento

En esta sección veremos dos campos del segmento TCP que son muy importantes para la transferencia de datos fiable de TCP. Específicamente, estos campos son número de secuencia y número de reconocimiento.

- **Número de secuencia:** este campo hace referencia al flujo de bytes transmitido y no a la serie de segmentos transmitidos. El *número de secuencia de un segmento* es el número del primer byte del segmento dentro del flujo de bytes.
- **Número de reconocimiento:** para poder entender qué es el número de reconocimiento, debemos recordar que TCP es una conexión *full-dúplex*. Esto significa que un *host A* puede estar recibiendo datos de un *host B* mientras envía datos al *host B*. El *número de reconocimiento* que el *host A* incluye en su segmento es el número de secuencia del siguiente byte que el *host A*, espera recibir del *host B*.

Le invitamos a revisar el artículo [Uso de telnet para probar puertos abiertos](#), donde se explica porque el uso de Telnet permite de manera sencilla verificar los puertos que están abiertos en un computador. El blog también ofrece una guía paso a paso de cómo puede usted mismo hacer esta verificación. Anímese a intentarlo.

11.4. Temporización

En esta sección veremos que TCP utiliza un mecanismo de fin de temporización/retransmisión para poder recuperarse de la pérdida de segmentos. Se sabe que el intervalo de fin de temporización debería ser mayor que el Tiempo de Ida y Vuelta (RTT) de la conexión. La cuestión es ¿cuánto mayor?, ¿cómo se debería estimar el RTT por primera vez? A continuación, daremos respuesta a estas preguntas.

11.4.1. Estimación del tiempo de ida y vuelta

Para poder determinar el Tiempo de Ida y Vuelta, TCP hace uso de la siguiente ecuación:

$$RTT_{estimado} = (1 - \alpha) \times RTT_{estimado} + (\alpha \times RTT_{muestra})$$

De acuerdo a la ecuación de estimación de RTT, TCP trabaja con un valor estimado basado en una muestra.

Se recuerda al estudiante que el valor $RTT_{muestra}$ se toma una muestra cada cierto período de tiempo y no para cada segmento.

Es importante saber que existe una estimación de cuánto se desvía $RTT_{muestra}$ de $RTT_{estimado}$, se conoce como variación de RTT y se define mediante la ecuación a continuación:

$$RTT_{desv} = (1 - \alpha) \times RTT_{desv} + (\beta \times |RTT_{muestra} - RTT_{estimado}|)$$

11.4.2. Gestión del intervalo de fin de temporización para retransmisión

¿Qué valor debe tomar el intervalo de fin de temporización de TCP?

La respuesta es que el valor deberá ser mayor o igual que RTT estimado. Pero es importante considerar que no deberá ser demasiado mayor a RTT estimado ya que, si esto sucede y si un segmento se pierde, el segmento no será retransmitido rápidamente por TCP. Como consecuencia, se producirán retardos muy largos en la transferencia de datos. Por lo tanto, el intervalo de fin de temporización de las retransmisiones está dado por la ecuación que sigue:

$$\text{IntervaloFinTemporización} = \text{RTT}_{\text{estimado}} + (4 \times \text{RTT}_{\text{desv}})$$

11.5. Transferencia de datos fiable

En esta sección revisaremos cómo TCP realiza una transferencia de datos fiable.

El concepto de fiable se refiere a que la información enviada por un emisor llega de forma correcta a su destino. En este sentido, TCP permite que la comunicación entre dos aplicaciones sea fiable.



Por lo tanto, las aplicaciones que usen TCP se desocupan de la integridad de la información, ya que asumen que todo lo que reciben es correcto.

La fiabilidad se considera importante en las capas de aplicación, transporte y enlace. Además, las características de un canal no fiable determinarán la complejidad del protocolo de transferencia de datos fiable.

Las principales consideraciones que tiene TCP para la transferencia de datos fiable son:

- Crea una transferencia de datos fiable sobre el servicio no fiable de IP.

- Envío de segmentos en cadena.
- Uso de ACK acumulativos.
- Uso de un único temporizador de retransmisión.
- Las retransmisiones se dan por eventos de temporizador a cero y ACK duplicados.
- Inicialmente, se considera un TCP simplificado, esto es, ignorar ACK duplicados, ignorar control de flujo y congestión de flujo.



Actividades de aprendizaje recomendadas

Con el propósito de reforzar los conocimientos sobre la temática, desarrolle las siguientes actividades:

1. Le invito a que revise el video: [Video educativo sobre negociación de la MSS](#), tomado del sitio UA - Universitat d'Alacant, donde encontrará la diferencia entre el Tamaño Máximo de Segmento (MSS, *Maximum Segment Size*) y la Unidad Máxima de Transmisión (MTU, *Maximum Transmission Unit*).
2. Realice la lectura del artículo [Formato del segmento TCP](#), para conocer la función de cada campo del segmento TCP, así como también su longitud en *bits*.
3. Revise el documento [RFC 6298](#) y observe qué valores iniciales de *IntervaloFinTemporización* se recomiendan usar.
4. Desarrolle la autoevaluación que se presenta a continuación. Si su nota es baja, por favor, vuelva a leer y revisar los contenidos.



Autoevaluación 12

Dados los siguientes enunciados, seleccione la alternativa que corresponda a la respuesta correcta.

1. Por lo general, la cabecera de TCP tiene:
 - a. 20 *bits*.
 - b. 60 *bits*.
 - c. 80 *bits*.



- d. 160 bits.
2. El campo ventana de recepción de 32 bits se utiliza para el control de flujo.
- a. Verdadero.
b. Falso.
3. ¿Cuáles son los campos que sirven para identificar la longitud y la posición en cada segmento?
- a. Número de secuencia.
b. Número de reconocimiento.
c. Suma de comprobación Internet.
d. Ventana de recepción.
4. ¿Qué utiliza TCP para el envío de datos fiable?
- a. Multiplexación y demultiplexación.
b. Paquetes ACK enviados por el receptor al emisor.
c. Números de secuencia de cada paquete.
d. Número de puerto del segmento TCP.
5. ¿Qué campos de TCP se utilizan para el establecimiento y cierre de conexiones?
- a. CWR.
b. RST.
c. SYN.
d. FIN.
6. ¿Qué campos de TCP no se utilizan en la práctica?
- a. RST.
b. ACK.
c. PSH.
d. URG.



7. Para calcular un estimado de RTT es necesario:

- a. Calcular un promedio de los valores de RTT_{muestra}.
- b. Calcular un promedio de los valores de RTT_{estimado}.
- c. Calcular un promedio de los valores de RTT_{desv.}

8. La cantidad máxima de datos que se pueden colocar en un segmento está limitada por:

- a. MTU.
- b. MSS.
- c. PPP.
- d. PSH.

9. ¿El intercambio de segmentos permite informar sobre el tamaño de ventana?

- a. Verdadero.
- b. Falso.

10. El campo Opciones dentro de la cabecera es opcional y de longitud variable, por lo general el valor es de:

- a. 1 bit.
- b. 3 bits.
- c. 4 bits.
- d. 5 bits.

[Ir al solucionario](#)

A través del presente resultado de aprendizaje, usted identificará cómo se realiza el control de flujo usando el protocolo TCP. Además, identificará las fases necesarias para establecer una conexión TCP.



Semana 14

Unidad 11. Transporte orientado a la Conexión – TCP

11.6. Control de flujo

Antes de iniciar con el tema de control de flujo por parte de TCP, es importante recordar lo siguiente:

- En TCP, el receptor tiene un *buffer* de recepción.
- Los *bytes* que son recibidos de forma correcta y en secuencia por la conexión TCP son colocados en el *buffer* de recepción.
- El proceso de aplicación leerá los datos de este *buffer*.
- La aplicación puede ser lenta con respecto a la lectura de los datos.
- El emisor puede desbordar el *buffer* de recepción enviando muchos datos demasiado rápidos.

Es en este punto, ante la posibilidad del desbordamiento de *buffer*, que TCP proporciona un servicio de control de flujo a sus aplicaciones. *Por lo tanto, el control de flujo es un servicio de adaptación de velocidades*. Básicamente, lo que hace es adaptar la velocidad a la que el transmisor está transmitiendo frente a la velocidad a la que la aplicación receptora está leyendo.

¿Cómo funciona el control de flujo?

Para que TCP pueda brindar el servicio de control de flujo, este mantiene en el emisor una variable que se conoce como *ventana de recepción*. La ventana de recepción permite dar al emisor una idea de cuánto espacio libre hay disponible en el *buffer* del receptor.

Ventana de recepción

Para estudiar la ventana de recepción, vamos a tomar como ejemplo una operación de transferencia de un archivo.

En este ejemplo se asume que un *host A* envía un archivo grande a un *host B* usando una conexión TCP. Para lo cual, el *host B* asigna un **buffer de recepción**. El tamaño de este *buffer* lo denominaremos como BufferRecepcion. Además, se consideran las variables indicadas en la Tabla 17.

Tabla 17

Variables para control de flujo en la transferencia de archivos

Variables de control de flujo	Descripción
UltimoByteLeido	Es el número del último byte del flujo de datos del buffer leído por el proceso de aplicación del host B.
UltimoByteRecibido	Es el número del último byte del flujo de datos que ha llegado procedente de la red, almacenado en el buffer de recepción del host B.

Nota. Rohoden, K., 2024.

Cabe recordar que en TCP no se permite el desbordamiento de *buffer* asignado, por lo que se debe cumplir la siguiente condición que se indica en la ecuación siguiente:

$$\text{UltimoByteRecibido} - \text{UltimoByteLeido} \leq \text{BufferRecepcion}$$

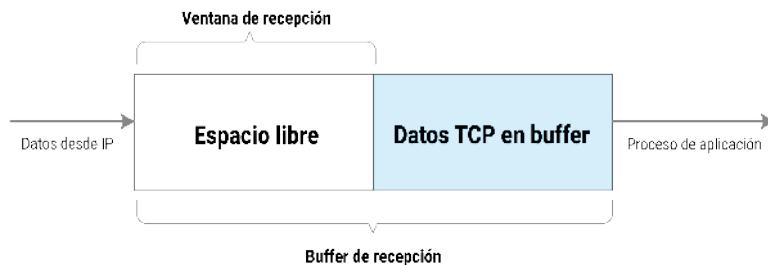
Por lo tanto, la ventana de recepción está dada por la ecuación:

$$\text{VentRepcion} = \text{BufferRecepcion} - [\text{UltimoByteRecibido} - \text{UltimoByteLeido}]$$

También se debe tener presente que la ventana de recepción es una variable dinámica, ver Figura 70.

Figura 70

Flujo de datos TCP en buffer de recepción



Nota. Rohoden, K., 2024.

11.7. Gestión de conexión TCP

El tema de gestión de conexión TCP se refiere específicamente al establecimiento y finalización de una conexión TCP. A continuación, en la Tabla 18, veremos el establecimiento de una conexión TCP mediante tres pasos (*three way handshake*).

Tabla 18

Proceso de acuerdo en tres fases

Paso	Descripción	Ilustración gráfica
1	<ul style="list-style-type: none"> • TCP cliente envía un segmento TCP. • Este segmento no contiene datos de la capa de aplicación. • El bit SYN de la cabecera del segmento se pone <>a 1. 	<p>Diagrama que muestra un cliente y un servidor conectados por una red. El cliente envía un segmento TCP con el bit SYN establecido (labeled 'SYN') hacia el servidor.</p>
2	<ul style="list-style-type: none"> • Extremo servidor envía un segmento al cliente que confirma (ACK) la recepción de SYN. • Este segmento no tiene datos de la capa de aplicación. • Contiene 3 segmentos, bit SYN se pone a 1, el campo de reconocimiento es igual a cliente_nsi+1, número de secuencia inicial del servidor igual a servidor_nsi. 	<p>Diagrama que muestra el servidor respondiendo al cliente con un segmento que incluye un ACK y un SYN (labeled 'SYN, ACK').</p>
3	<ul style="list-style-type: none"> • Extremo cliente envía una confirmación al SYN del servidor. • Este segmento no tiene datos de la capa de aplicación. • Conexión establecida. 	<p>Diagrama que muestra el cliente respondiendo al servidor con un ACK (labeled 'ACK'), estableciendo la conexión. Ambos extremos muestran un cuadro azul 'Conectado'.</p>

Nota. Adaptado de *REDES DE COMPUTADORAS: Un enfoque descendente* (7^a edición) (p. 209 – 211), por Kurose, J., y Ross, K., 2017, Pearson Education.



Actividades de aprendizaje recomendadas

Desarrolle las siguientes actividades:

1. Revise el video [Mecanismo de control de flujo por ventana deslizante](#), tomada del sitio Universitat Politècnica de València, en el cual se explica cómo usar la ventana de recepción para proporcionar el servicio de control de flujo. Luego realice una breve explicación.
2. Complete la siguiente tabla con el fin de recordar los principales conceptos de una conexión TCP.

Conceptos de una conexión TCP

Concepto	Relación con TCP
Segmento SYN	
Segmento TCP	
Segmento SYNACK	
Cliente_nsi	
Servidor_nsi	
Segmento de desconexión	

Nota: por favor, complete las actividades en un cuaderno o documento Word.

3. Lo invito a reforzar sus conocimientos a través del desarrollo de la siguiente autoevaluación. Si su nota es baja, por favor, vuelva a leer y revisar los contenidos.





Autoevaluación 13

Dados los siguientes enunciados, seleccione la alternativa que corresponda a la respuesta correcta.

1. El campo número de reconocimiento limita el tamaño de la ventana a:

- a. 60535 bits.
- b. 60535 octetos.
- c. 65535 bits.
- d. 65535 octetos.

2. El escalado de ventana permite escalar el valor de la ventana y utilizar ventanas:

- a. De mayor tamaño.
- b. De menor tamaño.
- c. De igual tamaño.
- d. De la mitad del tamaño.

3. ¿El campo *checksum* es un campo obligatorio?

- a. Verdadero.
- b. Falso.

4. El valor NSI+1 debe ir en el campo número de reconocimiento y corresponde a:

- a. Al primer *bit* que espera recibir.
- b. Al primer octeto que espera recibir.
- c. Al último *bit* que espera recibir.
- d. Al último octeto que espera recibir.

5. ¿El segmento SYN consume dos números de secuencia?

- a. Verdadero.
- b. Falso.

6. Una conexión TCP puede terminarse de forma simétrica o asimétrica.

La terminación asimétrica es unilateral, es decir:

- a. Uno de los dos *hosts* decide terminar y termina la conexión en ambos sentidos.
 - b. Uno de los dos *hosts* decide terminar y termina la conexión en un sentido.
 - c. Los dos *hosts* deciden terminar y terminan la conexión en ambos sentidos.
 - d. Los dos *hosts* deciden terminar y terminan la conexión en un sentido.
7. ¿La terminación asimétrica puede provocar la pérdida de información?
- a. Verdadero.
 - b. Falso.
8. ¿La terminación simétrica supone el intercambio de tres mensajes similar al proceso de conexión?
- a. Verdadero.
 - b. Falso.
9. ¿Para qué sirve el segmento SYN?
- a. Un *bit* de control del segmento TCP.
 - b. Un *bit* indicador de reconocimiento.
 - c. Un *bit* para indicar que se ha recibido un segmento TCP.
 - d. Un *bit* para indicar que el campo de puntero de urgencia es significativo.
10. El control de flujo es un servicio que:
- a. Limita la cantidad de datos introducidos en la red.
 - b. Limita la cantidad de datos introducidos en la ventana de recepción.



- c. Adapta la velocidad de transmisión a la velocidad de lectura.
- d. Adapta la velocidad de lectura a la velocidad de transmisión.

[Ir al solucionario](#)



Contenidos, recursos y actividades de aprendizaje recomendadas



Semana 15

En esta unidad revisaremos el control de congestión que realiza el protocolo TCP. Para comprender de mejor manera el control de congestión es necesario que tenga claros los conceptos de temporizador, ventana de congestión, ventana de recepción. Además, es muy importante que sepa cómo funciona el algoritmo de control de congestión, el cual está estandarizado en el documento RFC 5681.

Lo invitamos a revisar el documento titulado [Control de congestión en TCP](#). En este documento se presentan algunos algoritmos del control de congestión y algunas consideraciones de seguridad.

Unidad 12. Control de congestión

En esta unidad se revisarán los principios del control de congestión, así como las causas y los costes de la misma.

12.1. Introducción a la congestión

Cuando la red se congestionada, existe la pérdida de paquetes por lo general, es el resultado del desbordamiento en los *buffers* de los *routers*. Es así que para reducir la congestión de la red es necesario, mecanismos que regulen el flujo enviado por los emisores.

A continuación, en la Tabla 19 encontrará tres posibles escenarios de congestión (Kurose & Ross, 2017).

Tabla 19
Escenarios de congestión

Escenario	Características técnicas	Efecto observado / Consecuencia
Escenario 1	2 emisores, 2 receptores. 1 router, buffers infinitos. Sin retransmisiones.	Ante la congestión los retardos incrementan.
Escenario 2	1 router, buffers infinitos. El emisor retransmite paquetes perdidos.	Más trabajo para enviar los datos. Retransmisiones innecesarias.
Escenario 3	4 emisores. Caminos multi-salto. Mecanismo de fin de temporización/retransmisión.	Tasa de transferencia decrece. Capacidad de transmisión desperdiciada.

Nota. Adaptado de *REDES DE COMPUTADORAS: Un enfoque descendente* (7^a edición) (p. 215 – 219), por Kurose, J., y Ross, K., 2017, Pearson Education.

En conclusión, en el primer escenario al ser el router compartido entre dos conexiones, la tasa de transferencia para cada conexión será la mitad de la capacidad total del router. Con respecto al segundo escenario, la memoria temporal del router es finita por lo que si la memoria se llena los paquetes serán descartados. En el tercer escenario la complejidad se incrementa debido a la existencia de más enrutadores intermedios y conexiones.

12.2. Métodos para controlar la congestión

En esta sección revisaremos los dos métodos más comunes para controlar la congestión, específicamente, control de congestión terminal a terminal y control de congestión asistido por la red.

12.2.1. Control de congestión terminal a terminal

De acuerdo a este método, la presencia de congestión es inferida por los sistemas terminales mediante la pérdida de paquetes y los retardos. En este sentido, no existe un soporte explícito de la red y es el método que usa tradicionalmente TCP para controlar la congestión mediante el conocimiento de:

- Pérdida de segmentos TCP, la cual es indicada a través de un fin de temporización o por la recepción de un triple paquete ACK duplicado.
- Valores de retardo de ida y vuelta crecientes.

12.2.2. Control de congestión asistido por la red

En este método, los *routers* realimentan de forma explícita a los terminales informando el estado de la congestión de red. Esta realimentación se puede realizar de dos formas:

- Forma directa, con un mensaje explícito.
- Forma indirecta, marcando un campo en algún paquete. Esta forma involucra el uso de RTT.

12.3. Mecanismo de control de congestión de TCP

En esta sección revisaremos cómo TCP realiza el control de congestión.

Es importante recalcar que el método que utiliza TCP para realizar el control de congestión se basa en terminal a terminal y no en el asistido por la red. Esto se debe a que la capa IP no brinda una realimentación clara a los sistemas terminales en lo que se refiere a congestión de la red. El método empleado por TCP se puede resumir en la siguiente Figura 71 Control de congestión según TCP.

Figura 71

Control de congestión según TCP

- 1 Cada emisor limita la velocidad a la que transmite el tráfico a través de su conexión en función de la congestión de red percibida.
- 2 Al percibir la congestión, el emisor incrementará su velocidad de transmisión.
- 3 Si la congestión es percibida a lo largo de la ruta, el emisor reducirá su velocidad de transmisión.

Nota. Rohoden, K., 2024.

Además, recordemos que, para poder determinar la existencia de congestión, TCP utiliza el temporizador y la recepción de tres ACK del mismo segmento. Recuerde que:

- El temporizador finaliza indicando que el segmento se ha perdido (o ha sido descartado por los enrutadores intermedios).
- Los ACK duplicados informan que ha existido la pérdida de segmentos.

Ventana de congestión

La ventana de congestión es una variable utilizada por TCP para el control de congestión. Esta ventana restringe la velocidad a la que el emisor TCP puede enviar tráfico de la red. Es decir, la cantidad de datos no reconocidos en un emisor no puede exceder el mínimo de VentCongestión entre y VentRecepción, esto está definido por la siguiente ecuación:

$$\text{UltimoByteEnviado} - \text{UltimoByteReconocido} \leq \text{minVentCongestion}, \text{VentRepcion}$$

Por lo tanto, la tasa de datos está dada por la ecuación:

$$\text{tasa} = \frac{\text{VentCongestion}}{\text{RTT}} \text{bytes/s}$$

Recordemos que la ventana de congestión es dinámica, ya que la congestión de la red es percibida por el emisor.

Algoritmo de control de congestión de TCP

El algoritmo está estandarizado en el documento RFC 5681 y consta de cuatro componentes: arranque lento, evitación de la congestión, recuperación rápida y retransmisión rápida. A continuación, se indican las principales características de estos componentes.

1. Arranque lento

- Cuando la conexión se inicia, el valor de la ventana de congestión es pequeño. Este valor es igual a 1 MSS (Tamaño Máximo de Segmento).
- El ancho de banda disponible podría ser mucho mayor a MSS/ RTT.
- Cuando la conexión comienza, la velocidad se incrementa exponencialmente hasta el primer evento de pérdida.
- La ventana de congestión se incrementa al menos SMSS bytes por cada ACK nuevo recibido.

2. Evitación de la recuperación

- El valor de la ventana de congestión es aproximadamente igual a la mitad de su valor en el momento que se detectó congestión por última vez.
- El valor de VentCongestion incrementa en un MSS cada RTT, es decir, existe un crecimiento lineal.
- Luego de un tiempo de espera, VentCongestion vale 1 MSS. La ventana crece exponencialmente hasta un umbral, y luego crece linealmente.

3. Recuperación rápida

- *VentCongestion* se incrementa en 1 MSS por cada ACK duplicado recibido que corresponde al segmento que falta.
- Si llega un ACK para el segmento que falta, TCP pasa el estado de evitación de la congestión.
- Si se produce un fin de temporización, el mecanismo de recuperación rápida pasa al estado de arranque lento.

4. Retransmisión rápida

- Este método aprovecha la recepción de reconocimientos duplicados.
- Un ACK duplicado se puede dar por las siguientes situaciones:
 - Desorden de los paquetes en la red. TCP genera un ACK duplicado al recibir un segmento fuera de orden.
 - Pérdida de algún segmento de datos. TCP recibe segmentos fuera de orden y genera ACK duplicados.
- Por la producción de un pico de retardo en la red, esto quiere decir que el tiempo de ida y vuelta de un paquete se ha incrementado de forma repentina.
- La retransmisión rápida se activa al recibir el tercer ACK duplicado.



Actividades de aprendizaje recomendadas

Le invito a realizar las siguientes actividades con el propósito de reforzar los conocimientos de la temática abordada:

1. Revise el video [Control de congestión en TCP](#), tomado del sitio de la Universitat Politècnica de València, y realice un resumen de cada uno de los métodos de control de congestión.

Nota: por favor, complete la actividad en un cuaderno o documento Word.



2. Revise el video titulado [Tema 3 - TCP control de congestión](#) con el fin de mejorar la comprensión del algoritmo de control de congestión de TCP.

3. Desarrolle la autoevaluación que se presenta a continuación. Si su nota es baja, por favor, vuelva a leer y revisar los contenidos.



Autoevaluación 14

Dados los siguientes enunciados, seleccione la alternativa que corresponda a la respuesta correcta.

1. Cuando la ventana de congestión está debajo del valor umbral, el emisor está en la fase:

- a. Arranque lento.
- b. Evitación de la congestión.
- c. Recuperación rápida.
- d. Retransmisión rápida.

2. Cuando la ventana de congestión está sobre el valor umbral, el emisor está en la fase:

- a. Arranque lento.
- b. Evitación de la congestión.
- c. Recuperación rápida.
- d. Retransmisión rápida.

3. Cuando ocurre un triple ACK duplicado, el valor umbral es igual a:

- a. El valor de la ventana de congestión.
- b. Al doble del valor de la ventana de congestión.
- c. A la mitad del valor de la ventana de congestión.
- d. Ninguna de las anteriores.



4. Cuando expira el temporizador de retransmisión (*timeout*), el valor de la ventana de congestión es igual a:

- a. $\frac{1}{2}$ MSS.
- b. 1 MSS.
- c. 2 MSS.
- d. Ninguna de las anteriores.

5. En el método de control de congestión arranque lento, el valor de la ventana de congestión se dobla por cada RTT.

- a. Verdadero.
- b. Falso.

6. El número de ACK que puede recibir el receptor durante el tiempo de ida y vuelta es:

- a. Como mínimo el valor de la ventana de congestión.
- b. Como máximo, el valor de la ventana de congestión.
- c. Como mínimo el valor de la mitad de la ventana de congestión.
- d. Como máximo, el valor de la mitad de la ventana de congestión.

7. El valor del umbral inicial en Internet es de:

- a. 64 Kbytes.
- b. 128 Kbytes.
- c. 512 Kbytes.
- d. 1 Mbyte.

8. ¿En qué consiste el control de congestión terminal a terminal?

- a. Es el control final debido a las pérdidas de segmentos en el equipo terminal.
- b. Es el control de terminal cuando los segmentos finalmente se pierden.
- c. Es el control de congestión asistido por los enrutadores en una ruta definida para una comunicación.



- d. Al no proporcionar la capa de red soporte para el control de congestión, este proceso se lleva en la capa de transporte del emisor y el receptor.
9. La cantidad de datos que un emisor puede enviar no puede exceder el mínimo de entre la ventana de congestión y la ventana de recepción.
- Verdadero.
 - Falso.
10. Al establecerse la conexión TCP, el receptor propone un tamaño de ventana en función:
- Del buffer del receptor.
 - Del buffer del emisor.
 - Del tamaño de MSS.
 - Del tamaño del segmento.

[Ir al solucionario](#)



Resultados de aprendizaje 2 y 4:

- Diseñar y dimensionar escenarios de red.
- Describir las estrategias para garantizar la disponibilidad de acceso a la red en redes conmutadas y enrutadas.

Para alcanzar los resultados de aprendizaje, los estudiantes aprenderán a diseñar y construir múltiples redes interconectadas, identificando y aplicando protocolos de transferencia fiables y no fiables según las necesidades de la red. También adquirirán habilidades para diseñar escenarios de red, comprendiendo las diferencias entre los protocolos de transporte TCP y UDP y seleccionando el más adecuado para cada tipo de red. Finalmente, los estudiantes describirán estrategias para garantizar la disponibilidad de acceso en redes conmutadas y enrutadas, aprendiendo a identificar y analizar datagramas UDP mediante herramientas como Wireshark.

Contenidos, recursos y actividades de aprendizaje recomendadas



Semana 16

Actividades finales del bimestre

Repaso de unidades 8-12

En esta semana lo invitamos a revisar los contenidos estudiados en el segundo bimestre. Específicamente, deberá revisar las unidades 8 a la 12. Esta revisión le permitirá reforzar los conocimientos adquiridos, lo cual lo preparará para la evaluación bimestral.

También le recordamos que puede conectarse al *chat* de la tutoría para cualquier inquietud que tenga en el momento de revisar los contenidos del segundo bimestre. Además, no olvide repasar las autoevaluaciones y ejercicios planteados en las unidades antes mencionadas.



4. Solucionario

Autoevaluación 1

Pregunta	Respuesta	Retroalimentación
1	a	Los segmentos: un paquete IP contiene segmentos porque forma parte del proceso de encapsulación en el modelo OSI o TCP/IP. En este modelo, los segmentos pertenecen a la capa de transporte (por ejemplo, TCP o UDP), que se encarga de dividir los datos en partes más pequeñas y manejables para su envío a través de la red.
2	c	Un <i>router</i> es considerado un dispositivo de capa 3, que opera en la capa de red del modelo OSI (<i>Open Systems Interconnection</i>). La capa 3, o capa de red, es responsable del enrutamiento de paquetes de datos entre redes diferentes.
3	c	Un <i>host</i> debe enviar la información a su puerta de enlace predeterminada para comunicarse con un <i>host</i> remoto cuando este último se encuentra en una red diferente.
4	b	La longitud total del encabezado de un paquete IPv4 es de 20 bytes porque este tamaño es necesario para incluir la información mínima requerida para el enrutamiento y gestión de los paquetes a través de una red.
5	d	La longitud total del encabezado de un paquete IPv6 es de 40 bytes porque este tamaño es necesario para acomodar la información y las mejoras introducidas en el protocolo IPv6 en comparación con IPv4.
6	a	El campo TTL (<i>Time to Live</i>) en un datagrama IPv4 es un contador que se reduce en uno cada vez que el paquete pasa por un <i>router</i> para prevenir que los paquetes queden atrapados en bucles infinitos en la red.
7	d	El tamaño máximo de un paquete IP, incluido el encabezado y los datos, es comúnmente de 1500 bytes debido a la Unidad Máxima de Transmisión (MTU, por sus siglas en inglés) estándar para la mayoría de las redes Ethernet.
8	a	Una dirección MAC (<i>Media Access Control</i>), o dirección física, se compone de 48 bits porque este tamaño proporciona un espacio de direcciones lo suficientemente amplio para identificar de manera única cada dispositivo de red en el mundo.

Pregunta	Respuesta	Retroalimentación
9	b	Falso, la dirección MAC no se puede cambiar, ya que viene grabada en la NIC.
10	b	La PDU (<i>Protocol Data Unit</i>) de la capa de red es denominada "paquetes", porque en esta capa se agrupan y encapsulan los datos para su transmisión entre diferentes redes.

[Ir a la autoevaluación](#)



Autoevaluación 2

Pregunta	Respuesta	Retroalimentación
1	b	192.168.1.0/24, ya que todos los bits de host deben estar en 0 para ser dirección de red.
2	a	192.168.10.4/24, ya que la porción de host no está en 0.
3	b	192.168.10.255/24, todos los bits de la porción de host deben estar en 1.
4	c	255.255.255.0, el prefijo /24 indica que los 24 bits son para porción de red, es decir, los 3 primeros octetos deben estar en 1 en la máscara de subred.
5	b	192.168.10.255/24 es una dirección privada, ya que está en uno de los rangos asignados para ese tipo de dirección.
6	b	Una dirección IPv6, que tiene una longitud total de 128 bits, está estructurada en 8 grupos de 16 bits cada uno. Estos grupos de 16 bits se expresan en formato hexadecimal y son conocidos como hextetos.
7	a	La respuesta "2001:DCB::3/64" es correcta para identificar una dirección <i>unicast</i> global en IPv6 porque sigue la estructura de las direcciones <i>unicast</i> globales, que están destinadas a ser únicas en todo el ámbito de Internet.
8	b	Las direcciones IPv6 <i>link-local</i> están diseñadas para usarse únicamente dentro de una red local y no pueden ser enrutadas a través de redes públicas como <i>Internet</i> .
9	b	$64, /26 = 255.255.255.192$, Número mágico = $256-192 = 64$.
10	c	El Protocolo DHCP permite que los dispositivos en una red IPv4 obtengan automáticamente una dirección IP válida y otros parámetros de configuración, como máscara de subred y puerta de enlace, facilitando la administración de redes sin necesidad de configuraciones manuales.

[Ir a la autoevaluación](#)

Autoevaluación 3

Pregunta	Respuesta	Retroalimentación
1	b	La división con máscara fija no es eficiente porque todas las subredes tienen el mismo tamaño, lo que genera más desperdicio de direcciones comparado con VLSM.
2	b	Con VLSM (<i>Variable Length Subnet Mask</i>), las subredes pueden tener diferentes tamaños ajustados a sus necesidades, lo que reduce el desperdicio de direcciones y optimiza el uso del espacio IP.
3	c	Se deben usar 6 bits, $2^6 - 2 = 62$ hosts.
4	a	Se deben usar 4 bits, $2^4 = 16$ subredes.
5	a	La máscara de subred es: 255.255.255.240, el prefijo /28 indica 3 octetos + 4 bits, es decir, 255.255.255.11110000 = 255.255.255.240.
6	a	Hay 30 hosts: 224 = 11100000, 5 bits para porción de hosts. $2^5 - 2 = 30$ hosts.
7	c	La dirección es: 172.16.32.0. Número mágico = 256-240=16, 1. ^a subred 172.16.0.0/20, 2. ^a subred 172.16.16.0/20, 3. ^a subred 172.16.32.0/20.
8	a	La máscara de subred es 255.255.255.248, $2^3 - 2 = 6$ hosts, es decir, se requieren 3 bits para la porción de host, dejando 5 bits para la porción de red: 255.255.255.11111000.
9	b	El valor es 64, /26 = 255.255.255.192, Número mágico = 256-192 = 64.
10	a	La dirección es 176.16.48.255. Número mágico = 256-240 = 16, 1. ^a subred: 172.16.0.0/20, 2. ^a : 172.16.16.0/20, 3. ^a : 172.16.32.0/20, 4. ^a : 172.16.48.0/20; la dirección de broadcast será la última de esa red 172.16.63.255, ya que la siguiente red es 172.16.64.0/20.

[Ir a la autoevaluación](#)

Autoevaluación 4

Pregunta	Respuesta	Retroalimentación
1	a	La tabla de ruteo contiene las rutas y métricas necesarias para decidir la mejor ruta hacia el destino del paquete, facilitando el proceso de encaminamiento en la red.
2	a	El reenvío se refiere al proceso de mover paquetes de la interfaz de entrada a la interfaz de salida correcta dentro de un <i>router</i> .
3	b	El enrutamiento implica el cálculo y actualización de rutas, un proceso que es más lento y se realiza menos frecuentemente, mientras que el reenvío (<i>switching</i>) ocurre en nanosegundos para mantener la velocidad del tráfico.
4	b	El enrutamiento implica analizar métricas, como la distancia o el costo, para determinar la mejor ruta para enviar los paquetes a su destino.
5	b	El plano de datos se encarga de procesar y transferir los paquetes rápidamente entre interfaces, mientras que el plano de control gestiona la toma de decisiones y mantenimiento de rutas.
6	b	Las rutas remotas no están directamente conectadas al <i>router</i> , sino que se alcanzan mediante otros <i>routers</i> , por lo que requieren información de enrutamiento para llegar a su destino.
7	a	Una ruta con la dirección "0.0.0.0/0" es una ruta predeterminada en IPv4, lo que significa que todo el tráfico que no coincide con otra ruta se envía a través de esta.
8	a	Cuando no existe una ruta específica en la tabla de ruteo para la red de destino, el <i>router</i> utiliza la ruta predeterminada para enviar el paquete, dirigiéndolo hacia un <i>gateway</i> que puede conocer más rutas.
9	c	Si el <i>router</i> no encuentra la red de destino en su tabla de ruteo ni tiene una ruta predeterminada configurada, no sabe cómo encaminar el paquete, por lo que debe descartarlo para evitar pérdidas o errores en la red.
10	a	Serial 0/0/1, ya que la dirección de destino no está en la tabla de ruteo, se envía por la ruta predeterminada.

[Ir a la autoevaluación](#)

Autoevaluación 5

Pregunta	Respuesta	Retroalimentación
1	a	En un control por <i>router</i> , porque describe cómo funciona el enrutamiento en muchas redes. En un sistema de control por <i>router</i> , cada <i>router</i> en la red tiene la responsabilidad de ejecutar su propio protocolo de enrutamiento.
2	b	El control lógicamente centralizado generalmente se implementa mediante redes definidas por <i>software</i> (SDN), donde la inteligencia de red es separada del <i>hardware</i> y se centraliza en un controlador que gestiona la red de manera dinámica.
3	a	Algoritmo estado enlace. El algoritmo de enrutamiento centralizado también se refiere al algoritmo de estado enlace, que permite a los <i>routers</i> compartir información sobre la topología de la red, ayudando a calcular la mejor ruta para el tráfico.
4	c	Estado enlace. El algoritmo de Dijkstra es un algoritmo de enrutamiento que utiliza el enfoque de estado enlace. Calcula las rutas más cortas en un grafo ponderado y es ampliamente utilizado en protocolos de enrutamiento como OSPF.
5	b	Los protocolos dinámicos no requieren intervención humana para realizar cambios en la topología.
6	a	El control lógicamente centralizado permite una mejor gestión y optimización del tráfico de red, lo que puede ayudar a reducir la latencia y la carga del procesamiento en los dispositivos individuales al centralizar las decisiones de enrutamiento.
7	c	El algoritmo vector distancia no requiere que los <i>routers</i> conozcan toda la topología de la red; en cambio, solo necesita información sobre las rutas de sus vecinos y las distancias a esos destinos, lo que lo hace menos complejo que el algoritmo de estado enlace.
8	c	Todas las opciones, en el algoritmo estado enlace o Dijkstra los nodos deben conocer toda la topología.
9	c	El algoritmo vector distancia es comúnmente conocido como el algoritmo Bellman-Ford, que se utiliza para calcular las rutas más cortas en redes donde los enlaces pueden tener pesos negativos.
10	c	En el algoritmo de vector distancia, los nodos intercambian sus tablas repetidamente hasta que toda la red tiene la misma información y ya no hay cambios, logrando así la convergencia.

[Ir a la autoevaluación](#)

Autoevaluación 6

Pregunta	Respuesta	Retroalimentación
1	c	RIP significa <i>Routing Information Protocol</i> , que es un protocolo de enrutamiento utilizado para determinar la mejor ruta en una red basada en el número de saltos.
2	b	RIP utiliza el algoritmo de vector distancia.
3	b	La versión RIP V2 es la que soporta VLSM (<i>Variable Length Subnet Masking</i>), permitiendo el uso de subredes de diferentes tamaños dentro de la misma red.
4	b	En el protocolo RIP, el número máximo de saltos permitido es de 15. Un valor de 16 saltos se considera "infinito", lo que indica que la red es inalcanzable.
5	c	Las actualizaciones de rutas en RIP se envían cada 30 segundos, lo que permite a los <i>routers</i> intercambiar información sobre las rutas disponibles y sus métricas.
6	d	En RIP, cada ruta en la tabla de enrutamiento tiene un tiempo de vida o "timeout" de 180 segundos. Esto significa que si un <i>router</i> no recibe actualizaciones sobre una ruta específica dentro de ese período de 180 segundos, la ruta se considera inactiva o inválida y se marca para ser eliminada de la tabla de enrutamiento.
7	c	La distancia administrativa de RIP es 120. Este valor determina la confiabilidad de la ruta; a menor valor, mayor confiabilidad.
8	b	En RIP, la ruta escogida es la que tiene el menor número de saltos. El protocolo utiliza esta métrica para determinar la mejor ruta hacia un destino.
9	a	El concepto de horizonte partido en RIP implica que un <i>router</i> no debe anunciar rutas a través de la misma interfaz por la que las recibió, ayudando a evitar bucles de enrutamiento.
10	b	Una ruta estática tiene mayor prioridad que una ruta aprendida por RIP, ya que se configura manualmente y el router la usa antes que las rutas dinámicas.

[Ir a la autoevaluación](#)

Autoevaluación 7

Pregunta	Respuesta	Retroalimentación
1	c	OSPF (<i>Open Shortest Path First</i>) es un Protocolo de Gateway Interno (IGP) diseñado para operar dentro de un Sistema Autónomo (AS). Un AS es un grupo de redes y routers bajo un control administrativo común, y OSPF permite a los routers intercambiar información de enrutamiento dentro del AS.
2	a	Open Shortest Path First, un protocolo de enrutamiento basado en el algoritmo de estado de enlace que utiliza la métrica de menor costo para determinar la ruta más eficiente hacia el destino.
3	b	OSPF utiliza el algoritmo de estado de enlace (<i>Link-State</i>), que construye una base de datos completa de la topología de red y calcula la ruta más corta utilizando el algoritmo de Dijkstra. Esto es diferente de los algoritmos de vector de distancia que solo conocen la mejor ruta hacia los destinos, pero no la topología completa.
4	a	La base de datos de adyacencia en OSPF contiene información sobre los routers vecinos que han establecido una conexión OSPF. Esto es esencial para garantizar que los routers mantengan una relación activa y puedan intercambiar información de enrutamiento.
5	b	La base de datos de estado de enlace (<i>Link-State Database, LSDB</i>) en OSPF representa la topología de toda la red, es decir, contiene información sobre todos los routers y enlaces en la red, lo que permite calcular las rutas óptimas mediante el algoritmo de Dijkstra.
6	a	Los paquetes Hello de OSPF son utilizados para descubrir y mantener la relación con los routers vecinos. Estos paquetes se envían periódicamente para verificar que los vecinos estén activos y mantener la adyacencia entre routers.
7	d	El paquete LSR (<i>Link-State Request</i>) en OSPF se utiliza para solicitar información específica de la base de datos de estado de enlace (LSDB) de otros routers cuando se detectan discrepancias en los datos de enrutamiento.
8	a	El Estado Up no es un estado operativo en OSPF. Los estados de OSPF incluyen <i>Init</i> (inicialización), <i>Exstart</i> (preparación para el intercambio de información) y <i>Exchange</i> (intercambio de información de la base de datos de estado de enlace).
9	c	En OSPF, el área <i>backbone</i> se denomina Área 0. Todos las demás áreas deben conectarse directa o indirectamente al Área 0, que actúa como el núcleo de la topología de OSPF.



Pregunta Respuesta Retroalimentación

10

d

Un *Autonomous System Border Router* (ASBR) es un *router OSPF* que conecta un Sistema Autónomo a otros sistemas autónomos. El ASBR es responsable de intercambiar información de enrutamiento entre el Sistema Autónomo y redes externas.

[Ir a la autoevaluación](#)



Autoevaluación 8

Pregunta	Respuesta	Retroalimentación
1	a,b	Las principales características de la capa de transporte son la de establecer una sesión de comunicación entre dos aplicaciones. Además, se encarga de enlazar la capa de aplicación con las capas inferiores.
2	c	Para el transporte de datos existen dos protocolos. El protocolo orientado a la conexión TCP y el protocolo no orientado a la conexión UDP.
3	a	Los puertos bien conocidos son números que se reservan para servicios y aplicaciones.
4	b	Para crear un socket se necesita conocer la dirección IP y el puerto destino (no el puerto de origen).
5	c	Un número de puerto (ya sea de origen o destino, TCP o UDP), tiene una longitud de 16 bits.
6	b	Cada aplicación tiene un número de puerto que lo identifica, en el caso de FTP es el 21.
7	a	En la capa de transporte se manejan segmentos.
8	b	Los sockets identifican de manera exclusiva un proceso. Un socket es la combinación del número de puerto de la capa de transporte y de la dirección IP de la capa de red.
9	a	Esto es posible, ya que TCP proporciona al nivel de aplicación un servicio <i>full-dúplex</i> . Lo que quiere decir que los datos pueden circular en cada sentido de forma independiente.
10	c	Esto es necesario, ya que cada octeto que se intercambia es numerado.

[Ir a la autoevaluación](#)

Autoevaluación 9

Pregunta	Respuesta	Retroalimentación
1	b	DNS utiliza UDP cuando los clientes envían solicitudes a un servidor DNS.
2	c	Los puertos efímeros son puertos de corta duración. Por lo general son asignados de forma dinámica a las aplicaciones cliente cuando el cliente inicia una conexión a un servicio.
3	b	En este documento se describe de forma técnica el protocolo UDP. RFC 768 es un documento de la IETF (<i>Internet Engineering Task Force</i>).
4	b	UDP es un protocolo de la capa de transporte no fiable.
5	c	Recuerde que el tamaño del campo es de 16 <i>bits</i> , lo cual equivale a 2 <i>bytes</i> .
6	a	Esta pérdida de paquetes se debe a que las colas de los <i>routers</i> están llenas.
7	a	DHCP tiene asignado el puerto 68 cuando trabaja con el protocolo UDP.
8	b	La baja sobrecarga que ofrece el UDP se debe a que es un protocolo no orientado a la conexión. Además, no cuenta con mecanismos de retransmisión, secuenciación y control de flujo.
9	d	Estos valores representan el número máximo de <i>bytes</i> asignados para el campo de datos de usuario de datagrama UDP. Es importante indicar que, por lo general, las aplicaciones permiten cantidades menores a estos valores.
10	b, d	Ya que el UDP utiliza el protocolo IP, proporciona el mismo sistema de envío no fiable. Por lo tanto, los mensajes UDP pueden perderse, duplicarse o llegar fuera de orden.

[Ir a la autoevaluación](#)

Autoevaluación 10

Pregunta	Respuesta	Retroalimentación
1	d	Si el puerto asociado al datagrama no se encuentra, se envía un mensaje de error ICMP, el cual significa que el puerto es no alcanzable y, por lo tanto, se descarta el datagrama.
2	a	Si se encuentra el número de puerto de destino, el datagrama es encolado en dicho puerto donde el programa de aplicación puede acceder a él.
3	c	Si se encuentra el número de puerto de destino, el datagrama es encolado en dicho puerto donde el programa de aplicación puede acceder a él. Si el puerto se encuentra lleno, el datagrama será descartado.
4	a	Cuando un programa de aplicación negocia con el sistema operativo el uso de un determinado número de puerto, el sistema operativo crea una cola interna para almacenar los mensajes que llegan.
5	b	Este es el máximo tamaño que se puede asignar para los Sockets Stream. Son los más utilizados, hacen uso del protocolo TCP, el cual nos provee un flujo de datos bidireccional, secuenciado, sin duplicación de paquetes y libre de errores.
6	a	Este es el tamaño máximo de los Sockets Datagram. Los cuales hacen uso del protocolo UDP, el cual nos provee un flujo de datos bidireccional, pero los paquetes pueden llegar fuera de secuencia, pueden no llegar a contener errores. Se llaman también sockets sin conexión, porque no hay que mantener una conexión activa, como en el caso de sockets stream. Son utilizados para transferencia de información paquete por paquete.
7	d	En UDP, el tamaño máximo teórico de un datagrama es de 65,535 bytes (\approx 64 kB), que incluye la cabecera de 8 bytes y los datos. En la práctica, el tamaño real suele ser menor debido a limitaciones de la red subyacente.
8	c	La cabecera UDP contiene toda la información necesaria para la transmisión de datos utilizando el protocolo de transporte. La cabecera se compone de 4 campos y está dividida en 2 bloques de 32 bits.
9	b	Solo TCP puede corregir errores mediante retransmisiones y control de flujo. UDP solo detecta errores con checksum, pero no los corrige.



Pregunta Respuesta Retroalimentación

10

a

Tanto TCP como UDP incluyen mecanismos para detectar errores en los datos mediante sumas de verificación (*checksums*), aunque solo TCP garantiza la corrección y retransmisión de datos.

[Ir a la autoevaluación](#)



Autoevaluación 11

Pregunta	Respuesta	Retroalimentación
1	d	La suma de comprobación permite comprobar que el datagrama llega a su destino sin haber sufrido ninguna alteración.
2	d	Este número de secuencia permite que las funciones de la capa de transporte reensamblen los segmentos en el mismo orden en el que fueron transmitidos.
3	a	Los paquetes se deben guardar en <i>buffers</i> según sea necesario, para entregarlos en orden a la capa superior.
4	b	Las cabeceras tienen por defecto una longitud fija.
5	d	Son los eventos que se dan del lado del emisor cuando se usa el protocolo GBN (Go-Back-N).
6	a	La fiabilidad se refiere a la no pérdida, no alteración y/o no duplicación de datos.
7	b	Mediante el pipeline, el emisor permite el envío de múltiples paquetes a ser reconocidos.
8	a	Este tipo de protocolos son necesarios para proporcionar una comunicación fiable en presencia de paquetes perdidos o dañados.
9	b	Esto se debe a que TCP ofrece una conexión <i>full-dúplex</i> .
10	a	El número de secuencia a nivel de transporte emplea rangos muy grandes. TCP asigna un número de secuencia a cada octeto transmitido entre dos aplicaciones en un sentido. Este número de secuencia es un número de 32 bits sin signo que vuelve a 0 después de alcanzar el valor $2^{32} - 1$.

[Ir a la autoevaluación](#)

Autoevaluación 12

Pregunta	Respuesta	Retroalimentación
1	d	En realidad, la cabecera TCP está limitada a 60 octetos, sin embargo, su tamaño habitual es de 20 octetos, lo que equivale a 160 bits.
2	b	El campo de ventana de recepción es de 16 bits y sí se utiliza para el control de flujo.
3	a, b	Número de secuencia identifica a cada segmento y número de reconocimiento identifica la posición del segmento en la información enviada. El campo número de secuencia identifica la posición que ocupa el primer octeto de datos de cada segmento en la secuencia de datos correspondiente a una conexión. El campo número de reconocimiento contiene el número de secuencia del siguiente octeto que el emisor de un reconocimiento espera recibir.
4	b	TCP proporciona un servicio de transmisión fiable, considerando toda la información intercambiada durante una conexión como un flujo continuo de bytes. ACK es un campo significativo de acuse de recibo.
5	b, c, d	RST: Aborta una conexión, por motivos diversos. SYN: Solicita la conexión. FIN: Finaliza la conexión. Por otro lado, el campo CWR es utilizado para optimizar el flujo en caso de congestión.
6	c, d	PSH de TCP proporciona dos cosas: <ul style="list-style-type: none">• La aplicación remitente informa a TCP que los datos tienen que enviarse inmediatamente.• Informa al receptor de que los datos deben de ser pasados inmediatamente a la aplicación destino.
		El campo URG es utilizado para informar al extremo receptor de que ciertos datos dentro de un segmento son urgentes y deberían ser priorizados. Este campo no se emplea mucho en los protocolos modernos.
7	a	Los valores de RTT varían en cada instante; por lo tanto, según la especificación TCP original, se emplea una estimación del tiempo de retorno.
8	b	Es el tamaño más grande de datos, se especifica en bytes.
9	a	Recuerde que el tamaño de la ventana es un campo en el encabezado TCP que permite la administración de datos perdidos y el control del flujo.

10

d

El campo de opciones TCP permite añadir campos a la cabecera con el fin de realizar las siguientes operaciones:

- Monitorear los retrasos que experimentan los segmentos desde el origen hasta el destino.
- Aumentar el tamaño de la ventana.
- Indicar el Tamaño Máximo del Segmento (MSS) que el origen está preparado para recibir.

[Ir a la autoevaluación](#)



Autoevaluación 13

Pregunta	Respuesta	Retroalimentación
1	d	El campo de número de reconocimiento tiene una longitud de 16 bits y limita el tamaño de la ventana a 65535 octetos. Sin embargo, este valor puede variar con ayuda de la opción de factor de escala de ventana que permite extender el tamaño de la ventana más allá del límite.
2	a	La opción de factor de escala de ventana permite extender el tamaño de la ventana más allá del límite.
3	a	Con el fin de poder detectar cualquier modificación de los datos durante su transmisión, TCP calcula un <i>Checksum</i> que incluye en la cabecera y que verifica la integridad del segmento.
4	b	En donde NSI corresponde al Número de Secuencia Inicial. NSI corresponde al número de secuencia del primer octeto de datos enviado por el nodo.
5	b	El segmento SYN consume un número de secuencia porque se considera un byte en la secuencia, y durante el establecimiento de conexión, el SYN ocupa espacio en la numeración de secuencia, por lo que efectivamente consume dos números de secuencia en el proceso de <i>handshake</i> TCP.
6	a	Ya que en la conexión simétrica, cada host corta la conexión únicamente en el sentido que emite datos.
7	a	Esto es verdadero, ya que cuando un host ha enviado la TPDU de desconexión ya no acepta más datos; mientras tanto, el otro host podría haber enviado una TPDU de datos que no será aceptada.
8	a	De forma análoga al proceso de conexión, supone el intercambio de 3 mensajes, por lo que también se denomina saludo a tres vías; no existe forma fiable de terminar la conexión en menos mensajes sin correr el riesgo de perder datos.
9	a	Petición de sincronismo de números de secuencia para iniciar la conexión.
10	c	El control de flujo en el nivel de transporte es fundamental, ya que la velocidad con que los datos llegan al receptor puede ser muy variable al intervenir multitud de factores.

[Ir a la autoevaluación](#)

Autoevaluación 14

Pregunta	Respuesta	Retroalimentación
1	a	Por lo tanto, cuando la ventana de congestión alcanza un determinado umbral, la fase de arranque lento finaliza.
2	b	Por lo tanto, cuando la ventana de congestión alcanza el tamaño de la ventana de recepción, la fase de evitación de la congestión finaliza.
3	c	El recibir un triple ACK duplicado significa un evento de pérdida. Esto hace que TCP reduzca la ventana de congestión.
4	b	Luego la ventana crecerá exponencialmente hasta cierto umbral, luego de esto crecerá linealmente.
5	a	Esto indica que el procedimiento no es demasiado lento.
6	b	Cabe considerar que el incremento máximo en el tamaño de la ventana durante un RTT será de un segmento.
7	a	Se usa arranque lento hasta llegar al valor umbral. A partir de ahí, se incrementa linealmente la ventana de congestión.
8	d	En el control de congestión terminal a terminal, la capa de red sí proporciona soporte explícito a la capa de transporte para propósitos de control de congestión.
9	a	El número máximo de bytes que puede enviar el emisor es el mínimo de ambos tamaños de ventana.
10	a	Ya que Internet acepta el problema que existe en la capacidad del receptor.

[Ir a la autoevaluación](#)





5. Referencias bibliográficas

CISCO. (2019a). CCNA 1: *Introduction to networks v6.0.*

CISCO. (2019b). CCNA 2: *Routing and Switching Essentials V6.0.*

CISCO. (2019c). CCNA 3: *Scaling Networks v6.0.*

CISCO. (2004). CCNA 2: Intermediate TCP/IP v3.1.

Kurose, & Ross. (2017). REDES DE COMPUTADORAS : un enfoque descendente. In PEARSON Educación (7.^a ed.). Pearson.

Kurose, & Ross. (2007). REDES DE COMPUTADORAS. Un enfoque descendente. In PEARSON Educación (4.^a ed.). Pearson.

Salcedo, O., Hernández, C., & Manta, H. (2010). Análisis y evaluación del routing information protocol RIP. In *Tecnura* (Vol. 14, pp.89–108). scielo.

Sánchez Rubio, M., Barchino Plata, R. & Martínez Herráiz, J. J. (2020). Redes de computadoras. Editorial Universidad de Alcalá. <https://elibro.net/es/lc/bibliotecaupl/titulos/131606>