



UTPL
La Universidad Católica de Loja

Modalidad Abierta y a Distancia



Redes de dispositivos

Guía didáctica

Índice

Primer
bimestre

Segundo
bimestre

Solucionario

Referencias
bibliográficas



Departamento de Ciencias de la Computación y Electrónica

Sección departamental de Electrónica y Telecomunicaciones

Redes de dispositivos

Guía didáctica

Autores:

Rohoden Jaramillo Katty Alexandra
Martínez Curipoma Javier Francisco



Asesoría virtual
www.utpl.edu.ec

Índice

Primer bimestre

Segundo bimestre

Solucionario

Referencias bibliográficas

Índice

Primer bimestre

Segundo bimestre

Solucionario

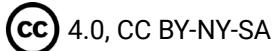
Referencias bibliográficas

Redes de dispositivos

Guía didáctica

Rohoden Jaramillo Katty Alexandra
Martínez Curipoma Javier Francisco

Universidad Técnica Particular de Loja



Diagramación y diseño digital:

Ediloja Cía. Ltda.

Telefax: 593-7-2611418.

San Cayetano Alto s/n.

www.ediloja.com.ec

edilojainfo@ediloja.com.ec

Loja-Ecuador

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



La versión digital ha sido acreditada bajo la licencia Creative Commons 4.0, CC BY-NY-SA: Reconocimiento-No comercial-Compartir igual; la cual permite: copiar, distribuir y comunicar públicamente la obra, mientras se reconozca la autoría original, no se utilice con fines comerciales y se permiten obras derivadas, siempre que mantenga la misma licencia al ser divulgada. <https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>

21 de octubre, 2020

Índice

Índice

1. Datos de información.....	11
1.1. Presentación de la asignatura	11
1.2. Competencias genéricas de la UTPL	11
1.3. Competencias específicas de la carrera.....	11
1.4. Problemática que aborda la asignatura	12
2. Metodología de aprendizaje.....	12
3. Orientaciones didácticas por resultados de aprendizaje.....	13
Primer bimestre	13
Resultado de aprendizaje 1	13
Contenidos, recursos y actividades de aprendizaje	13
Semana 1	14
Unidad 1. Generalidades capa de red	15
1.1. Procesos y dispositivos de la capa de red.....	15
Actividades de aprendizaje recomendadas	20
Actividades de aprendizaje recomendadas	22
Actividades de aprendizaje recomendadas	23
Actividades de aprendizaje recomendadas	28
1.2. Protocolos de la capa de red	29
1.3. Datagrama IPv4	30
Actividades de aprendizaje recomendadas	31
1.4. Datagrama IPv6	32
Actividades de aprendizaje recomendadas	33
1.5. Dispositivos de red	33
Actividades de aprendizaje recomendadas	38
Autoevaluación 1	39
Resultado de aprendizaje 2	42

Primer
bimestre

Segundo
bimestre

Solucionario

Referencias
bibliográficas

Contenidos, recursos y actividades de aprendizaje	42
Semana 2	42
 Unidad 2. Direccionamiento de capa de red	42
2.1. Direccionamiento IPv4	43
Actividades de aprendizaje recomendadas	51
2.2. Direccionamiento IPv6	51
Actividades de aprendizaje recomendadas	60
Autoevaluación 2	61
Resultado de aprendizaje 3	64
Contenidos, recursos y actividades de aprendizaje	64
 Semana 3	64
 Unidad 3. Subredes	64
3.1. División en Subredes.....	65
Actividades de aprendizaje recomendadas	69
Actividades de aprendizaje recomendadas	73
Autoevaluación 3	75
Resultado de aprendizaje 4	78
Contenidos, recursos y actividades de aprendizaje	78
 Semana 4	78
 Unidad 4. Generalidades de protocolos de enrutamiento	78
4.1. Reenvío y enrutamiento.....	79
Actividades de aprendizaje recomendadas	79
Actividades de aprendizaje recomendadas	83
4.2. Funcionamiento de un router.....	84
Actividades de aprendizaje recomendadas	86
4.3. Enrutamiento estático.....	87

Actividades de aprendizaje recomendadas	89
Autoevaluación 4	90
Resultado de aprendizaje 5	93
Contenidos, recursos y actividades de aprendizaje	93
Semana 5	93
Unidad 5. Algoritmos de enrutamiento.....	93
5.1. Introducción.....	94
5.2. Algoritmos de enrutamiento	95
Actividades de aprendizaje recomendadas	96
Actividades de aprendizaje recomendadas	100
Actividades de aprendizaje recomendadas	101
Autoevaluación 5	103
Resultado de aprendizaje 6	106
Contenidos, recursos y actividades de aprendizaje	106
Semana 6	106
Unidad 6. Protocolos de enrutamiento dinámico RIP.....	106
6.1. Protocolo RIP.....	107
Actividades de aprendizaje recomendadas	110
Actividades de aprendizaje recomendadas	113
Actividades de aprendizaje recomendadas	114
Actividades de aprendizaje recomendadas	115
Autoevaluación 6	116
Resultado de aprendizaje 7	119
Contenidos, recursos y actividades de aprendizaje	119

Índice

Primer
bimestre

Segundo
bimestre

Solucionario

Referencias
bibliográficas

Semana 7	119
 Unidad 7. Protocolos de enrutamiento dinámico OSPF	119
7.1. Protocolo OSPF	120
Actividades de aprendizaje recomendadas	121
Actividades de aprendizaje recomendadas	133
Autoevaluación 7	134
Actividades finales del bimestre.....	137
Semana 8	137
Segundo bimestre	138
Resultado de aprendizaje 8	138
Contenidos, recursos y actividades de aprendizaje	138
Semana 9	139
 Unidad 8. Servicios de la capa de transporte	139
8.1. Conexión entre capa de red y capa de transporte.....	139
Actividades de aprendizaje recomendadas	140
8.2. La capa de transporte en Internet	141
8.3. Multiplexación y demultiplexación.....	142
Actividades de aprendizaje recomendadas	143
Actividades de aprendizaje recomendadas	143
Actividades de aprendizaje recomendadas	145
Autoevaluación 8	146
Resultado de aprendizaje 9	149
Contenidos, recursos y actividades de aprendizaje	149

Unidad 9. Transporte sin conexión - UDP	150
9.1. Características de UDP	150
9.2. Estructura de un segmento UDP	151
Actividades de aprendizaje recomendadas	153
9.3. Proceso de comunicación en UDP	154
Autoevaluación 9	156
Resultado de aprendizaje 10	158
Contenidos, recursos y actividades de aprendizaje	158
Unidad 10. Principios de un servicio de transferencia de datos fiable	166
10.1. Construcción de un protocolo de transferencia de datos fiable.....	166
Actividades de aprendizaje recomendadas	170
10.2. Protocolo de transferencia de datos fiable con procesamiento en cadena	170
10.3. Retroceder N (GBN).....	173
Actividades de aprendizaje recomendadas	174
10.4. Repetición selectiva (SR)	175

Actividades de aprendizaje recomendadas	175
Actividades de aprendizaje recomendadas	176
Autoevaluación 11	178
Resultado de aprendizaje 12	181
Contenidos, recursos y actividades de aprendizaje	181
Semana 13	182
Unidad 11. Transporte orientado a la conexión – TCP.....	182
11.1.Características de TCP.....	182
11.2.La conexión TCP	183
Actividades de aprendizaje recomendadas	184
11.3.Estructura del segmento TCP	185
Actividades de aprendizaje recomendadas	185
11.4.Temporización	186
Actividades de aprendizaje recomendadas	188
11.5.Transferencia de datos fiable	188
Actividades de aprendizaje recomendadas	189
Autoevaluación 12	190
Resultado de aprendizaje 13.....	193
Contenidos, recursos y actividades de aprendizaje	193
Semana 14	193
11.6.Control de flujo	193
Actividades de aprendizaje recomendadas	195
11.7.Gestión de conexión TCP	196
Autoevaluación 13	198
Resultado de aprendizaje 2	201
Contenidos, recursos y actividades de aprendizaje	201
Semana 15	202

Unidad 12. Control de congestión	202
12.1.Introducción a la congestión	202
12.2.Métodos para controlar la congestión	203
Actividades de aprendizaje recomendadas	204
12.3.Mecanismo de control de congestión de TCP.....	204
Actividades de aprendizaje recomendadas	208
Autoevaluación 14	209
Actividades finales del bimestre.....	212
Semana 16	212
4. Solucionario	213
5. Referencias bibliográficas	234

Índice

Primer
bimestre

Segundo
bimestre

Solucionario

Referencias
bibliográficas

Índice

Primer bimestre

Segundo bimestre

Solucionario

Referencias bibliográficas



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.

Índice

Primer
bimestre

Segundo
bimestre

Solucionario

Referencias
bibliográficas

1.4. Problemática que aborda la asignatura

La asignatura aborda los aspectos básicos sobre la trasmisión 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, libro básico, páginas web, artículos científicos, videos tutoriales, que a su vez le permitirán resolver los problemas que se plantean en la asignatura.

Índice

Primer bimestre

Segundo bimestre

Solucionario

Referencias bibliográficas



3. Orientaciones didácticas por resultados de aprendizaje



Primer bimestre

Resultado de aprendizaje 1

Diseña y construye múltiples redes y las conecta entre sí.

Contenidos, recursos y actividades de aprendizaje

A través de este resultado de aprendizaje, usted identificará los conceptos básicos sobre la capa de red, aprenderá como está estructurada la información y como se direcciona la misma a lo largo de la red, esto se deberá lograr realizando lecturas del libro básico, de la guía didáctica además de recursos complementarios como videos y actividades interactivas.

Estimado estudiante es obligatorio antes de comenzar que usted realice las siguientes actividades:

Índice

Primer bimestre

Segundo bimestre

Solucionario

Referencias bibliográficas



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. Se debe seguir el curso y aprobarlo, para que adquiera la habilidad necesaria para elaborar las tareas.



Le invitamos a revisar el vídeo de [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!



Semana 1



Unidad 1. Generalidades capa de red

Estimado estudiante 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). 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 permite establecer funciones de manera estructurada a los diferentes dispositivos y aplicaciones de la red. Para lo cual recordemos los modelos de referencia de siete capas y cinco capas como son ISO y TCP/IP respectivamente (ver Figura 1).

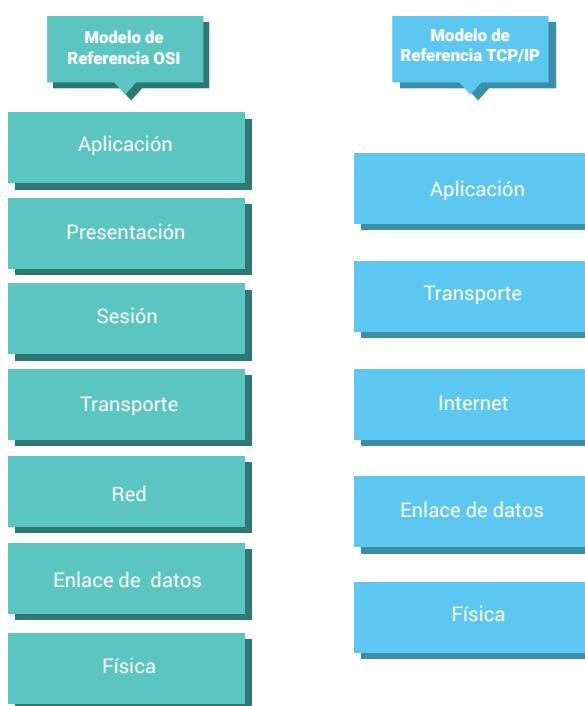


Figura 1. Comparación entre modelos de referencia de 7 capas (OSI) y 5 capas (TCP/IP)

Esta asignatura se enfocará en la revisión de las funciones y dispositivos en la capa 3 de ambos modelos que son equivalentes, como son las capas de red o Internet. 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 una 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 PDUs 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.

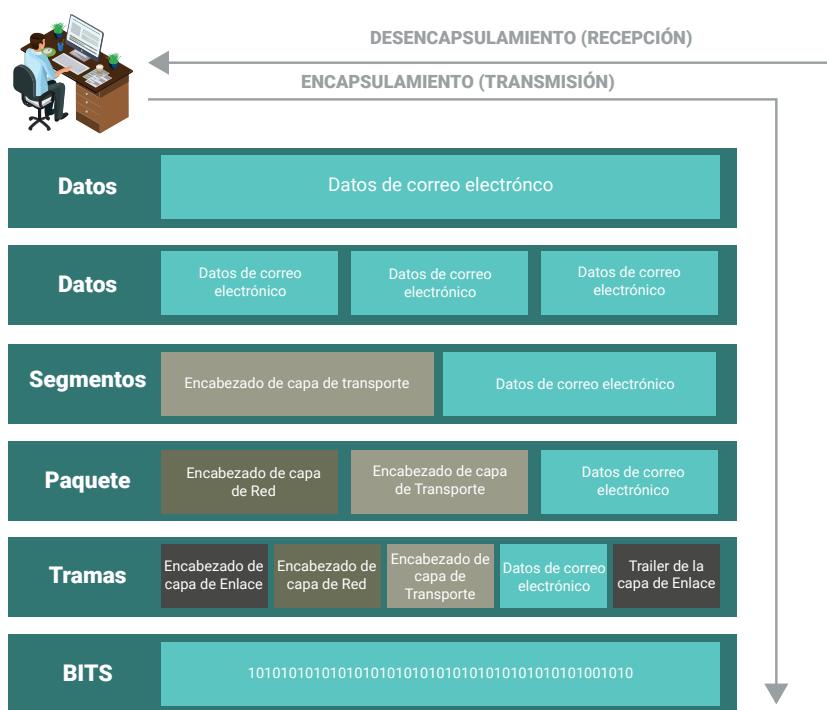


Figura 2. Procesos de encapsulamiento y desencapsulamiento de los datos en las diferentes capas

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

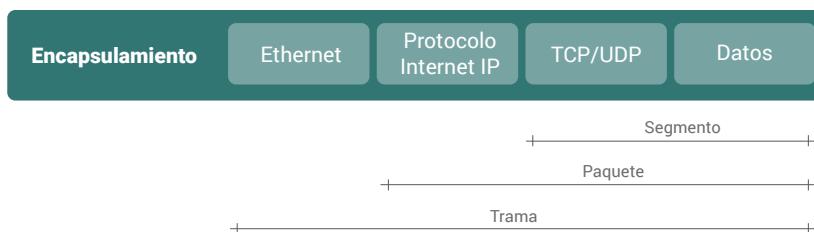


Figura 3. Estructura del encapsulamiento de protocolos de acuerdo a la PDU

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.

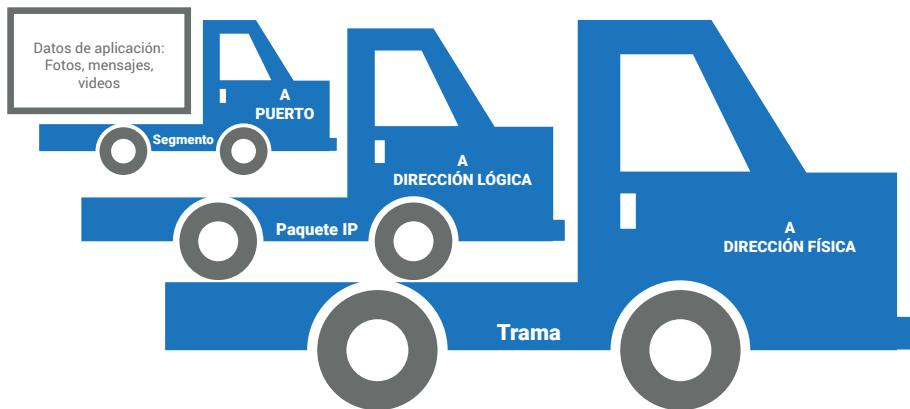


Figura 4. Analogía del encapsulamiento en redes de datos

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



Figura 5. Proceso de desencapsulamiento realizado para obtención de datos



Actividades de aprendizaje recomendadas

Estimado estudiante es muy importante complementar su lectura revisando el vídeo del canal de Youtube, Mastering IT, [Proceso de Encapsulamiento de Datos en Modelo OSI y TCP/IP](#), aquí podrá comprender de mejor manera el proceso de encapsulamiento en las redes de telecomunicaciones.

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.

1.1.2. Direccionamiento 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

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 commutación 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).

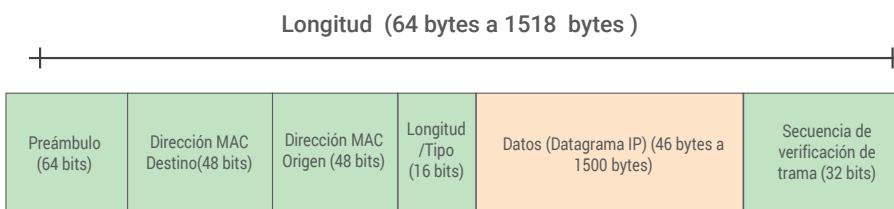


Figura 7. Formato de trama Ethernet IEEE 802.3

Toda trama que tenga 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.



Actividades de aprendizaje recomendadas

Estimado estudiante es muy importante que comprenda la función de cada uno de los campos de la trama Ethernet revisando el punto 6.4.2 del texto básico, y adicionalmente en la actividad interactiva [trama Ethernet](#), donde se muestra de manera didáctica la función de cada uno de estos campos.

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

Índice

Primer bimestre

Segundo bimestre

Solucionario

Referencias bibliográficas



Actividades de aprendizaje recomendadas

Estimado estudiante es importante complementar la teoría con la práctica, por lo que vamos a realizar una actividad, donde 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:

1. Estando en el escritorio de Windows, presionar las teclas + .
2. Escribimos en el cuadro de dialogo el comando: cmd y presionamos la tecla enter .
3. Se abrirá la consola de Windows, donde ingresaremos el comando: ipconfig /all y presionamos la tecla enter .

4. 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 8.

```
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
```

Figura 8. Ejemplo de información desplegada por el comando ipconfig /all de Windows.

5. 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.

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 realiza 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 9 donde se muestra el mapa vial, existen varias opciones para llegar al destino, los criterios que se utiliza 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.

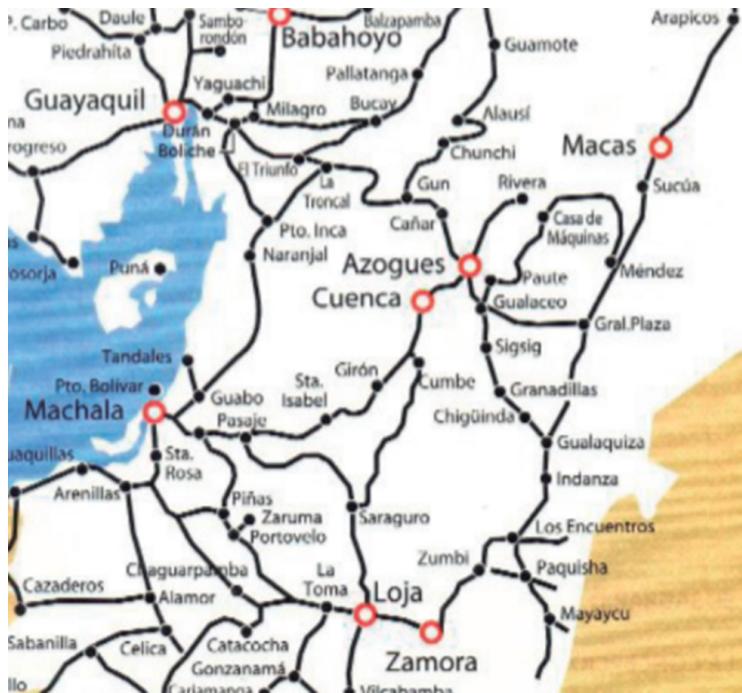


Figura 9. Las rutas posibles de conexión entre Loja y Guayaquil

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 ruteadores que usan las direcciones IP para la toma de decisiones y elección de la mejor ruta.

En la Figura 10 se puede observar una red de dispositivos, con varios enrutadores o routers 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.

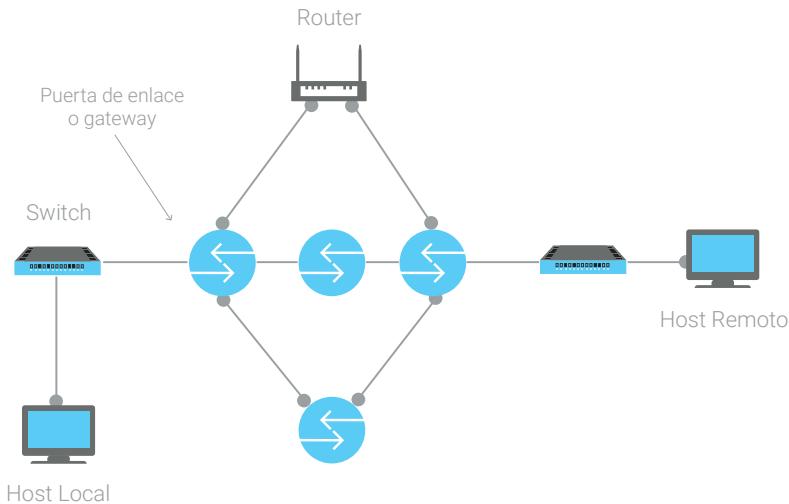


Figura 10. Ejemplo de red para comunicación remota entre host local y host remoto

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 11, donde se muestra un ejemplo básico de una red doméstica conectada al Internet.

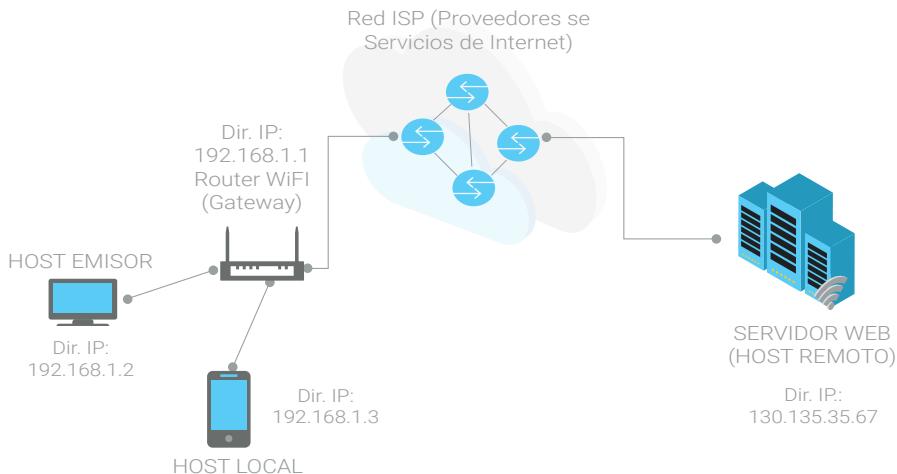


Figura 11. Ejemplo de red doméstica conectada a Internet

Veamos cómo se realiza el proceso de enruteamiento 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 ISPs, 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).



Actividades de aprendizaje recomendadas

Estimado estudiante, ahora vamos a realizar una actividad para 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:

1. Estando en el escritorio de Windows, presionar las teclas + .
2. Escribimos en el cuadro de dialogo el comando: cmd y presionamos la tecla Enter .

3. Se abrirá la consola de Windows, donde ingresaremos el comando: ipconfig y presionamos la tecla enter .
4. 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 12.

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
```

Figura 12. Ejemplo de información desplegada por el comando ipconfig, donde se puede observar la puerta de enlace o gateway.

5. 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.

Ahora veamos más a detalle los protocolos de capa de red como es el caso del Protocolo de Internet IP.

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.

Ahora revisaremos el formato de los datagramas IP en las versiones 4 y 6.

1.3. Datagrama IPv4

El datagrama IP o paquete permite establecer como 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 13), 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.

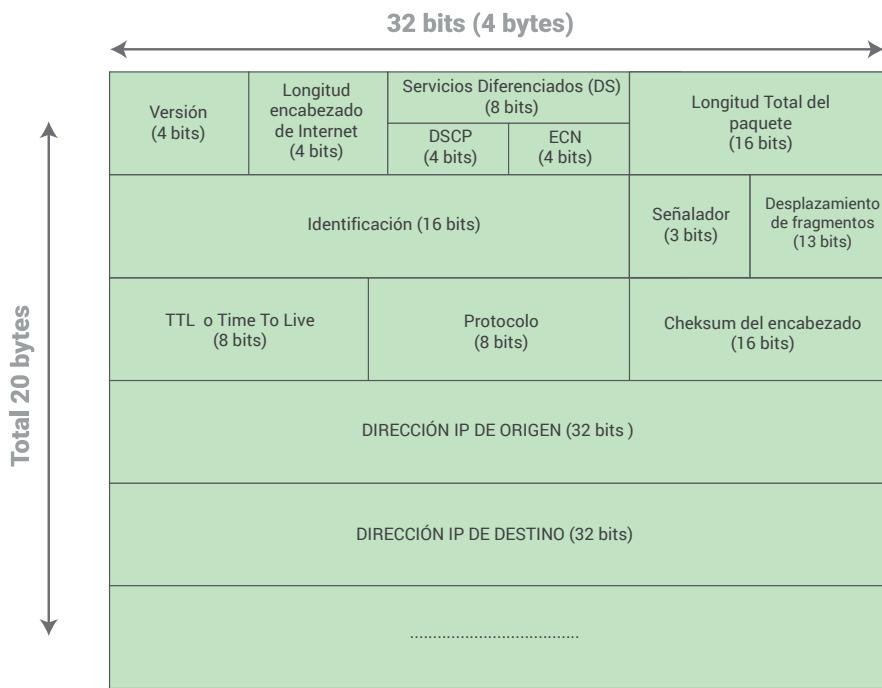


Figura 13. Formato del encabezado de un datagrama IPv4

Si observamos la Figura 13 las direcciones IPv4 de origen y destino tienen 32 bits de longitud.



Actividades de aprendizaje recomendadas

Estimado estudiante es muy importante que comprenda la función de cada uno de estos campos revisando el punto 4.3.1 del texto básico, y adicionalmente en la actividad interactiva [encabezado de datagrama IPv4](#), donde encontrará la función de cada uno de los campos del datagrama 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.

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 14.

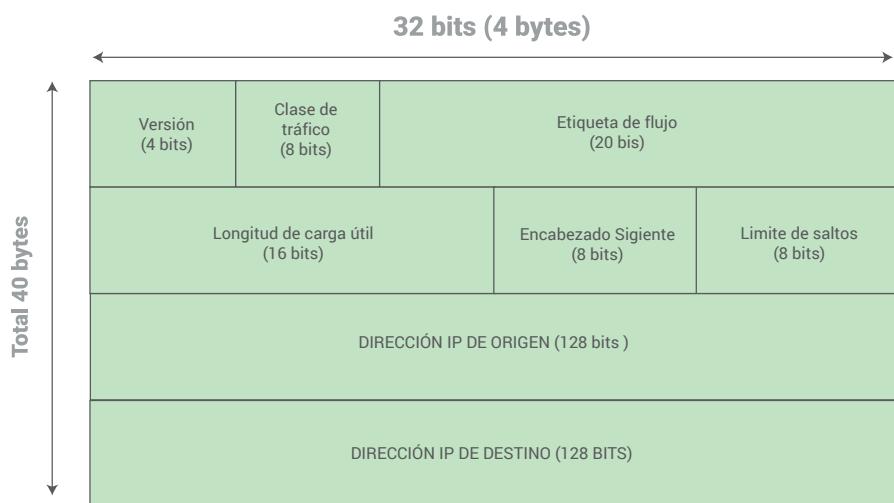


Figura 14. Formato del encabezado de un datagrama IPv6

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



Actividades de aprendizaje recomendadas

Es importante conocer la función de cada uno de los campos del encabezado, para lo cual debe revisar el punto 4.3.5 del texto básico y también acceder la actividad interactiva [encabezado de datagrama IPv6](#) donde encontrará la función de cada uno de los campos del datagrama IPV4.

1.5. Dispositivos de red

Estimado estudiante 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, TVs 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 dispositivos como laptops, TV, consolas de juegos, entre otros (ver Figura 15).



Figura 15. Interfaz de red cableada del tipo RJ45

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 recomendables 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 en base a una tabla de direcciones MAC donde tienen asociadas las direcciones físicas con la interfaz de red a la que están conectadas. Estos dispositivos

Índice

Primer bimestre

Segundo bimestre

Solucionario

Referencias bibliográficas

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 16.

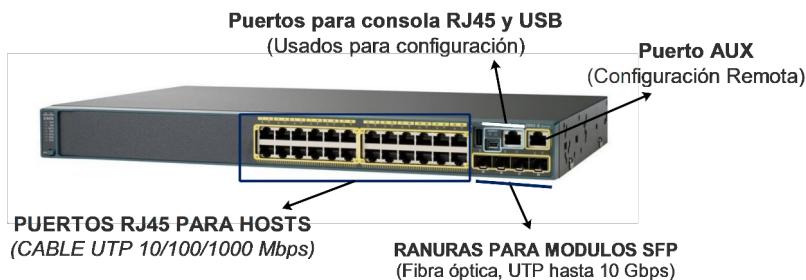


Figura 16. Puertos del switch o comutador capa 2, modelo Cisco2960 de 24 puertos

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 ruteadores

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 ruteador permite aislar el tráfico interno de la red de otras redes e Internet, conecta una red LAN con una WAN (ver Figura 17).

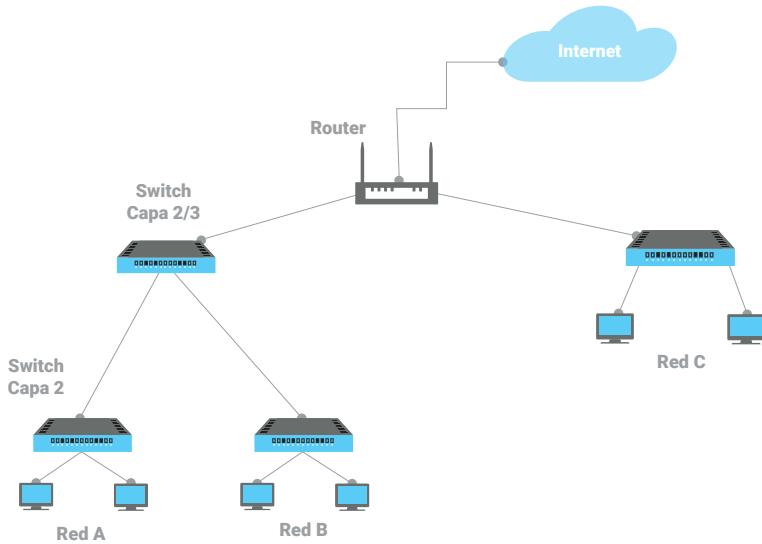


Figura 17. Ejemplo de red de una empresa con varias redes interconectadas por un router

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 su pueden observar en la Figura 18. *Las interfaces del router que se conecten deberán tener configurada una dirección IP.*

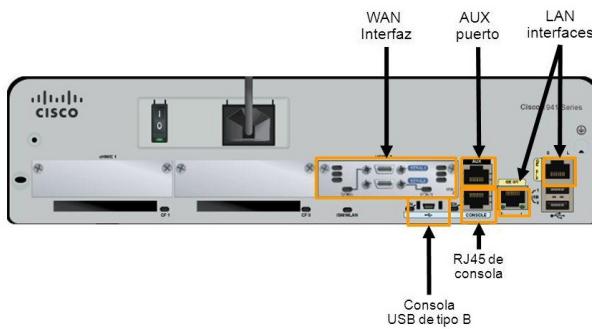


Figura 18. Interfaces de un ruteador, en este caso marca Cisco modelo 1941(CISCO, 2019b)

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 19).

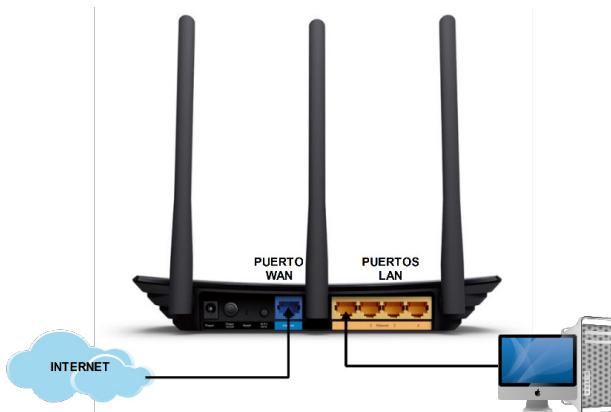


Figura 19. Interfaces de un ruteador doméstico, modelo TP-Link TL-WR940N



Actividades de aprendizaje recomendadas

Estimado estudiante es muy importante realizar una lectura del punto 4.2 al 4.2.1 del texto básico, donde deberá comprender los diferentes puertos de entrada y salida, y el procesamiento que se da en los puertos.

También debe revisar el vídeo del canal de Youtube, Mastering IT, [¿cómo funcionan los routers y los switches dentro de una red?](#). Aquí podrá complementar la lectura para conocer el funcionamiento y partes de un switch.

Ahora lo invitamos a revisar los 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.

Índice

Primer
bimestre

Segundo
bimestre

Solucionario

Referencias
bibliográficas

10. La 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**Contenidos, recursos y actividades de aprendizaje**

Para lograr el objetivo 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.

**Semana 2****Unidad 2. Direccionamiento de capa de red**

Estimado estudiante 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).

2.1. Direccionamiento IPv4

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).

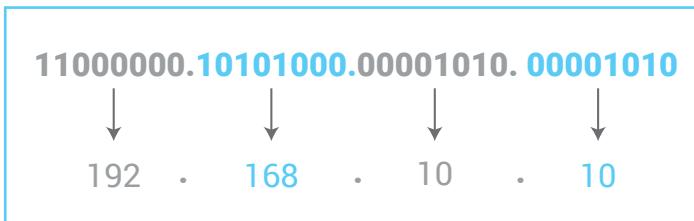


Figura 20. Representación de dirección IPv4 de 32 bits en notación decimal punteada

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).

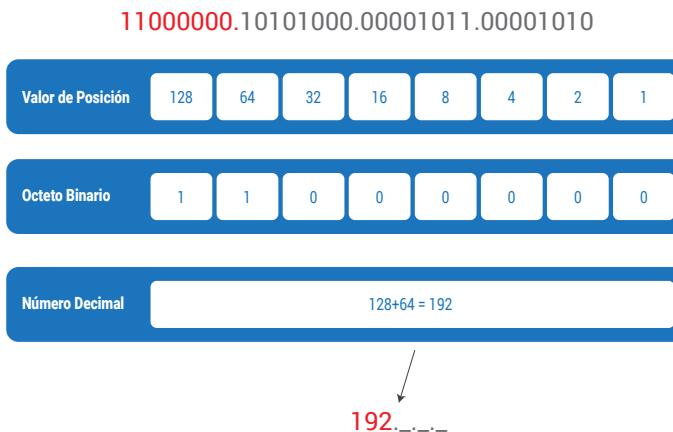


Figura 21. Conversión del octeto en binario a número decimal

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:

$$\text{Octeto 1: } 128 + 64 + 16 + 8 = \mathbf{216}$$

$$\text{Octeto 2: } 128 + 8 = \mathbf{136}$$

$$\text{Octeto 3: } 8 + 2 = \mathbf{10}$$

$$\text{Octeto 4: } 128 + 32 + 8 = \mathbf{168}$$

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.

Índice

Primer bimestre

Segundo bimestre

Solucionario

Referencias bibliográficas

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).

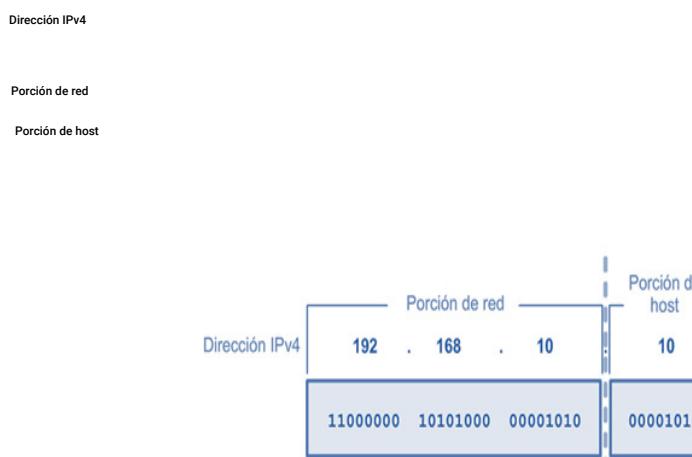


Figura 22. Porción de red y porción de host en una dirección IPv4 (CISCO, 2019a)

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 broadcast. 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 puedes 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.

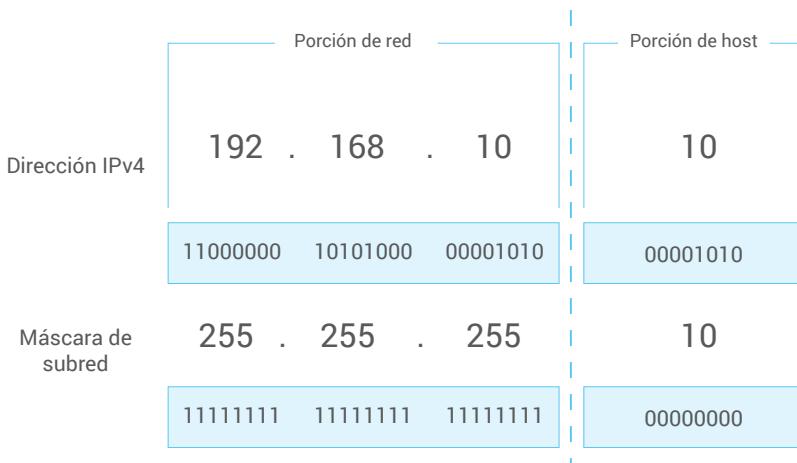


Figura 23. Máscara de subred de una dirección IP de host IPv4.(CISCO, 2019a)

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

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 o 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 o 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

Índice

Primer bimestre

Segundo bimestre

Solucionario

Referencias bibliográficas

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 o 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 de subred	Prefijo CIDR	Máscara de subred	Prefijo CIDR	Máscara de subred
/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

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.



Actividades de aprendizaje recomendadas

Estimado estudiante es muy importante realizar una lectura del punto 4.3.3 del texto básico, donde deberá comprender como se asignan las direcciones IP.

2.2. Direccionamiento IPv6

Ahora estimado estudiante, 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

Índice

Primer bimestre

Segundo bimestre

Solucionario

Referencias bibliográficas

tiene 128 bits, aproximadamente unas $340 \times 10^{36} (2^{128})$ 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 representan 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 hekteto (16 bits). En total la dirección IPv6 está compuesta por ocho hektetos (ver Figura 25).

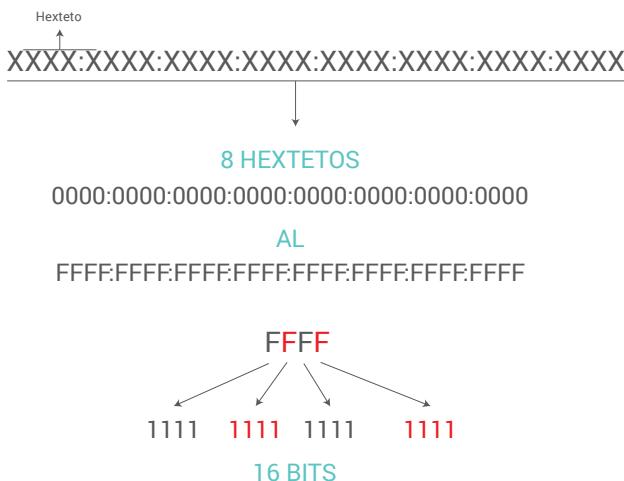


Figura 25. Estructura de una dirección IPv6

Índice

Primer bimestre

Segundo bimestre

Solucionario

Referencias bibliográficas

Un ejemplo de dirección IPv6 sería: 2001:0DB8:0000:1111:0000:0000:0000:0200, 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 :

2001:0DB8:0000:1111:0000:0000:0000:0200

La dirección simplificada 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

La notación comprimida sería

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 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.

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

Ejemplo: FE80:100::/64

FE80:0100:0000:0000	0000:0000:0000:0000
---------------------	---------------------

Figura 26. Longitud del prefijo de una dirección IPv6

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.

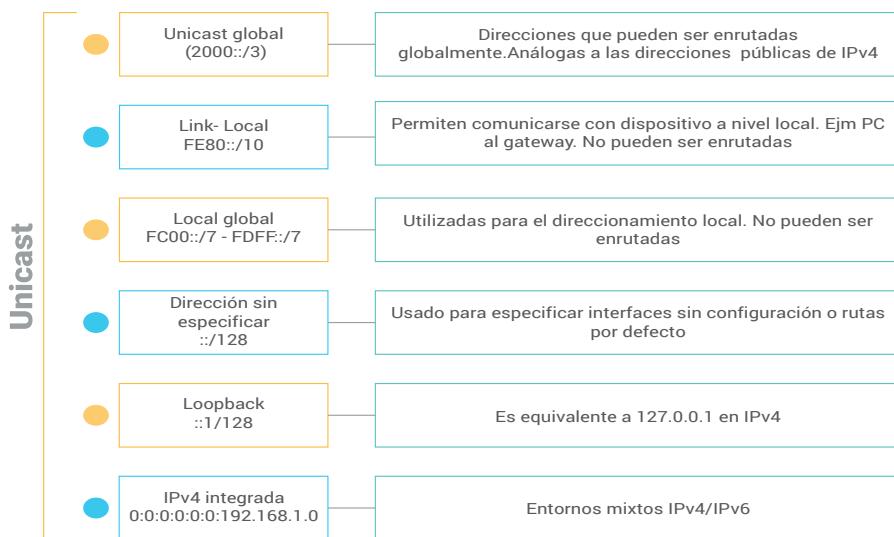


Figura 27. Tipos de direcciones unicast de IPv6 y su aplicación

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 enrutasadas globalmente en Internet.

Prefijo Routing Global 48 bits	ID de la Subred	ID de la interfaz
2001:0DB8:ACAD	001	0000:0000:0000:0000

Figura 28. Formato de dirección global unicast, prefijo de ruteo global, id de subred y de interfaz

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 un 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.

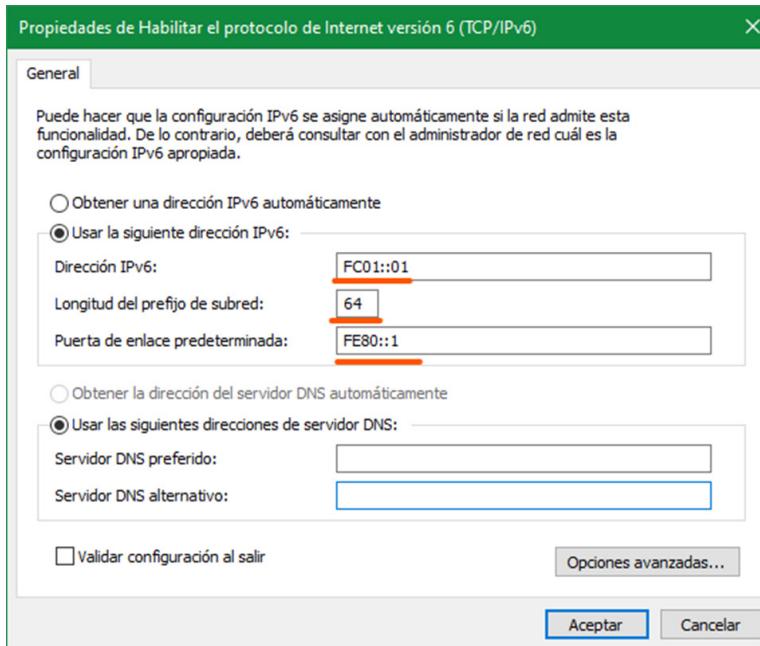


Figura 29. Asignación de dirección IPv6 en PC con Windows 10

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.

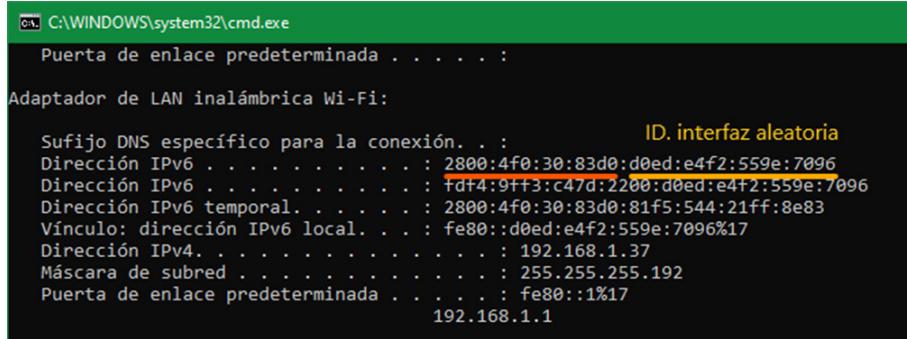
- Y un combinado con SLAAC con DHCPv6 sin información de estado, donde un router puede configurar la dirección IPv6, pero información adicional como la dirección del servidor DNS se la tiene que obtener de un servidor DHCPv6. Utiliza SLAAC para asignar la dirección unicast global y la dirección del gateway,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

En SLACC 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 7mo 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 7mo 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 la 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 la ID de la interfaz, también que una interfaz puede tener más de una dirección IPV6 asignada.

En el caso del sistema operativo Windows genera una ID de interfaz de manera aleatoria.(ver Figura 30).



```
C:\WINDOWS\system32\cmd.exe
Puerta de enlace predeterminada . . . . . :
Adaptador de LAN inalámbrica Wi-Fi:
    Sufijo DNS específico para la conexión. . . . . : ID. interfaz aleatoria
    Dirección IPv6 . . . . . : 2800:4f0:30:83d0:d0ed:e4f2:559e:7096
    Dirección IPv6 . . . . . : fd+4:9ff3:c47d:2200:d0ed:e4f2:559e:7096
    Dirección IPv6 temporal. . . . . : 2800:4f0:30:83d0:81f5:544:21ff:8e83
    Vínculo: dirección IPv6 local. . . . . : fe80::d0ed:e4f2:559e:7096%17
    Dirección IPv4. . . . . : 192.168.1.37
    Máscara de subred . . . . . : 255.255.255.192
    Puerta de enlace predeterminada . . . . . : fe80::1%17
                                                192.168.1.1
```

Figura 30. Ejemplo de ID de interfaz aleatoria generada por Windows

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 para poder realizar la comunicación.

Índice

Primer bimestre

Segundo bimestre

Solucionario

Referencias bibliográficas



Actividades de aprendizaje recomendadas

Estimado estudiante es muy importante complementar la lectura revisando el material que se recomienda a continuación:

Visualizar la serie de videos del canal enRedOS NET de Youtube, Entendiendo IPv6 - Direccionamiento y Subredes: [Parte 1](#), [Parte 2](#). En el primer video podrá encontrar información acerca del direccionamiento IPv6, y el segundo video encontrará información sobre la estructura de las direcciones IPv6.

Ahora lo invitamos a revisar los conocimientos adquiridos. Si su nota es baja por favor vuelva a leer y revisar los contenidos.



Autoevaluación 2

Dadas las siguientes preguntas 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.

Índice

Primer
bimestre

Segundo
bimestre

Solucionario

Referencias
bibliográficas

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 hexetos.
 - c. 4 hexetos.
 - 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. Conteste Verdadero o Falso: Una dirección IPv6 link-local puede ser enrutada 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.

Índice

Primer
bimestre

Segundo
bimestre

Solucionario

Referencias
bibliográficas

10. Protocolo usado por IPv4 para asignar direcciones dinámicamente

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

[Ir al solucionario](#)

Resultado de aprendizaje 3 | Diseñar y dimensionar escenarios de red**Contenidos, recursos y actividades de aprendizaje**

Con este objetivo de aprendizaje usted deberá realizar lectura de la guía, revisar y comprender los ejemplos de división de subredes, así como también revisar los recursos complementarios como son los videos, que le permitirá diseñar redes en distintos escenarios y adaptar el direccionamiento lógico de la misma.

**Semana 3****Unidad 3. Subredes**

Estimado estudiante, 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).

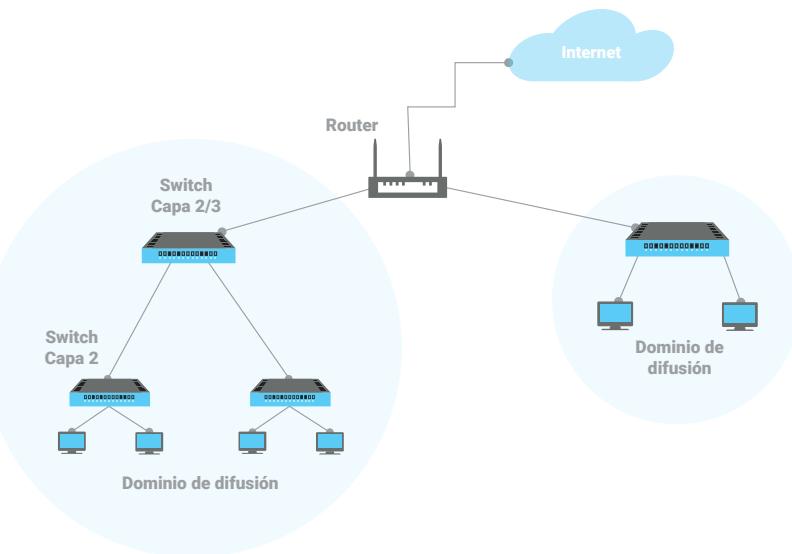


Figura 31. Dominios difusión en una red de dispositivos

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 un switch multicapa o router.

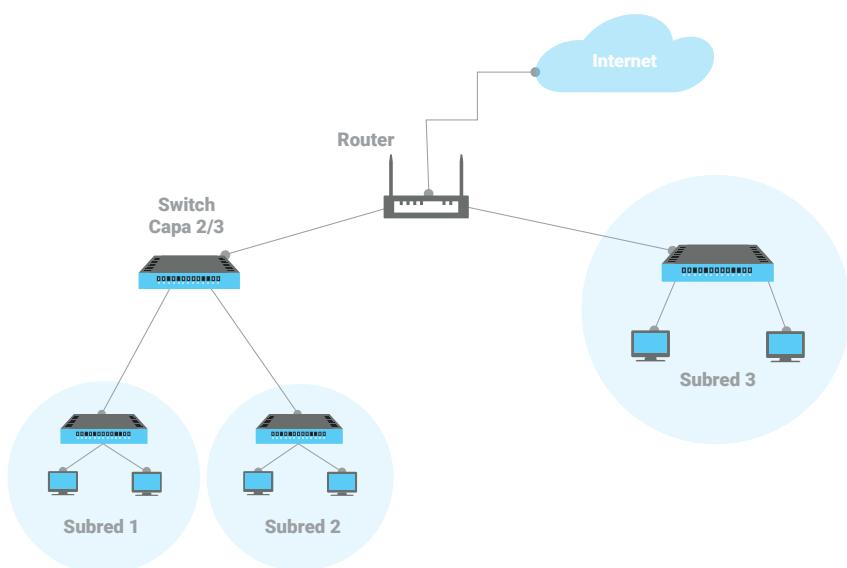


Figura 32. Subdivisión de dominios de difusión mediante subredes

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

Índice

Primer bimestre

Segundo bimestre

Solucionario

Referencias bibliográficas

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:

- a. 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.**000**00000/**27** o 192.168.1.0/**27**

- b. 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,

Índice

Primer bimestre

Segundo bimestre

Solucionario

Referencias bibliográficas

si se necesitará más hosts se debería subdividir una red con prefijo menor como por ejemplo 192.168.0.0/16.

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

$$255.255.255.\textcolor{red}{11100000} = 255.255.255.(128+64+32) = \\ 255.255.255.\textcolor{red}{224}$$

- 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 direcciones para hosts	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

Índice

Primer bimestre

Segundo bimestre

Solucionario

Referencias bibliográficas

Área	Dirección de subred	Rango direcciones para hosts	Dirección Broadcast	Máscara de Subred	Prefijo
Contabilidad	192.168.1.128	192.168.1.129 a 192.168.1.158	192.168.1.159	255.255.255.224	/27

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.



Actividades de aprendizaje recomendadas

Estimado estudiante es muy importante complementar la lectura revisando el material que se recomienda a continuación:



Visualizar el vídeo del canal de Gabriel Marcano de Youtube, [Direccionamiento IPv4 y Subredes](#). En este vídeo podrá conocer sobre el proceso y ejemplos de división en subredes usando direcciones IPv4.

Realice el direccionamiento de la red 172.16.0.0/16, para un total de 12 subredes, y llene la Tabla 3 con las cinco primeras subredes.

Tabla 3. *Ejercicio de división de subredes*

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

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 Subnetting 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:

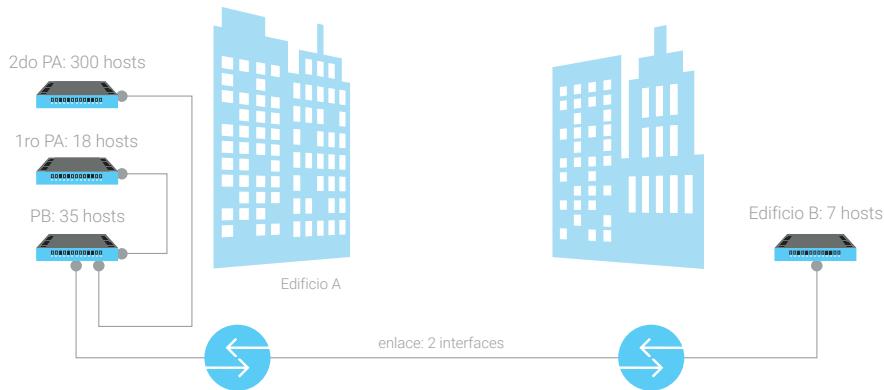


Figura 33. Requerimientos para ejemplo de VLSM

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: 50 hosts
 - 1ra Planta Alta: 18 hosts
 - Edificio B: 7 hosts
 - Enlace: 2 interfaces

Índice

Primer bimestre

Segundo bimestre

Solucionario

Referencias bibliográficas

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 172.16.0000000.0.0000000, donde los bits en rojo son los que vamos a usar para la porción de hosts.

$$\text{Número de hosts} = 2^9 - 2 = 512 \text{ hosts}$$

Luego que el prefijo para esta subred sería: $32-9 = 23$ (/23), que le corresponde la máscara de subred 255.255.252.0, con esto calculamos el número mágico para saber el siguiente rango a dividir:

Luego el rango iría de **172.16.0.0/23 a 172.16.3.255/23** para la primera subred, ya que la primera dirección de la siguiente subred sería 192.168.4.0 por lo que se resta 1. Siendo 192.168.0.0 la dirección de subred y 192.168.3.255 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 tiene la misma máscara que la anterior subred, el rango iría de **172.16.4.0/26 a 172.16.4.127/26** para la segunda subred.

4. Para 18 hosts se requieren de cinco (5) bits:

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

Índice

Primer bimestre

Segundo bimestre

Solucionario

Referencias bibliográficas

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:

$$\text{Número de hosts}=25-2=30 \text{ hosts}$$

Por lo que el rango iría de **172.16.4.128/27** a **172.16.4.159/27** para la tercera subred.

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

$$\text{Número de hosts}=24-2=14 \text{ hosts}$$

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 **172.16.4.160/28** a **172.16.4.175/28** para la cuarta subred.

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

$$\text{Número de hosts}=22-2=2 \text{ hosts}$$

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 **172.16.4.176/30 a 172.16.4.179/30** para la quinta subred. Con esto el esquema de división de subredes con VLSM a usar, se resume en la Tabla 4.

Tabla 4. *Ejemplo de división en subredes con VLSM*

Área	Dirección de subred	Rango direcciones para hosts	Dirección Broadcast	Máscara de Subred	Prefijo
2da Planta Alta (300 hosts)	172.16.0.0	172.16.0.1 a 192.168.3.254	172.16.3.255	255.255.252.0	/23
Planta Baja (35 hosts)	172.16.4.0	172.16.4.1 a 172.16.4.126	172.16.4.127	255.255.255.224	/26
1ra Planta Alta (18 hosts)	172.16.4.128	172.16.4.129 a 172.16.4.158	172.16.4.159	255.255.255.224	/26
Edificio B (7 hosts)	172.16.4.160	172.16.4.161 a 172.16.4.174	172.16.4.175	255.255.255.240	/28
Enlace (2 hosts)	172.16.4.176	172.16.4.177 a 172.16.4.178	172.16.4.179	255.255.255.252	/30



Actividades de aprendizaje recomendadas

Estimado estudiante es muy importante complementar la lectura revisando el material que se recomienda a continuación:

Visualizar el vídeo del canal de Gabriel Marcano de Youtube, [VLSM Explicado en un ejemplo](#). Aquí podrá revisar la resolución de un ejemplo usando VLSM para la división de subredes.

Realice la división en subredes de la red 10.0.0.0/8 con VLSM, para un total de 5 subredes, que son Ventas: 600 hosts, Recursos Humanos: 300 hosts, TI: 150 hosts, Contabilidad: 80 hosts, Enlace 1: 2 interfaces, Enlace 2: 2 interfaces, y llene la Tabla 5.

Índice

Primer bimestre

Segundo bimestre

Solucionario

Referencias bibliográficas

Tabla 5. *Ejercicio de división de subredes*

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

Ahora lo invitamos a revisar los conocimientos adquiridos. Si su nota es baja por favor vuelva a leer y revisar los contenidos.



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.

Índice

Primer
bimestre

Segundo
bimestre

Solucionario

Referencias
bibliográficas

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 3ra 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.

Índice

Primer
bimestre

Segundo
bimestre

Solucionario

Referencias
bibliográficas

9. Si la 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 4ta subred?
- a. 172.16.48.255.
 - b. 172.16.31.255.
 - c. 172.16.32.255.
 - d. 172.16.47.255.

[Ir al solucionario](#)

Índice

Primer bimestre

Segundo bimestre

Solucionario

Referencias bibliográficas

Resultado de aprendizaje 4

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

Contenidos, recursos y actividades de aprendizaje

Mediante este objetivo 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.



Semana 4



Unidad 4. Generalidades de protocolos de enrutamiento

Estimado estudiante 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).

4.1. Reenvío y enrutamiento

La función de reenvío y enrutamiento es muy sencilla, ya que el dispositivo despacha los paquetes recibidos y los conmuta 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 conmutado 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 enviado.



Actividades de aprendizaje recomendadas

Estimado estudiante le invitamos a revisar el punto 4.1.1 del texto básico, donde podrá conocer sobre las funciones de reenvío y enrutamiento en los planos de datos y de control.

Cuando el router recibe un paquete que está dirigido hacia una red remota, éste 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.

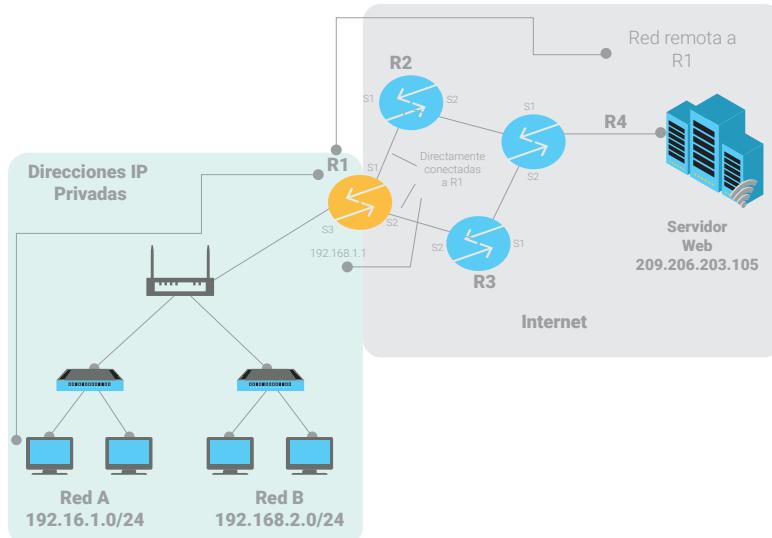


Figura 34. Tipos de rutas y redes con respecto al router R1

Índice

Primer bimestre

Segundo bimestre

Solucionario

Referencias bibliográficas

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.

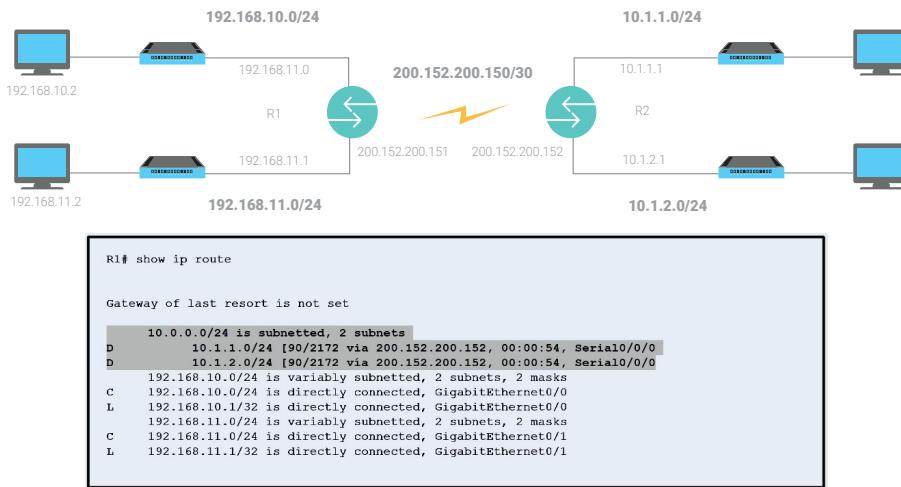


Figura 35. Tabla de ruteo de un router marca CISCO

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 indican 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.

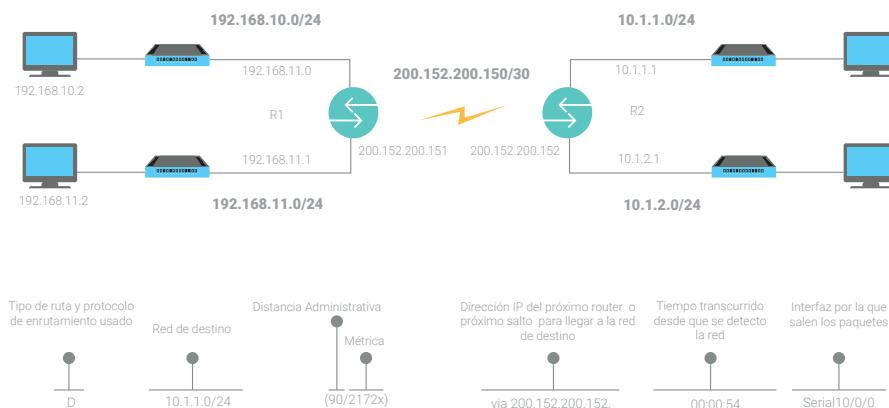


Figura 36. Interpretación de líneas de tablas de ruteo



Actividades de aprendizaje recomendadas

Estimado estudiante, ahora vamos a realizar una actividad para obtener las tablas de ruteo que están almacenadas en su PC. Para lo cual seguiremos los siguientes pasos:

1. Estando en el escritorio de Windows, presionar las teclas + .
2. Escribimos en el cuadro de dialogo el comando: cmd y presionamos la tecla enter .
3. Se abrirá la consola de Windows, donde ingresaremos el comando: netstat -r y presionamos la tecla enter .

4. Aquí se desplegará información de las interfaces que dispone, y se mostrarán las tablas de ruteo para IPv4 e IPv6 (ver Figura 37).

IPv4 Tabla de enruteamiento				
Rutas activas:	Máscara de red	Puerta de enlace	Interfaz	Métrica
0.0.0.0	0.0.0.0	192.168.1.1	192.168.1.17	35
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

Figura 37. Tabla de enrutamiento de un host de Windows, obtenida mediante el comando netstat -r

5. Con la información desplegada de su computador, identifique la ruta predeterminada (0.0.0.0), a que dirección IP son enviados los paquetes: _____. Esta dirección pertenece al _____. ¿Qué máscara de subred tiene la ruta por defecto? _____.
6. 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.

4.2. Funcionamiento de un router

Como habíamos dicho los routers o ruteadores son dispositivos de capa 3, es decir que trabajan desde la capa 1 hasta la capa 4, pueden procesar las PDUs 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 38), 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.

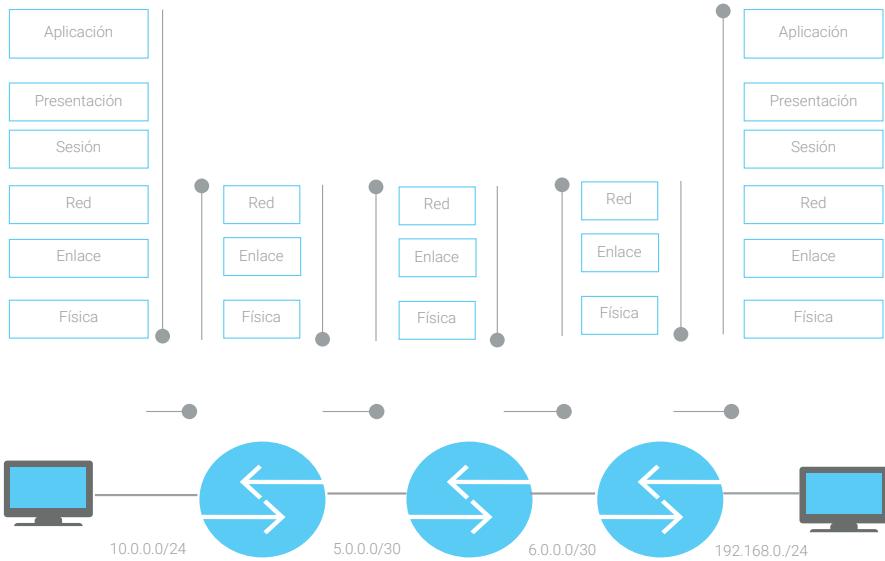


Figura 38. Encapsulamiento y desencapsulamiento en routers

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 39). 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.

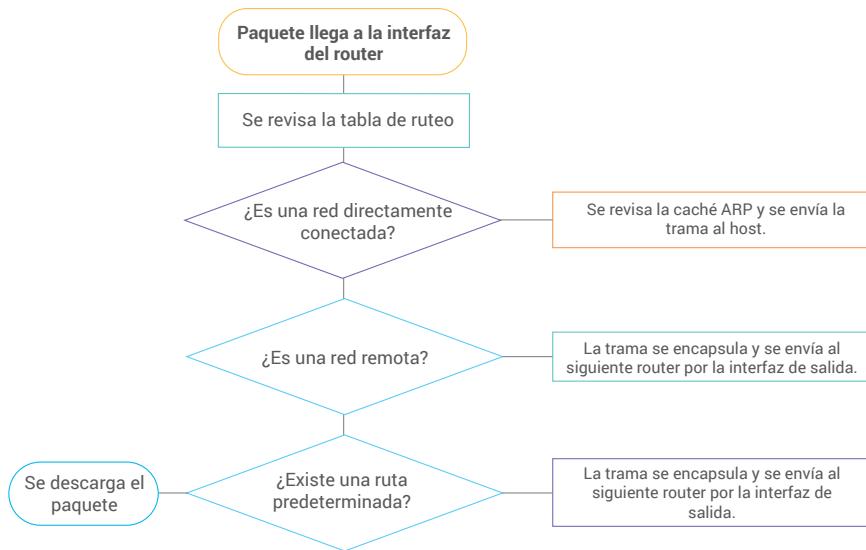


Figura 39. Proceso de enrutamiento de paquetes en los routers



Actividades de aprendizaje recomendadas

Estimado estudiante le invitamos a revisar el punto 4.2 del texto básico, donde podrá conocer sobre los aspectos del proceso de conmutación de paquetes, colas de entrada y salida, y la planificación de paquetes.

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 40.



Figura 40. Tipos de enrutamiento en las redes de dispositivos

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 bajos 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 41.

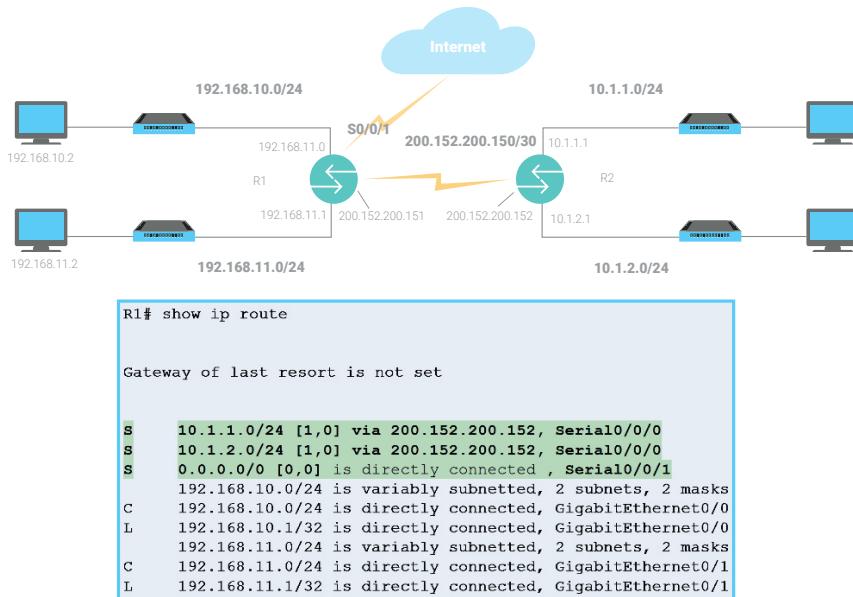


Figura 41. Ejemplo de tabla de ruteo con rutas estáticas

Índice

Primer bimestre

Segundo bimestre

Solucionario

Referencias bibliográficas



Actividades de aprendizaje recomendadas

Estimado estudiante le invitamos a realizar la actividad interactiva [Enrutamiento Estático](#), use como referencia la tabla de la Figura 41.

Ahora lo invitamos a revisar los conocimientos adquiridos. Si su nota es baja por favor vuelva a leer y revisar los contenidos.



Autoevaluación 4

Dado los siguientes ítems, seleccionar la respuesta correcta:

1. Un router para poder reenviar o enrutar un paquete debe revisar:
 - a. 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 permiten 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 a 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
 - a. Ruta predeterminada.
 - b. Ruta a red remota.
 - c. 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?
 - a. Se devuelve a emisor.
 - b. Se envía por todas las interfaces.
 - c. Se descarta el paquete.
 - d. Se a 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#
```

Figura 42. Tabla de ruteo de ejemplo para autoevaluación 1

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

[Ir al solucionario](#)

Resultado de aprendizaje 5

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

Contenidos, recursos y actividades de aprendizaje

Mediante este objetivo 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 fondo como un router decide que ruta escoger.



Semana 5

**Unidad 5. Algoritmos de enrutamiento**

Estimado estudiante 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).

5.1. Introducción

Un router una vez que recibe un paquete tiene que buscar en su tabla de enrutamiento para saber por cual ruta debe reenviarlo, para ellos podemos usar el enrutamiento estático, pero a medida que las redes crecen o cambian se vuelve muy complicado y tedioso realizar 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 43). Revisaremos los protocolos RIP, OSPF y BGP.

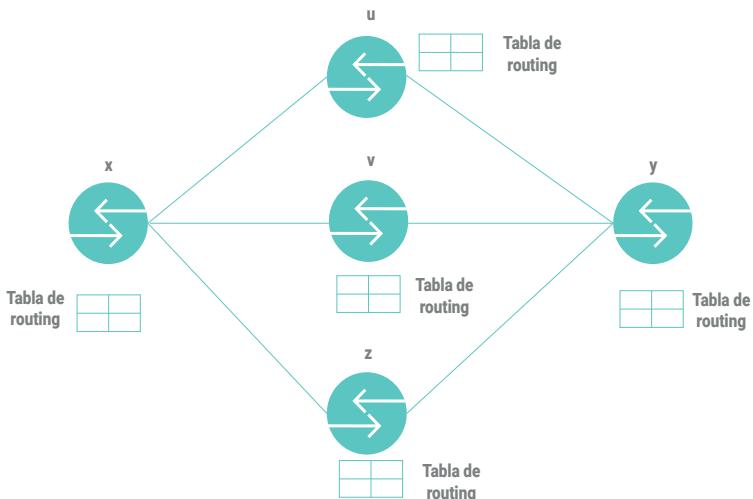


Figura 43. Enrutamiento con control por router

Control lógicamente centralizado, en este caso un controlador centralizado calcula, y distribuye las tablas de enrute 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 44). El control centralizado se implementa mediante la técnica SDN (Software Defined Network) o redes definidas por software.

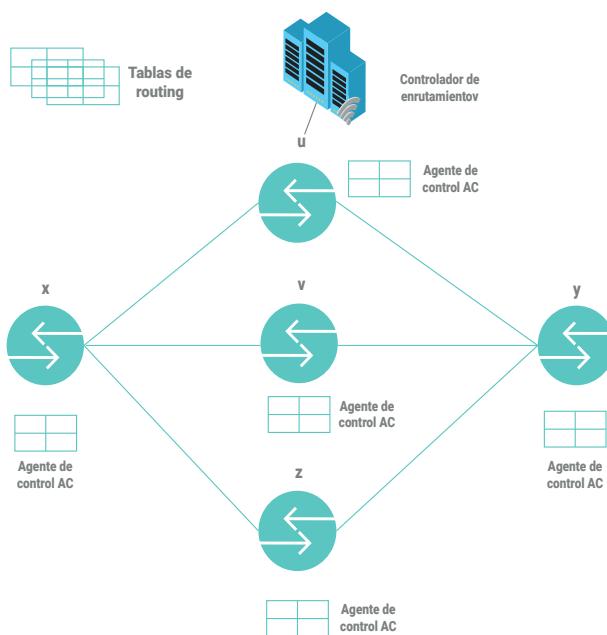


Figura 44. Enrutamiento con control lógicamente centralizado

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 enrutamiento tenemos dos tipos:

Índice

Primer bimestre

Segundo bimestre

Solucionario

Referencias bibliográficas

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.



Actividades de aprendizaje recomendadas

Estimado estudiante le invitamos a leer el punto 5.1 del texto básico para profundizar ambos conceptos.

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

Índice

Primer bimestre

Segundo bimestre

Solucionario

Referencias bibliográficas

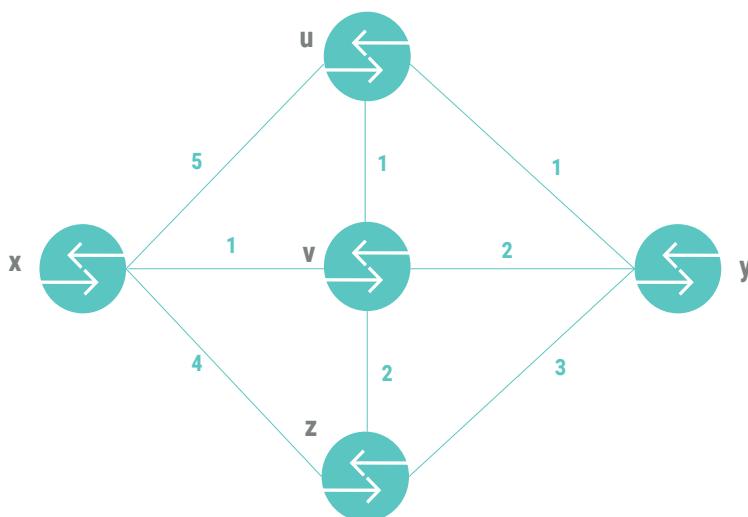


Figura 45. Grafo para ejemplo de funcionamiento del algoritmo Dijkstra

Para implementar el algoritmo tenemos que formar pares donde es el costo del enlace desde 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 6.

Tabla 6. *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				

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 7).

Tabla 7. *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				

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 8).

Tabla 8. *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 , V)  (2 , V)	
V		(1 , X)  (1 , X)		
Z		(4 , X)	(1 + 2 , V)	
Y				

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 9).

Tabla 9. *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 , V)  (2 , V)	
V		(1 , X)  (1 , X)		
Z		(4 , X)	(1 + 2 , V)	
Y				(2 + 1 , U) = (3 , U)

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 46). Si en alguna iteración hay dos nodos con el mismo coste acumulado, eso significa que haya más de un mejor camino al destino.

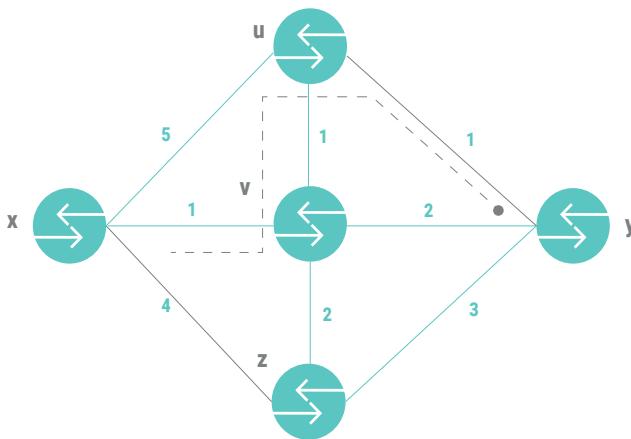


Figura 46. Mejor camino entre X e Y obtenido por el algoritmo Dijkstra



Actividades de aprendizaje recomendadas

Estimado estudiante le invitamos a revisar el punto 5.2.1 del texto básico donde podrá revisar cómo funciona el algoritmo Dijkstra, con mayor detalle.

 Revisar el vídeo del canal de YouTube Studios CAT, denominado [Algoritmo de DIJKSTRA](#), donde podrá encontrar un ejemplo del mismo, y el vídeo de la Universidad Rey Juan Carlos, denominado [Algoritmos de enrutamiento: Estado de enlaces](#), donde se explican los conceptos sobre este tipos de enrutamiento.

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

Índice

Primer bimestre

Segundo bimestre

Solucionario

Referencias bibliográficas

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 1 del mismo nombre, la cual es:

Ecuación 1: Ecuación de Bellman-Ford

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

Donde:

$d_x(y)$: el coste mínimo de la ruta mínima 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

Estimado estudiante le invitamos a revisar el punto 5.2.2 del texto básico donde podrá revisar cómo funciona el algoritmo vector distancia. Adicionalmente realice las siguientes actividades complementarias.

 Revisar el vídeo del canal de YouTube de la Universidad Rey Juan Carlos denominado [Algoritmos de enrutamiento: Vector de Distancias](#), donde se exponen los conceptos sobre este tipo de enrutamiento.

Calcular la mejor ruta usando los algoritmos de estado enlace LS y vector distancia DV del diagrama de la Figura 47.

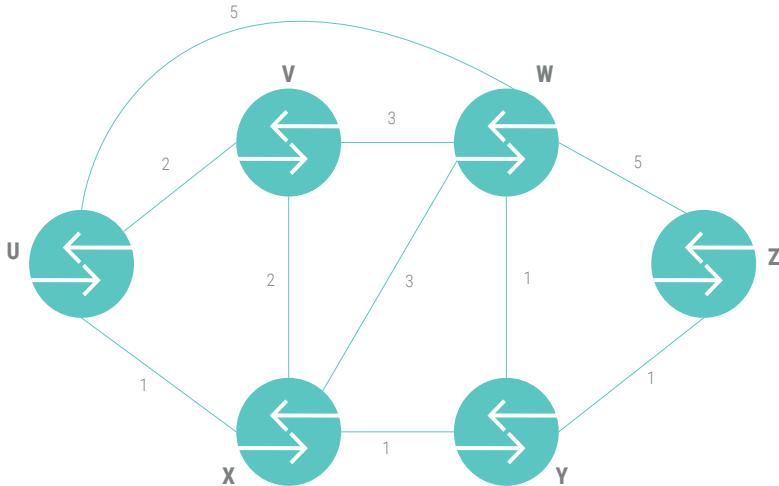


Figura 47. Ejercicio planteado para resolución de algoritmo de enrutamiento

Ahora lo invitamos a revisar los conocimientos adquiridos. 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 enrutamiento 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.

Índice

Primer bimestre

Segundo bimestre

Solucionario

Referencias bibliográficas

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.

Índice

Primer bimestre

Segundo bimestre

Solucionario

Referencias bibliográficas

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](#)

Índice

Primer bimestre

Segundo bimestre

Solucionario

Referencias bibliográficas

Resultado de aprendizaje 6

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

Contenidos, recursos y actividades de aprendizaje

Mediante este objetivo de aprendizaje se revisará los conceptos básicos sobre el protocolo de enrutamiento dinámico RIP, cuáles son sus principales parámetros, configuraciones y funcionamiento.



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 basado en (CISCO, 2019b).

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 se 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 enruteadores 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 48).

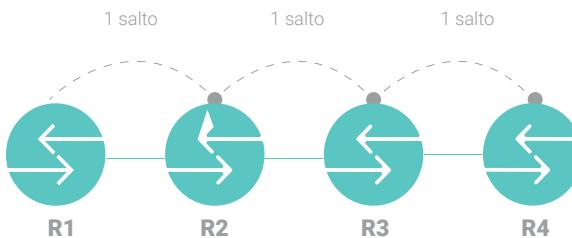


Figura 48. Ejemplo de definición de saltos en una ruta

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 reciben 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 49).

Hacia	Por medio de	Métrica									
A	A	0	B	B	0	C	C	0	D	D	0



Figura 49. Paso inicial del protocolo RIP con anuncios de rutas de redes directamente conectadas a los nodos

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 recibido (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 50).

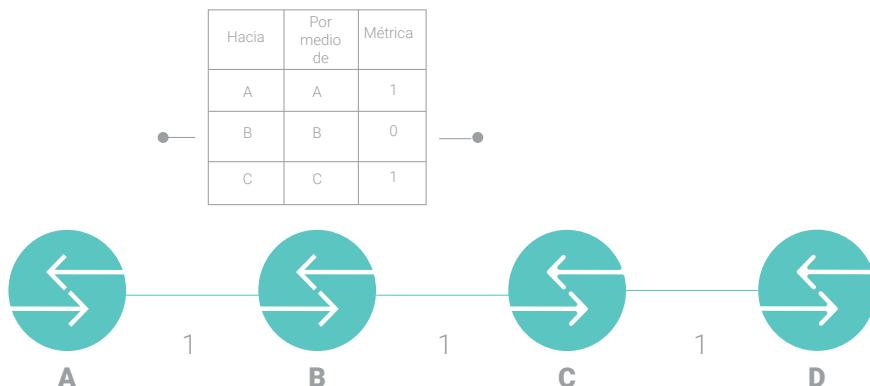


Figura 50. Tablas de ruteo del nodo B con las rutas anunciadas desde A y agregadas

Índice

Primer bimestre

Segundo bimestre

Solucionario

Referencias bibliográficas

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 51). A este tiempo se le conoce como *tiempo de convergencia*.

Hacia	Por medio de	Métrica
A	A	0
B	B	1
C	B	2
D	B	3

Hacia	Por medio de	Métrica
A	A	1
B	B	0
C	C	1
D	C	2

Hacia	Por medio de	Métrica
A	B	2
B	B	1
C	C	0
D	D	1

Hacia	Por medio de	Métrica
A	C	3
B	C	2
C	C	1
D	D	0

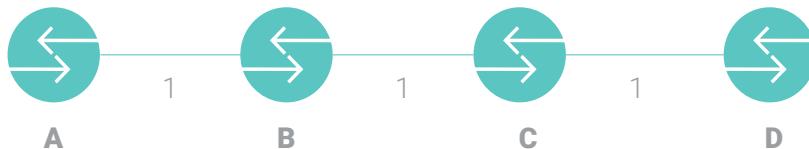


Figura 51. Tablas de ruteo actualizadas en todos los nodos



Actividades de aprendizaje recomendadas

Estimado estudiante le invitamos a realizar las siguientes actividades complementarias.

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.

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. Estimado estudiante 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 en la Figura 52.

```
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        10.10.10.0/32 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
```

Figura 52. Tabla de ruteo en router CISCO® obtenido con el comando `show ip route`

En la tabla de ruteo de la Figura 52, 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 53.

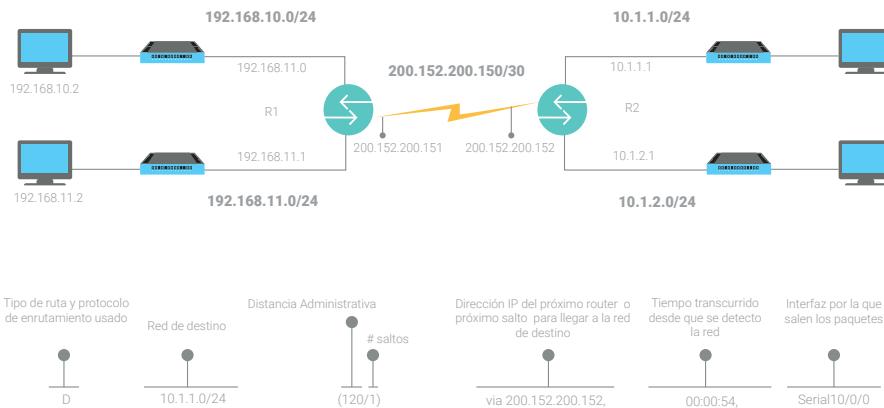


Figura 53. Componentes de una ruta aprendida en una tabla de ruteo de un router CISCO®

Podemos observar en la Figura 53 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 10.

Tabla 10. 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

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 54.

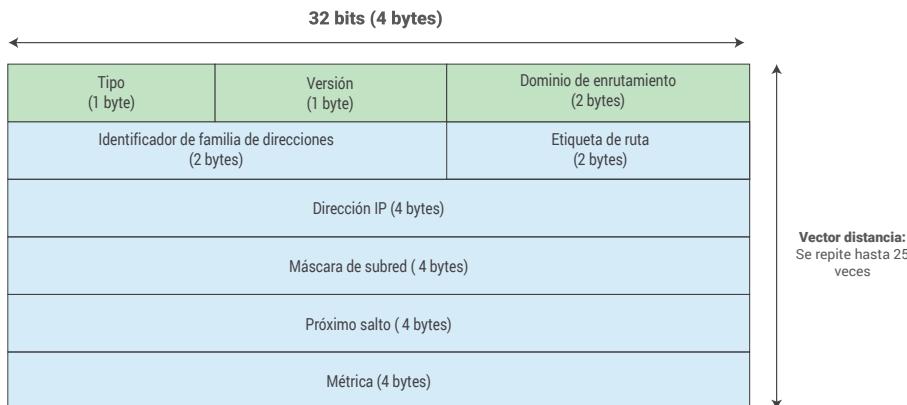


Figura 54. Mensaje del protocolo RIPv2 de acuerdo al RFC 2453



Actividades de aprendizaje recomendadas

Estimado estudiante le invitamos a revisar la utilización de cada campo del mensaje del RIPv2 en la [RFC2453](#).

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 55), el tamaño máximo de los datagramas depende de la MTU de la tecnología de transmisión empleada.(Salcedo et al., 2010)

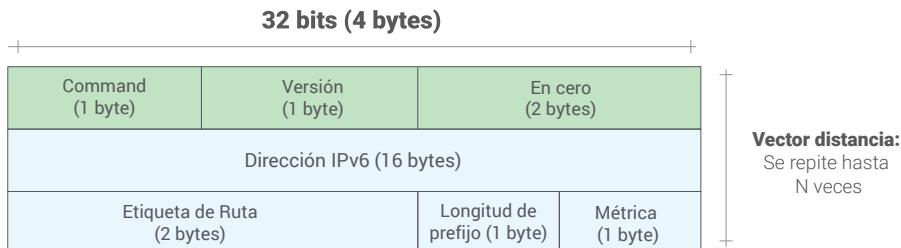


Figura 55. Mensaje del protocolo RIPng de acuerdo a la RFC2080



Actividades de aprendizaje recomendadas

Estimado estudiante le invitamos a revisar la utilización de cada campo del mensaje del RIPng en la [RFC2080](#).

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

Índice

Primer bimestre

Segundo bimestre

Solucionario

Referencias bibliográficas

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 mencionada 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

Estimado estudiante le invitamos a realizar una lectura del artículo [Análisis y evaluación del Routing Information Protocol RIP](#). Donde se explican los conceptos y aspectos más importantes sobre el protocolo RIP.

Ahora lo invitamos a revisar los conocimientos adquiridos. 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.

Índice

Primer bimestre

Segundo bimestre

Solucionario

Referencias bibliográficas

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](#)

Índice

Primer bimestre

Segundo bimestre

Solucionario

Referencias bibliográficas

Resultado de aprendizaje 7

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

Contenidos, recursos y actividades de aprendizaje

Mediante este objetivo de aprendizaje se revisarán los conceptos básicos sobre el protocolo de enrutamiento dinámico OSPF, sus parámetros principales, configuraciones y su funcionamiento.

**Semana 7****Unidad 7. Protocolos de enrutamiento dinámico OSPF**

Estimado estudiante 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).

7.1. Protocolo OSPF

Estimado estudiante 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

- *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



Actividades de aprendizaje recomendadas

Estimado estudiante le invitamos a realizar una lectura del punto 5.3 del texto básico, para comprender más a fondo los aspectos básicos sobre el protocolo OSPF.

7.1.2. Componentes de OSPF

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 al 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 ejecuta 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 permiten 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 que 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 a lo especificado en la Figura 56.

-
- ```

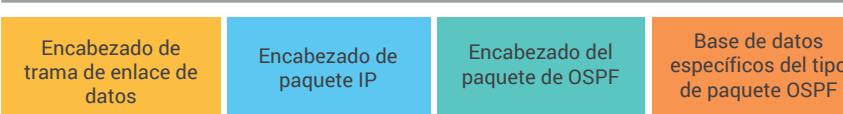
graph LR
 A[1. Se envía paquetes HELLO para establecer adyacencias] --> B[2. Se usan LSA para inundar el área con información con costos y estados enlace]
 B --> C[3. Routers crean la tabla de topología LSDB]
 C --> D[4. Se crea el SPF mediante la ejecución del algoritmo SPF sobre la LSD]
 D --> E[5. Routers crean una tabla de ruteo con las rutas calculadas con sus métricas y costos]

```
1. Se envía paquetes HELLO para establecer adyacencias
2. Se usan LSA para inundar el área con información con costos y estados enlace
3. Routers crean la tabla de topología LSDB
4. Se crea el SPF mediante la ejecución del algoritmo SPF sobre la LSD
5. Routers crean una tabla de ruteo con las rutas calculadas con sus métricas y costos

*Figura 56. Secuencia de funcionamiento de OSPF*

#### 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 57). El encabezado del paquete de OSPF identifica el tipo de paquete OSPF, la identificación del router y el número de área. 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 57. Encapsulamiento en el protocolo OSPF (CISCO, 2019c)*

El encabezado del paquete OSPF está estructurado según se especifica en la Figura 58.

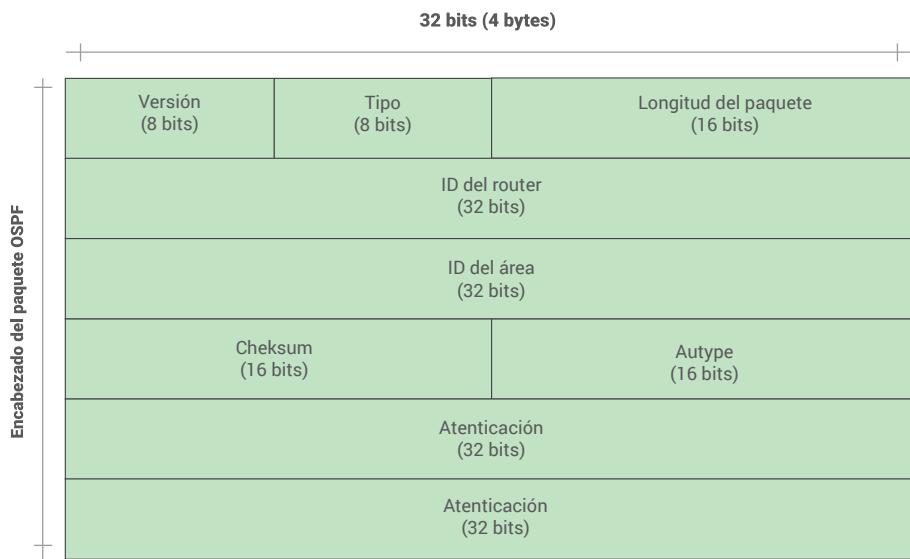


Figura 58. Encabezado de paquete OSPF

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 en la Figura 59.

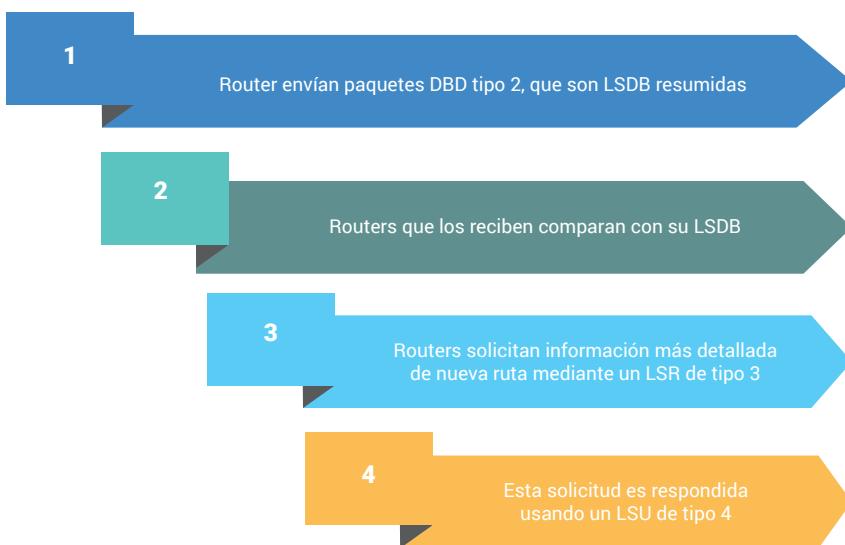


Figura 59. Actualizaciones de estado enlace

### 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 Figura 60.

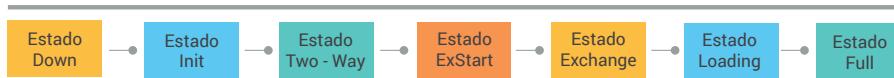


Figura 60. Estados operativos de OSPF

Ahora veamos que significa cada uno de estos estados:

- **Estado Down:** no se reciben paquetes de saludo, en este estado el router envía paquetes de saludo.
- **Estado Init:** los paquetes de saludo que contienen la ID de los routers emisores son recibidos.
- **Estado Two-Way (Dos vías):** en este estado se emplea para seleccionar al DR (Designated-Router) y BDR (Backup

Designated Router), que son los encargados de recopilar las LSDB y luego difundirlas.

- **Estado Exstart:** se establece las relaciones esclavo/maestro entre routers y se selecciona el número de secuencia de los paquetes DBD, luego el maestro inicializa el envío y recepción de paquetes DBD.
- **Estado Exchange:** se intercambian los paquetes DBD, si el router requiere información adicional se pasa al estado Loading, caso contrario se pasa directamente al estado Full.
- **Estado Loading (Cargando):** se intercambian LSR y LSU para solicitar cambios en la topología de la red, las rutas se obtienen mediante el algoritmo de la ruta más corta primero SPF, la transición se realiza al estado Full
- **Estado Full (Completo):** toda los routers tienen bases de datos convergentes.

#### 7.1.8. Router Designando DR y Router Designado de respaldo BDR

Debido 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 LSAs 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 Ecuación 2:

*Ecuación 2: 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 61).

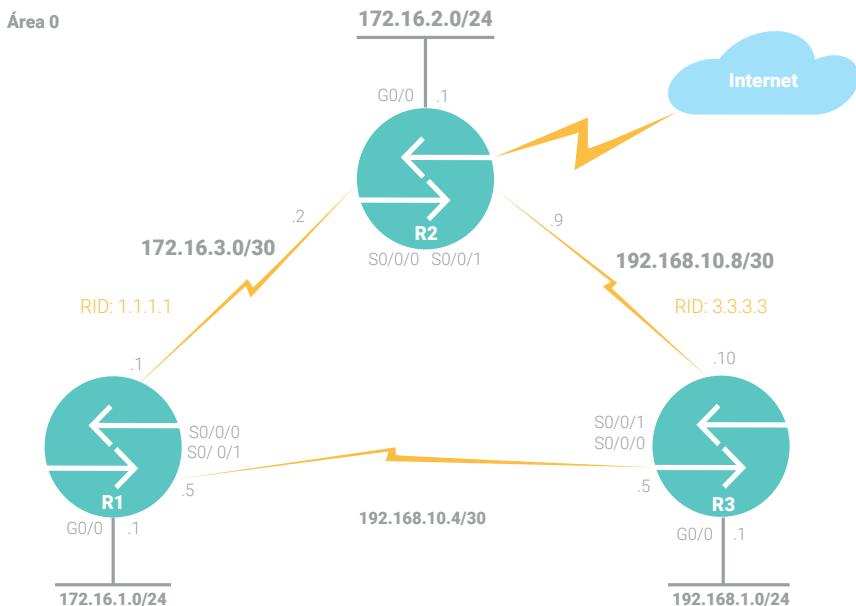


Figura 61. Topología de OSPF para área única (CISCO, 2019c)

Como se observa en la Figura 61, 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 62)

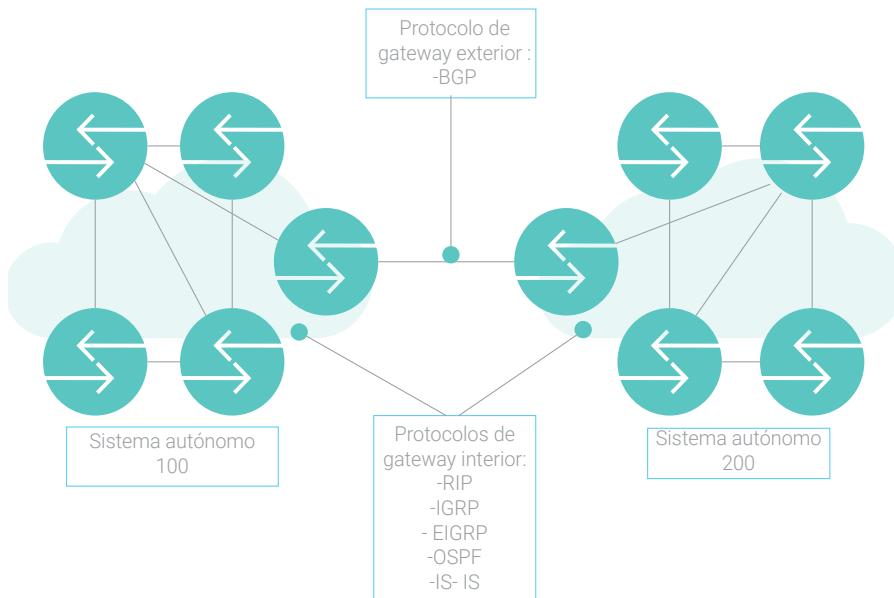


Figura 62. Sistemas autónomos y protocolos de gateway interno y externo  
(CISCO, 2019c)

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 63).

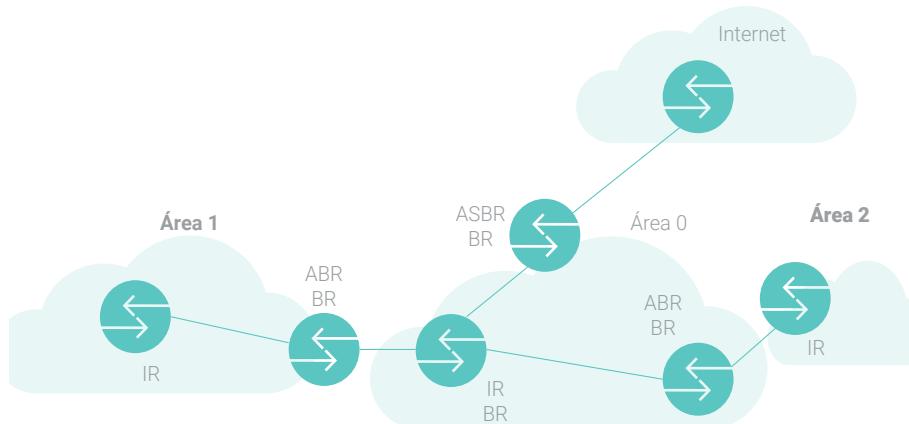


Figura 63. Tipos de routers en el protocolo OSPF

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 LSAs, 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:** estás áreas no pueden propagar LSAs de tipo 5, solo pueden conectarse fuera del AS mediante una ruta por defecto.
- **Área totally Stub:** no pueden propagar LSAs 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:** Estás áreas se usan para conectarse a un ISP, no admiten LSAs 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 64.

Índice

Primer bimestre

Segundo bimestre

Solucionario

Referencias bibliográficas

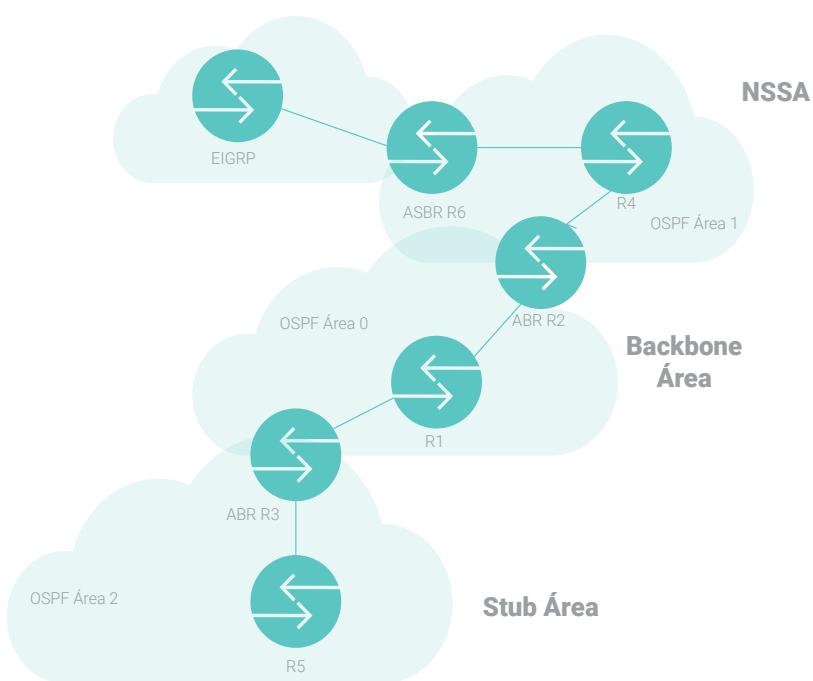


Figura 64. Tipos de áreas en el protocolo OSPF

#### 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 11.

Tabla 11. Comparación entre protocolos OSPFv2 y OSPFv3

| Característica         | OSPFv2         | OSPFv3                       |
|------------------------|----------------|------------------------------|
| Protocolo IP soportado | IPv4           | IPv6                         |
| Dirección IP origen    | Dirección IPv4 | Dirección IPv6 de link-local |

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

Una dirección IPv6 link-local permite que los dispositivos que se comuniquen 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

Estimado estudiante le invitamos a realizar una lectura del punto 5.3 del texto básico sobre enrutamiento al interior de un AS usando OSPF.



También le recomendamos revisar el vídeo donde se exponen los conceptos básicos sobre OSPF, denominado: [Protocolo de Routing de Redes OSPF](#).

Ahora lo invitamos a revisar los conocimientos adquiridos. 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. Representar 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. Representar 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.

Índice

Primer  
bimestre

Segundo  
bimestre

Solucionario

Referencias  
bibliográficas

10. Tipo de router en OSPF multiárea que permite conectar el sistema autónomo con otros AS.
- a. Internal Router IR.
  - b. Backbone Router BR.
  - c. Area Border Router ABR.
  - d. Autonomous System Border Router ASBR.

[Ir al solucionario](#)



## Actividades finales del bimestre



### Semana 8

## REPASO DE UNIDADES 1-7

Estimado estudiante, en esta semana lo invitamos a revisar los contenidos estudiados en el segundo 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 revisar los contenidos del segundo bimestre. Además, no olvide repasar las autoevaluaciones y ejercicios planteados en las unidades antes mencionadas.



## Segundo bimestre

### Resultado de aprendizaje 8

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

### Contenidos, recursos y actividades de aprendizaje

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 lecturas del libro básico, de la guía didáctica además de recursos complementarios como videos y actividades interactivas.

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



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

Índice

Primer bimestre

Segundo bimestre

Solucionario

Referencias bibliográficas



## Semana 9



### Unidad 8. Servicios de la capa de transporte

Estimado estudiante, 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 diferentes.

- Por otro lado, un protocolo de capa de red facilita la comunicación lógica entre hosts.

En la Tabla 12 se indican las principales diferencias entre la capa de red y la capa de transporte.

Tabla 12. *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. |



### Actividades de aprendizaje recomendadas

Estimado estudiante le invitamos a revisar la sección 3.1.1. del libro base con el fin de mejorar la comprensión de los contenidos revisados. En esta sección encontrará una analogía sobre la relación entre la capa de transporte y la capa de red.

### 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. Por lo tanto, por favor lea la sección 3.1.2 del libro base.

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.

Es importante que a lo largo de esta guía y siguiendo las recomendaciones del libro base, denominemos segmentos cuando nos refiramos a paquetes tanto TCP como UDP, reservando el término datagrama para los paquetes de la capa de red.

Con el fin de tener claras las características de los protocolos TCP y UDP, le invitamos a que llene la siguiente Tabla 13 comparativa entre TCP y UDP.

Tabla 13. *Comparación entre TCP y UDP.*

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

### 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 continuación, leer las secciones 2.7 y 3.2. del libro base.

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.

Con respecto a los sockets, de acuerdo con el libro base, 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).



## Actividades de aprendizaje recomendadas

Le invitamos a leer un poco más sobre los puertos, en especial sobre los denominados puertos bien-conocidos. Dichos puertos son asignados por la Autoridad de Números Asignados de Internet (IANA). Para lo cual referirse a la [página principal de asignación de puertos](#).

Una vez que ha recordado los conceptos de puertos y sockets procedemos a revisar 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.



## Actividades de aprendizaje recomendadas

Usando el software Wireshark, ingrese a la [página web de UTPL](#) y obtenga los componentes del socket.

### 8.3.1. Multiplexación y demultiplexación sin conexión

Para tener una mejor comprensión de la multiplexación y demultiplexación sin conexión, es necesario, estimado estudiante, que revise la sección 3.2. del libro base.

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 tupla 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.

Índice

Primer bimestre

Segundo bimestre

Solucionario

Referencias bibliográficas



Estimado estudiante con el fin de reforzar los contenidos relacionados con esta unidad, por favor, revisar el [video sobre nmap](#). En este video encontrará información relacionada con el programa nmap. Nmap es un programa que le permitirá realizar un escáner de puertos.



### Actividades de aprendizaje recomendadas

Descargar el programa [nmap de la página](#) y proceder a realizar un escaneo de puertos. Puede realizar una tabla e indicar los puertos encontrados (TCP y UDP). Además, indicar si los puertos encontrados son puertos abiertos, cerrados o inalcanzables. Se recomienda revisar la sección 3.5.6 del libro base para mayor información de nmap.

Estimado estudiante, en la unidad 3 nos centramos en conocer la capa de transporte. Además, de conocer los procesos de multiplexación y demultiplexación. A continuación, le invitamos a desarrollar la Autoevaluación 8 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:
- Dirección IP de destino y número de puerto de origen.
  - Dirección IP de destino y número de puerto de destino.
  - Número de puerto de origen y número de puerto de destino.
  - Dirección IP de origen y dirección IP de destino.
5. Un número de puerto se representa mediante:
- 8 bits.
  - 12 bits.
  - 16 bits.
  - 32 bits.
6. ¿Qué número de puerto utiliza FTP?
- 20.
  - 21.
  - 22.
  - 23.
7. ¿En la capa de transporte se manejan paquetes?
- Falso.
  - Verdadero.
8. ¿Cómo se identifican de forma única las conexiones en un mismo equipo?
- Mediante las direcciones IP de origen y destino.
  - Mediante sockets.
  - Mediante la dirección de la tarjeta de la red del equipo.
  - Mediante numeración de conexiones entrantes y salientes.

Índice

Primer bimestre

Segundo bimestre

Solucionario

Referencias bibliográficas

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](#)

**Resultado de aprendizaje 9**

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

**Contenidos, recursos y actividades de aprendizaje**

A través de este resultado de aprendizaje, usted conocerá 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.

Estimado estudiante 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](#). Estas diapositivas le permitirán revisar de manera simplificada las principales características del protocolo UDP.



## Semana 10



### Unidad 9. Transporte sin conexión - UDP

Estimado estudiante, 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). Le recordamos que el protocolo UDP es estudiado en la sección 3.3. del libro base y le invitamos a revisarla para complementar con los contenidos de esta guía.

#### 9.1. Características de UDP

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

##### ¿Qué significa que un protocolo sea no 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 Tabla 14. Esta estructura se encuentra definida en el documento RFC 768.

Tabla 14. *Estructura del segmento UDP.*

| Bit (0)                    | Bit (15) Bit (16)              | Bit(31) |
|----------------------------|--------------------------------|---------|
| Puerto de origen (16 bits) | Puerto de destino (16 bits)    |         |
| Longitud total (16 bits)   | Suma de comprobación (16 bits) |         |
| Datos (longitud variable)  |                                |         |

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 comprobación 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, como se indica en la sección 3.3.1. del libro base, 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 comprobación es usada para la detección de errores. El proceso de suma de comprobación 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 comprobación del segmento UDP.

Para un mejor entendimiento explicaremos aquí el ejemplo propuesto en la sección 3.3.2. del libro base.

[Índice](#)[Primer bimestre](#)[Segundo bimestre](#)[Solucionario](#)[Referencias bibliográficas](#)

### Ejemplo:

Tabla 15. Descripción del proceso de suma de comprobación

|                                                                                                              |                                                                                                                                                                                                                                              |
|--------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Se tienen tres palabras de 16 bits<br><b>0110011001100000</b><br><b>0101010101010101</b><br>1000111100001100 | Se realiza la suma de las dos primeras palabras de 16 bits:<br><b>0110011001100000</b><br><b>0101010101010101</b><br><b>1011101110110101</b>                                                                                                 |
|                                                                                                              | A continuación, se suma la tercera palabra a la suma anterior:<br><b>1011101110110101</b><br><b>1000111100001100</b><br><b>0100101011000010</b>                                                                                              |
|                                                                                                              | Como paso final, se realiza el complemento a 1 de la suma resultante ( <b>0100101011000010</b> ), 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:<br><b>1011010100111101.</b> |

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.



### Actividades de aprendizaje recomendadas

Realice el cálculo del complemento a 1 para el ejemplo anterior en el lado del receptor. Como un segundo ejercicio, cambie algunos bits en las tres palabras iniciales simulando un error en el envío y realice nuevamente el cálculo en el lado del receptor.

### 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 datagramas 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 datagramas que están desordenados no se vuelven a ordenar, ver Figura 65.

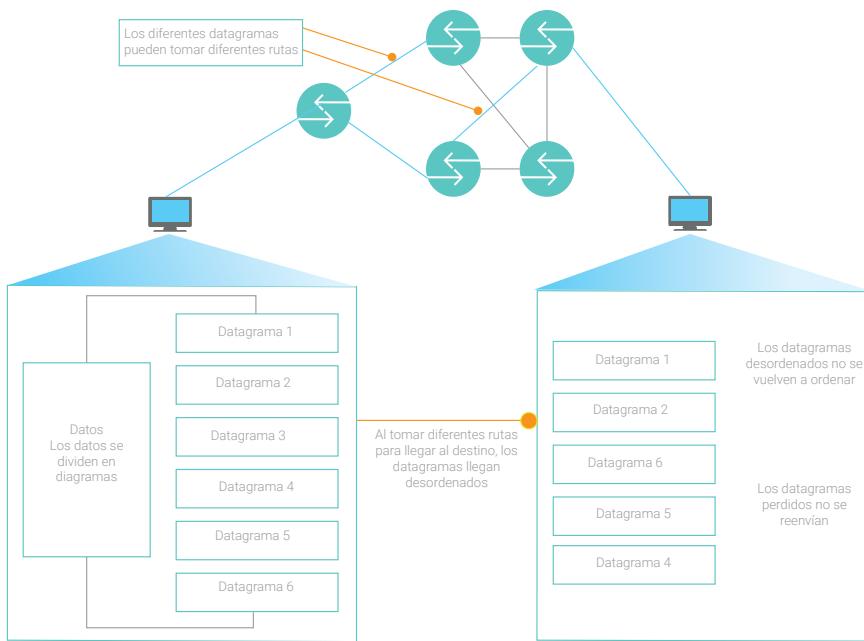


Figura 65. Comunicación de Datos (CISCO, 2019a)

### **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.

Ahora lo invitamos a revisar los conocimientos adquiridos, 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.

Índice

Primer bimestre

Segundo bimestre

Solucionario

Referencias bibliográficas

6. La ausencia de un mecanismo de control de congestión en 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 UDP establece una conexión antes de enviar los datos.
  - b. A que UDP no establece una conexión antes de enviar los datos.
  - c. A que UDP realiza la suma de comprobación.
  - d. A que 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

**Resultado de aprendizaje 10**

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

**Contenidos, recursos y actividades de aprendizaje**

Para lograr el resultado de aprendizaje planteado, en esta unidad 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.

**Semana 11**

Continuando con el estudio del protocolo UDP, en esta sección 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.

Índice

Primer bimestre

Segundo bimestre

Solucionario

Referencias bibliográficas

Estimado estudiante, con el fin de conocer los puertos de ciertas aplicaciones, en la Tabla 16 se indican los diferentes tipos de números de puerto.

Tabla 16. *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. |



### Actividades de aprendizaje recomendadas

Para profundizar en el tema de aplicaciones que utilizan UDP, se recomienda al estudiante realizar la siguiente práctica usando [Wireshark](#). Mediante el uso de wireshark identificar los campos de cabecera UDP usando una captura de sesión de TFTP.

## 9.5. Diferencias entre UDP y TCP

En esta sección se presentan las principales diferencias entre UDP y TCP. Para lo cual, estimado estudiante le pedimos llenar la siguiente Tabla 17 identificando en mayor detalle las diferencias entre estos protocolos.

Tabla 17. *Diferencias entre UDP y TCP.*

| DIFERENCIAS |     |
|-------------|-----|
| UDP         | TCP |
|             |     |
|             |     |
|             |     |
|             |     |

Índice

Primer bimestre

Segundo bimestre

Solucionario

Referencias bibliográficas

A continuación, se presenta una Tabla 18, con número de puerto, protocolo, aplicación y acrónimo para que sean llenadas por usted y así reforzar los conocimientos adquiridos hasta el momento.

Tabla 18. *Aplicaciones con sus números de puerto conocidos*

| Número de puerto | Protocolo | Aplicación                                             | Acrónimo |
|------------------|-----------|--------------------------------------------------------|----------|
| 20               |           | Protocolo de transferencia de archivos (datos).        | FTP      |
|                  | TCP       | Protocolo de transferencia de archivos (control).      |          |
| 22               |           |                                                        | SSH      |
| 23               |           | Telnet                                                 | X        |
|                  | TCP       |                                                        | SMTP     |
|                  |           | Servicio de nombres de dominios.                       | DNS      |
| 67               | UDP       |                                                        | DHCP     |
| 68               |           | Protocolo de configuración dinámica de host (cliente). |          |
|                  | UDP       | Protocolo de transferencia de archivos trivial.        |          |
|                  |           |                                                        | HTTP     |
|                  | TCP       |                                                        | POP3     |
|                  | TCP       | Protocolo de acceso a mensajes de Internet.            |          |
|                  |           | Protocolo de administración de redes simple.           |          |
| 443              |           |                                                        | HTTPS    |

Índice

Primer bimestre

Segundo bimestre

Solucionario

Referencias bibliográficas



## Actividades de aprendizaje recomendadas

Estimado estudiante, lo invitamos a reforzar los conocimientos adquiridos mediante la realización de los problemas propuestos en el libro al final del capítulo 3. Específicamente realizar los ejercicios desde R1 hasta R8 y los problemas P3 y P4.

Estimado estudiante, hemos llegado al final de la unidad que estudia el protocolo UDP. A continuación, lo invitamos a desarrollar la siguiente autoevaluación para que así pueda profundizar en los conocimientos adquiridos de ser el caso o pueda corroborar lo ya aprendido.

Ahora lo invitamos a revisar los conocimientos adquiridos, 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 demultiplexa en base a los puertos, si el puerto asociado al datagrama no se encuentra:
  - a. El datagrama es encolado.
  - b. El datagrama es encolado luego de generarse un comando ICMP.
  - c. El datagrama es descartado.
  - d. El datagrama es descartado luego de generarse un comando ICMP.
2. UDP demultiplexa en base a los puertos, si el puerto asociado al datagrama se encuentra:
  - a. El datagrama es encolado.
  - b. El datagrama es encolado luego de generarse un comando ICMP.
  - c. El datagrama es descartado.
  - d. El datagrama es descartado luego de generarse un comando ICMP.
3. UDP demultiplexa en base a los puertos, si el buffer se encuentra lleno:
  - a. El datagrama es encolado.
  - b. El datagrama es encolado luego de generarse un comando ICMP.
  - c. El datagrama es descartado.
  - d. El datagrama es descartado luego de generarse un comando ICMP.

4. ¿Cada puerto tiene asociada una cola?
- Verdadero.
  - Falso.
5. TCP reserva para cada puerto (socket):
- Un buffer de 8 KB.
  - Dos buffers de 8 KB.
  - Un buffer de 8 Kb.
  - Dos buffers de 8 Kb.
6. UDP reserva para cada puerto (socket):
- Un buffer de 8 KB.
  - Dos buffers de 8 KB.
  - Un buffer de 8 Kb.
  - Dos buffers de 8 Kb.
7. En UDP, el tamaño máximo del mensaje es de:
- 32 Kb.
  - 32 KB.
  - 64 Kb.
  - 64 KB.
8. El tamaño de la cabecera de UDP es de:
- 20 bytes.
  - 20 bits.
  - 8 bytes.
  - 8 bits.

Índice

Primer  
bimestre

Segundo  
bimestre

Solucionario

Referencias  
bibliográficas

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 11** | Diseñar y dimensionar escenarios de red.**Contenidos, recursos y actividades de aprendizaje**

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.

Estimado estudiante, para poder realizar un buen dimensionamiento de una red es necesario trabajar con protocolos de transferencia de datos fiable. 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.



## Semana 12



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

Estimado estudiante, una vez revisado el protocolo UDP, en esta unidad procederemos a revisar 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 revisando 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 sencillo, 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). La definición de dichas máquinas se encuentra en la sección 3.4.1., por favor, se pide revisar esta sección para poder continuar.

En la Figura 66 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 cual contiene los datos y envía el paquete al canal. Por otro lado, en el lado del receptor, se recibe un paquete, se extrae los datos del paquete y se pasan los datos a la capa superior.

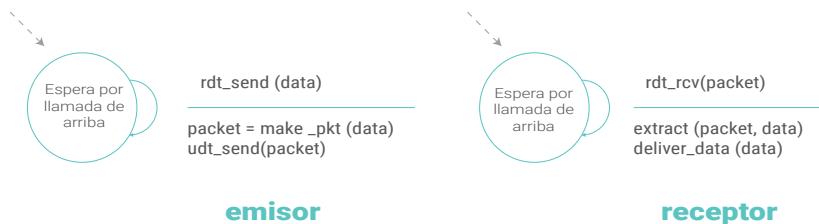


Figura 66. Protocolo para un canal fiable (Kurose & Ross, 2007)

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 ACKs, el emisor informa al receptor que el paquete llegó bien.
  - Mediante el uso de NAKs, 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 ACKs y NAKs.

Estimado estudiante, es necesario que revise la sección 3.4.1. para profundizar los contenidos de esta unidad.

### 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 ACKs. Para esto, se cuenta con suma de comprobación, número de secuencia, ACKs. 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 procede a retransmitir.

- Si, por el contrario, los datos o ACKs 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 67 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.

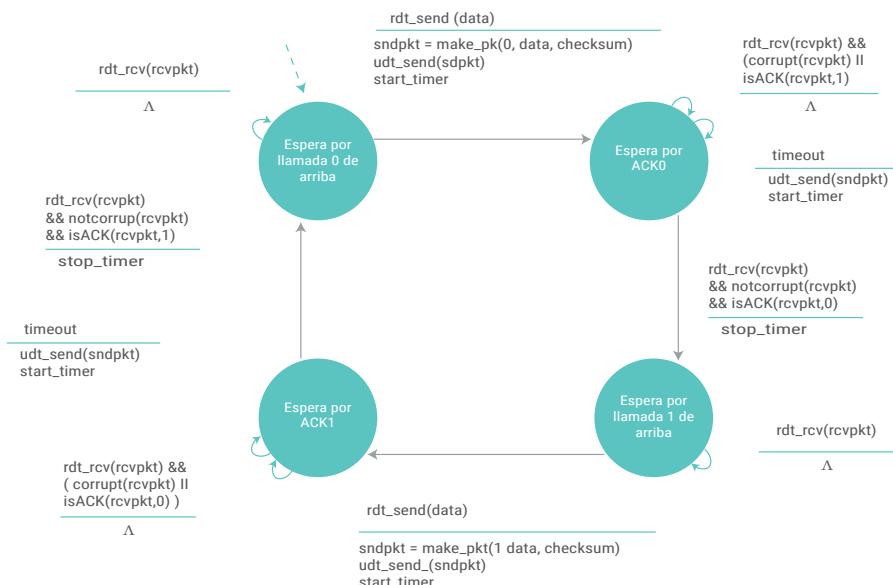


Figura 67. Máquina de estados en el lado del emisor (Kurose & Ross, 2007)



## Actividades de aprendizaje recomendadas

Se recomienda realizar una revisión de los números de secuencia y como son usados en la versión del protocolo. Además, analizar en la FSM de la versión del protocolo en qué estados se realizan los procesos de inicialización y finalización de los temporizadores.

### 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. Antes de continuar, estimado estudiante por favor lea la sección 3.4.2. del libro base.

A continuación, realizaremos 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  $L = 1000 \text{ bytes} (8000 \text{ bits})$ .

En base a los datos antes dados el tiempo necesario para transmitir el paquete por un enlace de 1 Gbps está dado por la Ecuación 1:

*Ecuación 3*

$$d_{trans} = \frac{L}{R} = \frac{8000 \text{ bits/paquete}}{10^9 \text{ bits/segundo}} = 8 \text{ microsegundos } (\mu\text{s})$$

Índice

Primer bimestre

Segundo bimestre

Solucionario

Referencias bibliográficas

En la Figura 68, 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 2:

*Ecuación 4*

$$t = RTT + \frac{L}{R} = 30,008 \text{ ms}$$

Por lo tanto, la tasa de utilización estará dada por la Ecuación 3:

*Ecuación 5*

$$U_{emisor} = \frac{\frac{L}{R}}{RTT + \frac{L}{R}} = \frac{0,008}{30,008} = 0,00027$$

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 30,008ms una tasa de transferencia efectiva de solo 267 Kbps.

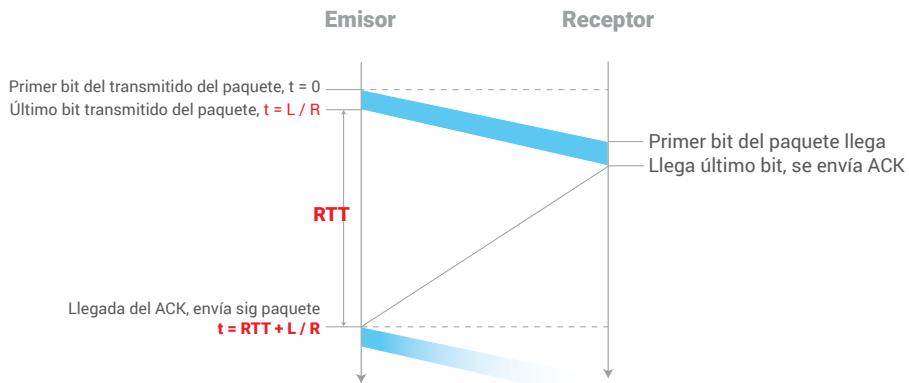


Figura 68. Protocolo de parada y espera (Kurose & Ross, 2007)

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 69.

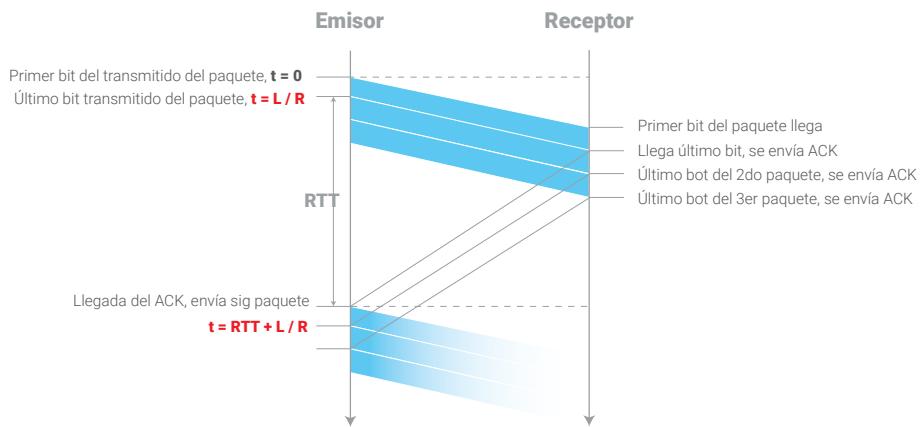


Figura 69. Protocolos con procesamiento en cadena

Observando la Figura 69, veremos que el emisor transmite tres paquetes antes de tener que esperar a los paquetes de

[Índice](#)[Primer bimestre](#)[Segundo bimestre](#)[Solucionario](#)[Referencias bibliográficas](#)

reconocimiento. En este caso, la utilización del emisor se triplica, como se indica con la siguiente Ecuación 4:

*Ecuación 6*

$$U_{emisor} = \frac{\frac{3 * L}{R}}{RTT + \frac{L}{R}} = \frac{0,024}{30,008} = 0,0008$$

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)

Estimado estudiante le invitamos a revisar la sección 3.4.3. del libro base, 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 70. 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.

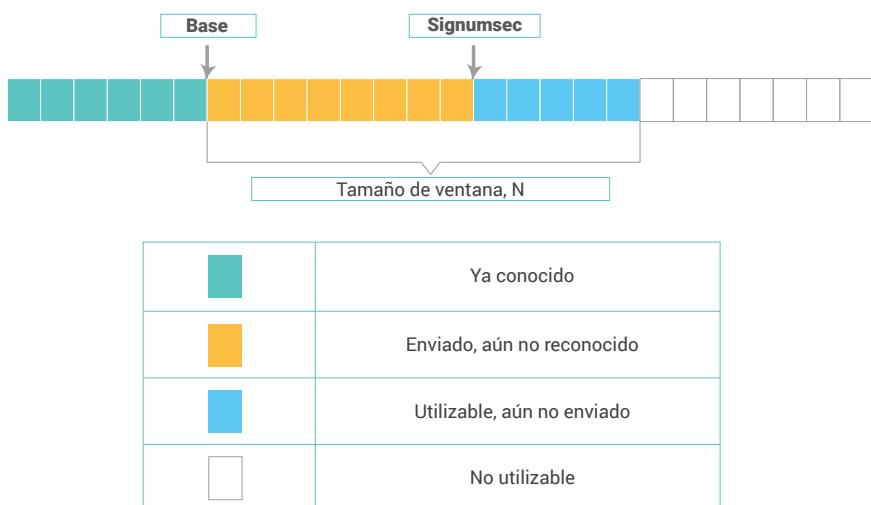


Figura 70. Números de secuencia, Retroceder  $N$



### Actividades de aprendizaje recomendadas

Estimado estudiante, existe [una herramienta en línea que le permitirá mejorar el conocimiento del protocolo GBN](#). Lo invitamos a que la revise, se familiarice con ella y aprenda el funcionamiento de la misma con respecto al protocolo GBN.

## 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.



### Actividades de aprendizaje recomendadas

Estimado estudiante, [existe una herramienta en línea que le permitirá mejorar el conocimiento del protocolo SR](#). Lo invitamos a que la revise, se familiarice con ella y aprenda el funcionamiento de la misma con respecto al protocolo SR.

En la Tabla 19 encontrará las principales características de SR.

Tabla 19. *Características del 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 temporizado por cada paquete no confirmado.                                                                                                                            |
| La ventana del emisor cuenta con:                                                 | <ul style="list-style-type: none"> <li>▪ N números de secuencia consecutivos.</li> <li>▪ Los números de secuencia de paquetes de envío se limita a los paquetes no confirmados.</li> </ul> |

Estimado estudiante, para profundizar en el funcionamiento del protocolo SR, le invitamos a revisar la sección 3.4.4. del libro base.



### Actividades de aprendizaje recomendadas

Ahora se pide que realice un mapa conceptual o una tabla resumen de los servicios que brindan los protocolos GBN y SR. En Internet encontrará gran variedad de herramientas para la realización de mapas conceptuales, por ejemplo, [la herramienta Lucidchart](#).

Hemos llegado a la parte final relacionada con los protocolos para la transferencia de datos fiable. Por lo tanto, a manera de resumen, se sugiere revisar la siguiente Figura 71 y corroborar los conocimientos adquiridos.

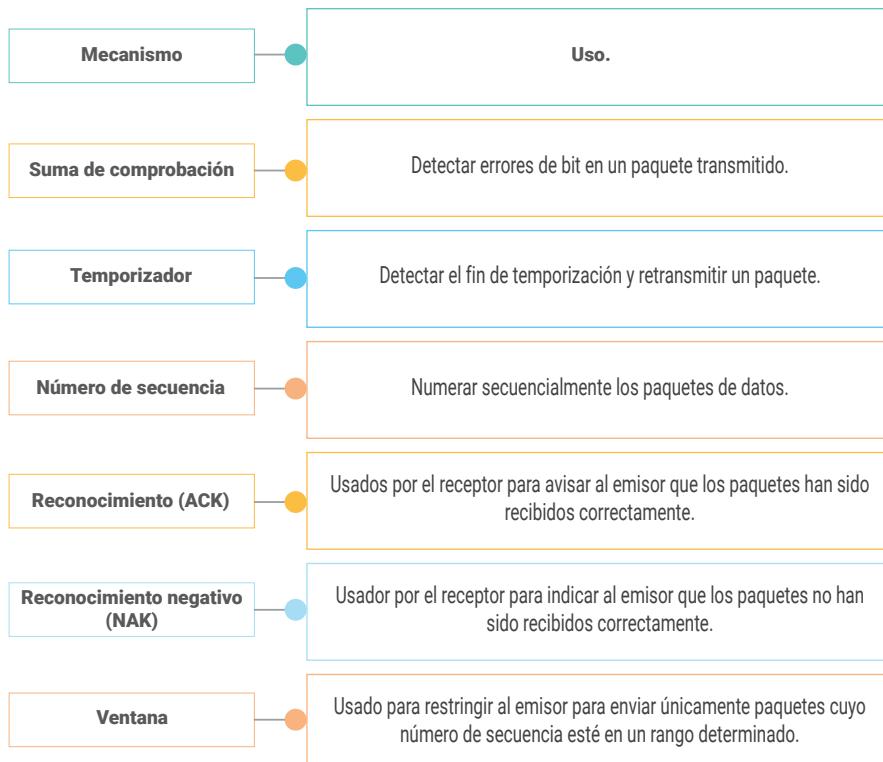


Figura 71. Resumen mecanismos de transferencia de datos fiable

Ahora lo invitamos a revisar los conocimientos adquiridos, 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.

Índice

Primer bimestre

Segundo bimestre

Solucionario

Referencias bibliográficas

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 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.

Índice

Primer bimestre

Segundo bimestre

Solucionario

Referencias bibliográficas

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.  $[0, 2^k - 1]$ .
  - b.  $[0, 2^{k-1} - 1]$ .
  - c.  $[2^k - 1, 0]$ .
  - d.  $[2^{k-1} - 1, 0]$ .

Ir al solucionario

**Resultado de aprendizaje 12** | Diseñar y dimensionar escenarios de red.

### Contenidos, recursos y actividades de aprendizaje

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.

Estimado estudiante en esta unidad revisaremos el protocolo orientado a la conexión TCP.



Lo invitamos a revisar el siguiente video sobre [TCP](#). En dicho video se presenta de manera resumida las principales características de TCP, del segmento TCP y la transferencia de datos fiable.



## Semana 13



### 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. Para esto le invitamos a revisar la sección 3.5. del libro base.

#### 11.1. Características de TCP

Estimado estudiante, a modo de resumen hemos puesto en la Tabla 20 las principales características de TCP.

Tabla 20. *Características de TCP*

|                                       |                                                                   |
|---------------------------------------|-------------------------------------------------------------------|
| <b>Punto-a-punto</b>                  | Un emisor, un receptor.                                           |
| <b>Fiable, ordenamiento por bytes</b> | Sin límites de mensajes.                                          |
| <b>Procesamiento en cadena</b>        | Esquemas de control de congestión y flujo inicializan la ventana. |
| <b>Cuenta con buffers</b>             | Para envío y recepción.                                           |

|                             |                                                                                                                                                   |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Punto-a-punto</b>        | Un emisor, un receptor.                                                                                                                           |
| <b>Datos en full-dúplex</b> | <ul style="list-style-type: none"> <li>▪ Flujo de datos bidireccional en la misma conexión.</li> <li>▪ MSS: Tamaño máximo de segmento.</li> </ul> |
| <b>Orientado a conexión</b> | Intercambio de mensajes de control, inicializan el estado del emisor y el receptor antes de intercambiar datos.                                   |
| <b>Flujo controlado</b>     | El receptor no será saturado por el emisor.                                                                                                       |

## 11.2. La conexión TCP

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

Este concepto de 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.

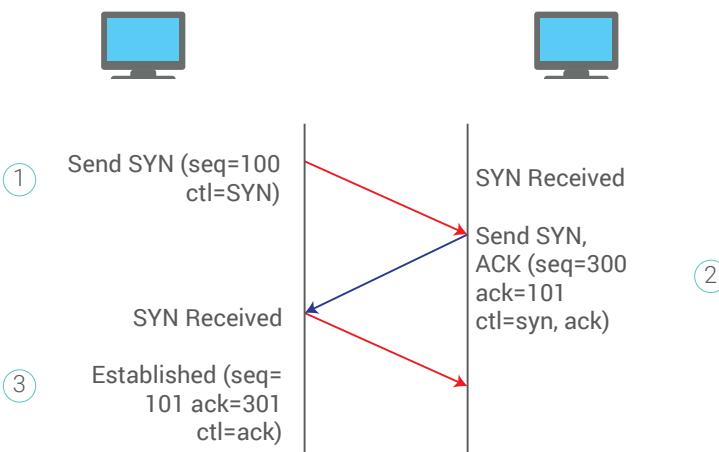
Ahora sí, estamos listos para conocer sobre la conexión TCP. Es una conexión lógica que contiene un estado en común en los niveles TCP de los dos sistemas terminales que se comunican. Una conexión TCP se caracteriza por:

- 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 72. 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.



### Actividades de aprendizaje recomendadas

En este punto es importante que usted, estimado estudiante, sepa la diferencia entre el tamaño máximo de segmento (MSS, Maximum Segment Size) y la unidad máxima de transmisión (MTU, Maximum

[Índice](#)[Primer bimestre](#)[Segundo bimestre](#)[Solucionario](#)[Referencias bibliográficas](#)

Transmission Unit). Para lo cual, le pedimos que revise la sección 3.5.1. del libro base.

### 11.3. Estructura del segmento TCP

La estructura del segmento TCP se indica en la Tabla 22. 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.



#### Actividades de aprendizaje recomendadas

Se recomienda revisar la sección 3.5.2. del libro base para conocer la función de cada campo del segmento TCP, así como también su longitud en bits.

Tabla 21. *Estructura del segmento TCP*

| Número de puerto de origen    |          |     |     |     |     |     |     |     |     |                      | Número de puerto de destino |
|-------------------------------|----------|-----|-----|-----|-----|-----|-----|-----|-----|----------------------|-----------------------------|
| Número de secuencia           |          |     |     |     |     |     |     |     |     |                      |                             |
| Número de reconocimiento      |          |     |     |     |     |     |     |     |     |                      |                             |
| Long. cabecera                | No usado | CWR | ECE | URG | ACK | PSH | RST | SYN | FIN | Ventana de recepción |                             |
| Suma de comprobación Internet |          |     |     |     |     |     |     |     |     |                      | Puntero de datos urgente    |
| Opciones                      |          |     |     |     |     |     |     |     |     |                      |                             |
| Datos                         |          |     |     |     |     |     |     |     |     |                      |                             |

### 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 la figura 3.31 del libro base, en donde se describe los números de secuencia y de reconocimiento en una aplicación Telnet simple sobre TCP. El análisis de este ejemplo le ayudará a mejorar los conocimientos adquiridos hasta el momento.

### 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.

Índice

Primer bimestre

Segundo bimestre

Solucionario

Referencias bibliográficas

#### 11.4.1. Estimación del tiempo de ida y vuelta

Se recomienda al estudiante revisar detenidamente la sección 3.5.3. del libro base. Para poder determinar el tiempo de ida y vuelta, TCP hace uso de la siguiente Ecuación 5:

*Ecuación 7*

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

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 cuanto se desvía  $RTT_{muestra}$  de  $RTT_{estimado}$ , se conoce como variación de RTT y se define mediante la Ecuación 6:

*Ecuación 8*

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

#### 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

Índice

Primer bimestre

Segundo bimestre

Solucionario

Referencias bibliográficas

de datos. Por lo tanto, el intervalo de fin de temporización de las retransmisiones está dado por la Ecuación 7:

*Ecuación 9*

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



### Actividades de aprendizaje recomendadas

Se recomienda revisar el documento RFC 6298 y ver qué valores iniciales de **IntervaloFinTemporización** se recomiendan usar.

## 11.5. Transferencia de datos fiable

Estimado estudiante, en esta sección revisaremos cómo TCP realiza una transferencia de datos fiable. De hecho, las mismas estrategias revisadas en la unidad 5 son usadas por TCP para la 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 despreocupan 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 ACKs acumulativos.
- Uso de un único temporizador de retransmisión.
- Las retransmisiones se dan por eventos de temporizador a cero y ACKs duplicados.
- Inicialmente se considera un TCP simplificado, esto es, ignorar ACKs duplicados, ignorar control de flujo y congestión de flujo.



### Actividades de aprendizaje recomendadas

Realizar un cuadro comparativo de cada uno de los escenarios de transferencia fiable que realiza TCP y que están descritos en el libro base sección 3.5.4.

Ahora lo invitamos a revisar los conocimientos adquiridos, 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.

Índice

Primer bimestre

Segundo bimestre

Solucionario

Referencias bibliográficas

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<sub>muestra</sub>.
  - b. Calcular un promedio de los valores de RTT<sub>estimado</sub>.
  - c. Calcular un promedio de los valores de RTT<sub>desv</sub>
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.

Índice

Primer  
bimestre

Segundo  
bimestre

Solucionario

Referencias  
bibliográficas

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](#)

**Resultado de aprendizaje 13** | Diseñar y dimensionar escenarios de red.**Contenidos, recursos y actividades de aprendizaje**

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**

### 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 rápido.

Es en este punto, ante la posibilidad del desbordamiento de buffer, que TCP proporciona un servicio de control de flujo a

Índice

Primer bimestre

Segundo bimestre

Solucionario

Referencias bibliográficas

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, ver sección 3.5.5 del libro base.

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 22.

Tabla 22. Variables para control de flujo en la transferencia de archivos.

|                    |                                                                                                                                       |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| 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. |

Índice

Primer bimestre

Segundo bimestre

Solucionario

Referencias bibliográficas

Recordar que en TCP no se permite el desbordamiento de buffer asignado, por lo que se debe cumplir la siguiente condición, Ecuación 8:

*Ecuación 10*

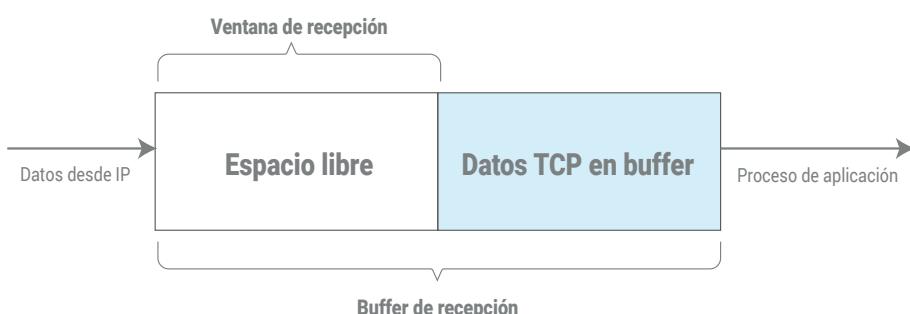
$$\text{UltimoByteRecibido} - \text{UltimoByteLeido} \leq \text{BufferRecepcion}$$

Por lo tanto, la ventana de recepción está dada por la Ecuación 9:

*Ecuación 11*

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

También se debe tener presente que la ventana de recepción es una variable dinámica, ver Figura 73.



### Actividades de aprendizaje recomendadas

En la sección 3.5.5 del libro base, página 208 revisar el párrafo que explica ¿cómo utiliza la conexión la variable VentRecepcion para proporcionar el servicio de control de flujo? Luego realice una breve explicación.

## 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 23, veremos el establecimiento de una conexión TCP mediante tres pasos (three way handshake).

Tabla 23. Proceso de acuerdo en tres fases (Kurose & Ross 2007)

|        |                                                                                                                                                                                                                                                                                                                                                                                       |  |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| Paso 1 | TCP cliente envía un segmento TCP.<br>Este segmento no contiene datos de la capa de aplicación.<br>El bit SYN de la cabecera del segmento se pone a 1.                                                                                                                                                                                                                                |  |
| Paso 2 | <ul style="list-style-type: none"> <li>▪ Extremo servidor envía un segmento al cliente que confirma (ACK) la recepción de SYN.</li> <li>▪ Este segmento no tiene datos de la capa de aplicación.</li> <li>▪ 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.</li> </ul> |  |

|        |                                                                                                                                                                                                              |  |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| Paso 3 | <ul style="list-style-type: none"> <li>Extremo cliente envía una confirmación al SYN del servidor.</li> <li>Este segmento no tiene datos de la capa de aplicación.</li> <li>Conexión establecida.</li> </ul> |  |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|

Estimado estudiante para profundizar en el tema de gestión de una conexión TCP le recomendamos revisar la sección 3.5.6 del libro base. Además, con el fin de recordar los principales conceptos de una conexión TCP le sugerimos llenar la siguiente Tabla 24.

Tabla 24. *Principales conceptos de una conexión TCP*

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

Ahora lo invitamos a revisar los conocimientos adquiridos, 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.

Índice

Primer  
bimestre

Segundo  
bimestre

Solucionario

Referencias  
bibliográficas

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.

Índice

Primer  
bimestre

Segundo  
bimestre

Solucionario

Referencias  
bibliográficas

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 venta 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](#)

**Resultado de aprendizaje 2** | Diseñar y dimensionar escenarios de red.**Contenidos, recursos y actividades de aprendizaje**

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

Estimado estudiante 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 [Control de congestión en TCP](#). En este documento se presentan algunos algoritmos del control de congestión y algunas consideraciones de seguridad.



## Semana 15



## 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. Le recordamos estimado estudiante que este tema se encuentra en la sección 3.6 del libro base.

### 12.1. Introducción a la congestión

Cuando la red se congestionada existe la pérdida de paquetes que 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 25 resumiremos los tres escenarios de congestión indicados en el libro base, sección 3.6.

Tabla 25. Escenarios de congestión

|                    |                                                                                   |                                              |
|--------------------|-----------------------------------------------------------------------------------|----------------------------------------------|
| <b>Escenario 1</b> | 2 emisores, 2 receptores.<br>1 router, buffers infinitos.<br>Sin retransmisiones. | Ante la congestión los retardos incrementan. |
|--------------------|-----------------------------------------------------------------------------------|----------------------------------------------|

|                    |                                                                                       |                                                                           |
|--------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------|
| <b>Escenario 2</b> | 1 router, buffers infinitos<br>El emisor retransmite paquetes perdidos.               | Más trabajo para los datos dados.<br>Retransmisiones innecesarias.        |
| <b>Escenario 3</b> | 4 emisores<br>Caminos multi-salto<br>Mecanismo de fin de temporización/retransmisión. | Tasa de transferencia decrece.<br>Capacidad de transmisión desperdiciada. |

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. Le sugerimos que revise la sección 3.6.2 del libro base para ampliar sus conocimientos sobre estos métodos.

### 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 RTTs.



#### Actividades de aprendizaje recomendadas

Para la mejor comprensión de los métodos de control de congestión se sugiere realizar un resumen de cada uno de ellos, para lo cual debe revisar el libro base, sección 3.6.2.

### 12.3. Mecanismo de control de congestión de TCP

En esta sección revisaremos cómo TCP realiza el control de congestión. Le recordamos al estudiante que este tema lo puede profundizar revisando la sección 3.7 del libro base.

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 75 Control de congestión según TCP.

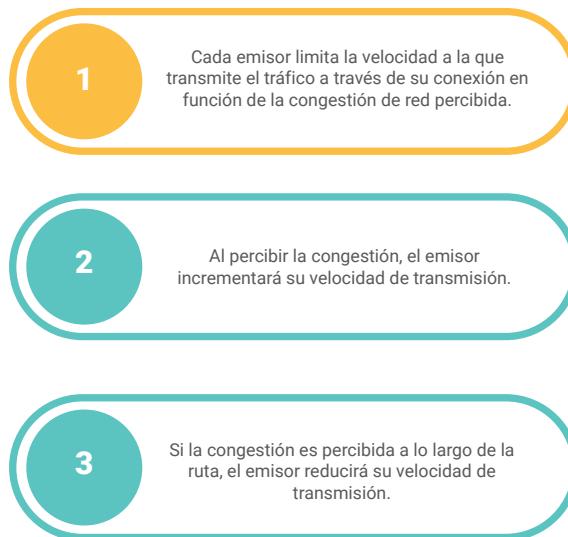


Figura 74. Control de congestión según TCP

Además, recordemos que, para poder determinar la existencia de congestión, TCP utiliza el temporizador y la recepción de tres ACKs del mismo segmento. Recuerde que:

- El temporizador finaliza indicando que el segmento se ha perdido (o ha sido descartado por los enrutadores intermedios).
- Los ACKs 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

Índice

Primer bimestre

Segundo bimestre

Solucionario

Referencias bibliográficas

de VentCongestion entre y VentRecepción, esto está definido por la Ecuación 10:

*Ecuación 12*

$$\text{UltimoByteEnviado} - \text{UltimoByteReconocido} \leq \min \{\text{VentCongestion}, \text{VentRecepcion}\}$$

Por lo tanto, la tasa de datos está dada por la Ecuación 13:

*Ecuación 13*

$$\text{tasa} = \frac{\text{VentCongestion}}{\text{RTT}} \text{ bytes/s}$$

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 ACKs 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.

Índice

Primer  
bimestre

Segundo  
bimestre

Solucionario

Referencias  
bibliográficas



## Actividades de aprendizaje recomendadas

Estimado estudiante lo invitamos a que revise el [siguiente video](#) con el fin de mejorar la comprensión del algoritmo de control de congestión de TCP.

Ahora lo invitamos a revisar los conocimientos adquiridos, 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.

Índice

Primer bimestre

Segundo bimestre

Solucionario

Referencias bibliográficas

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 ACKs 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.

Índice

Primer bimestre

Segundo bimestre

Solucionario

Referencias bibliográficas

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.
  - a. Verdadero.
  - b. Falso.
10. Al establecerse la conexión TCP, el receptor propone un tamaño de ventana en función:
  - a. Del buffer del receptor.
  - b. Del buffer del emisor.
  - c. Del tamaño de MSS.
  - d. Del tamaño del segmento.

[Ir al solucionario](#)

Índice

Primer bimestre

Segundo bimestre

Solucionario

Referencias bibliográficas



## Actividades finales del bimestre



## Semana 16

### REPASO DE UNIDADES 8-12

Estimado estudiante, 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.

Índice

Primer bimestre

Segundo bimestre

Solucionario

Referencias bibliográficas



## 4. Solucionario

Autoevaluación 1

| Pregunta | Respuesta | Retroalimentación                                                           |
|----------|-----------|-----------------------------------------------------------------------------|
| 1        | a         | Los segmentos                                                               |
| 2        | c         | Capa 3                                                                      |
| 3        | c         | A su puerta de enlace                                                       |
| 4        | b         | 20 bytes                                                                    |
| 5        | d         | 40 bytes                                                                    |
| 6        | a         | TTL (Time To Live)                                                          |
| 7        | d         | 1500 bytes                                                                  |
| 8        | a         | 48 bits                                                                     |
| 9        | b         | Falso, la dirección MAC no se puede cambiar ya que viene grabada en la NIC. |
| 10       | b         | Los paquetes IP                                                             |

Ir a la  
autoevaluación

| <b>Autoevaluación 2</b> |           |                                                                                                                                                        |
|-------------------------|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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         | 8 hexámetros                                                                                                                                           |
| 7                       | a         | 2001:DCB::3/64 es una dirección de tipo global                                                                                                         |
| 8                       | b         | Falso , ya que las direcciones link-local no pueden ser enrutadas en redes públicas.                                                                   |
| 9                       | b         | 2001:DB8::ABCD:0:0:1                                                                                                                                   |
| 10                      | c         | DHCP, es usado para asignar direcciones IPV4 de manera dinámica.                                                                                       |

Ir a la  
autoevaluación

[Índice](#)[Primer bimestre](#)[Segundo bimestre](#)[Solucionario](#)[Referencias bibliográficas](#)

| Autoevaluación 3 |           |                                                                                                                                                                                                                                                            |
|------------------|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Pregunta         | Respuesta | Retroalimentación                                                                                                                                                                                                                                          |
| 1                | b         | Falso, con VLSM se produce menos desperdicio de direcciones.                                                                                                                                                                                               |
| 2                | b         | Falso, con VLSM se tiene distinto número de hosts por subred                                                                                                                                                                                               |
| 3                | c         | 6 bits , $2^6 - 2 = 62$ hosts                                                                                                                                                                                                                              |
| 4                | a         | 4 bits, $2^4 = 16$ subredes                                                                                                                                                                                                                                |
| 5                | a         | 255.255.255.240, el prefijo /28 indica 3 octetos + 4 bits es decir 255.255.255.11110000 = 255.255.255.240                                                                                                                                                  |
| 6                | a         | 30 hosts $224 = 11100000$ , 5 bits para porción de hosts $2^5 - 2 = 30$ hosts.                                                                                                                                                                             |
| 7                | c         | 172.16.32.0 , Número mágico = $256-240= 16$ , 1ra subred 172.16.0.0/20, 2da subred 172.16.16.0/20, 3ra subred 172.16.32.0/20                                                                                                                               |
| 8                | a         | 255.255.255.248, $2^{23}-2 = 6$ hosts es decir se requieren 3 bits para la porción de host lo que dejan 5 bits para la porción de red 255.255.255.11111000.                                                                                                |
| 9                | b         | $64, /26 = 255.255.255.192$ , Número mágico = $256-192 = 64$                                                                                                                                                                                               |
| 10               | a         | 176.16.48.255, Número mágico = $256-240 = 16$ , 1ra subred: 172.16.0.0/20, 2da 172.16.16.0/20, 3ra 172.16.32.0/20, 4ta 172.16.48.0/20, luego 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](#)

Índice

Primer bimestre

Segundo bimestre

Solucionario

Referencias bibliográficas

| Autoevaluación 4 |           |                                                                                                                         |
|------------------|-----------|-------------------------------------------------------------------------------------------------------------------------|
| Pregunta         | Respuesta | Retroalimentación                                                                                                       |
| 1                | a         | Tabla de ruteo                                                                                                          |
| 2                | a         | Verdadero                                                                                                               |
| 3                | c         | falso, el enrutamiento tiene una escala de segundos                                                                     |
| 4                | b         | Analizar métricas que permiten determinar la ruta de salida                                                             |
| 5                | b         | De datos, revisar el punto 4.1.1 del texto básico.                                                                      |
| 6                | b         | Es accesible a través de otros routers                                                                                  |
| 7                | a         | Ruta predeterminada                                                                                                     |
| 8                | a         | Ruta predeterminada, los paquetes cuyo destino no encuentra en la tabla de ruteo, se envían por la ruta predeterminada. |
| 9                | c         | Se descarta el paquete, ya que no hay una ruta predeterminada.                                                          |
| 10               | a         | Serial 0/0/1, ya que la dirección de destino no está en la tabla de ruteo, se envían por la ruta predeterminada.        |

Ir a la  
autoevaluación



Índice

Primer bimestre

Segundo bimestre

Solucionario

Referencias bibliográficas

| Autoevaluación 5 |           |                                                                                                         |
|------------------|-----------|---------------------------------------------------------------------------------------------------------|
| Pregunta         | Respuesta | Retroalimentación                                                                                       |
| 1                | a         | Control por router                                                                                      |
| 2                | b         | Redes definidas por software                                                                            |
| 3                | c         | Algoritmo estado enlace                                                                                 |
| 4                | b         | Estado enlace                                                                                           |
| 5                | b         | Falso, los protocolos dinámicos no requieren intervención humana para realizar cambios en la topología. |
| 6                | a         | Control lógicamente centralizado                                                                        |
| 7                | c         | Algoritmo vector distancia                                                                              |
| 8                | c         | Todas las opciones, en el algoritmo estado o Dijkstra los nodos deben conocer toda la topología.        |
| 9                | c         | Algoritmo Bellman-Ford                                                                                  |
| 10               | c         | Comparten información hasta que no haya más información.                                                |

Ir a la  
autoevaluación



Índice

Primer bimestre

Segundo bimestre

Solucionario

Referencias bibliográficas

| Autoevaluación 6 |           |                                                                                            |
|------------------|-----------|--------------------------------------------------------------------------------------------|
| Pregunta         | Respuesta | Retroalimentación                                                                          |
| 1                | c         | Routing Information Protocol                                                               |
| 2                | b         | Falso, usa algoritmo vector distancia                                                      |
| 3                | b         | RIP V2                                                                                     |
| 4                | b         | 15 saltos                                                                                  |
| 5                | c         | 30 segundos                                                                                |
| 6                | d         | 180 segundos                                                                               |
| 7                | c         | 120, la distancia administrativa del protocolo RIP.                                        |
| 8                | b         | Ruta con menor número de saltos                                                            |
| 9                | a         | Verdadero.                                                                                 |
| 10               | a         | Falso una ruta estática tiene mayor prioridad que una ruta aprendida con el protocolo RIP. |

Ir a la  
autoevaluación

Índice

Primer bimestre

Segundo bimestre

Solucionario

Referencias bibliográficas

| Autoevaluación 7 |           |                                              |
|------------------|-----------|----------------------------------------------|
| Pregunta         | Respuesta | Retroalimentación                            |
| 1                | c         | Se usa para comunicarse al interior de un AS |
| 2                | a         | Open Shortest Path First                     |
| 3                | b         | Estado enlace                                |
| 4                | a         | Contiene información de cada vecino OSPF     |
| 5                | b         | Representar la topología de la red           |
| 6                | a         | Paquete Hello                                |
| 7                | d         | Paquete LSR                                  |
| 8                | a         | Estado Up                                    |
| 9                | c         | Area 0                                       |
| 10               | d         | Autonomous System Border Router ASBR         |

Ir a la  
autoevaluación

**Autoevaluación 8**

| Pregunta | Respuesta | Retroalimentación                                                                                                                                                                                                                                                                                                                                           |
|----------|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1        | a, b      | <p>a. Establece una sesión de comunicación temporal entre dos aplicaciones.</p> <p>b. Enlaza la capa de aplicación con capas inferiores. 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.</p> |
| 2        | c         | <p>TCP, UDP.</p> <p>Para el transporte de datos existen dos protocolos, el protocolo orientado a la conexión TCP y el protocolo no orientado a la conexión UDP.</p>                                                                                                                                                                                         |
| 3        | a         | <p>0-1023</p> <p>Los puertos bien conocidos son números que se reservan para servicios y aplicaciones.</p>                                                                                                                                                                                                                                                  |
| 4        | b         | <p>Dirección IP de destino y número de puerto de destino.</p> <p>Para crear un socket se necesitan conocer la dirección IP y el puerto destino (no el puerto de origen).</p>                                                                                                                                                                                |
| 5        | c         | <p>16 bits.</p> <p>Un número de puerto (ya sea de origen o destino, TCP o UDP) tiene una longitud de 16 bits.</p>                                                                                                                                                                                                                                           |
| 6        | a         | <p>21.</p> <p>Cada aplicación tiene un número de puerto que lo identifica, en el caso de FTP es el 21.</p>                                                                                                                                                                                                                                                  |
| 7        | a         | <p>Falso.</p> <p>En la capa de transporte se manejan segmentos.</p>                                                                                                                                                                                                                                                                                         |
| 8        | b         | <p>Mediante sockets.</p> <p>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.</p>                                                                                                                                                   |
| 9        | a         | <p>Se realiza sobre la misma conexión de transporte, además, soporta transmisiones full-dúplex.</p> <p>Esto es posible ya que TCP proporciona al nivel de aplicación un servicio full-dúplex. Lo que quiere decir que los datos pueden circular en cada sentido de forma independiente.</p>                                                                 |

Índice

Primer bimestre

Segundo bimestre

Solucionario

Referencias bibliográficas

### Autoevaluación 8

| Pregunta | Respuesta | Retroalimentación                                                                                                                                          |
|----------|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 10       | c         | <p>El número de reconocimiento del siguiente octeto que se espera recibir.</p> <p>Esto es necesario ya que cada octeto que se intercambia es numerado.</p> |

Ir a la  
autoevaluación

[Índice](#)[Primer bimestre](#)[Segundo bimestre](#)[Solucionario](#)[Referencias bibliográficas](#)

### Autoevaluación 9

| Pregunta | Respuesta | Retroalimentación                                                                                                                                                                                                                                                     |
|----------|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1        | b         | Falso.<br>DNS utiliza UDP cuando los clientes envían solicitudes a un servidor DNS.                                                                                                                                                                                   |
| 2        | c         | Puerto efímeros.<br>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         | 768.<br>En este documento se describe de forma técnica el protocolo UDP. RFC 768 es un documento de la IETF (Internet Engineering Task Force).                                                                                                                        |
| 4        | b         | Falso.<br>UDP es un protocolo de la capa de transporte no fiable.                                                                                                                                                                                                     |
| 5        | c         | 2.<br>Recuerde que el tamaño del campo es de 16 bits lo cual equivale a 2 bytes.                                                                                                                                                                                      |
| 6        | a         | Altas tasas de pérdidas entre emisor y receptor.<br>Esta pérdida de paquetes se debe a que las colas de los routers están llenas.                                                                                                                                     |
| 7        | a         | Verdadero.<br>DHCP tiene asignado el puerto 68 cuando trabaja con el protocolo UDP.                                                                                                                                                                                   |
| 8        | b         | A que UDP no establece una conexión antes de enviar los datos.<br>La baja sobrecarga que ofrece 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         | 65507 bytes en IPv4, 65527 bytes en IPv6.<br>Estos valores representan el número máximo de bytes 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. |



Índice

Primer bimestre

Segundo bimestre

Solucionario

Referencias bibliográficas

### Autoevaluación 9

| Pregunta | Respuesta | Retroalimentación                                                                                                                                                                                                                                                     |
|----------|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 10       | b, d      | <p>No protege contra la duplicación de datagramas.</p> <p>d. No provee fiabilidad.</p> <p>Ya que 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.</p> |

Ir a la  
autoevaluación

| Autoevaluación 10 |           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Pregunta          | Respuesta | Retroalimentación                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 1                 | d         | <p>El datagrama es descartado luego de generarse un comando ICMP.</p> <p>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.</p>                                                                                                                                                                                                               |
| 2                 | a         | <p>El datagrama es encolado.</p> <p>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.</p>                                                                                                                                                                                                                                                                                       |
| 3                 | c         | <p>El datagrama es descartado.</p> <p>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.</p>                                                                                                                                                                                                                      |
| 4                 | a         | <p>Verdadero.</p> <p>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.</p>                                                                                                                                                                                                                                                   |
| 5                 | a         | <p>Un buffer de 8 KB.</p> <p>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.</p>                                                                                                                                                                                              |
| 6                 | b         | <p>Dos buffers de 8 KB.</p> <p>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 o 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.</p> |

Índice

Primer bimestre

Segundo bimestre

Solucionario

Referencias bibliográficas

| Autoevaluación 10 |           |                                                                                                                                                                                                                    |
|-------------------|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Pregunta          | Respuesta | Retroalimentación                                                                                                                                                                                                  |
| 7                 | d         | 64 KB.<br>Esto representa un tamaño máximo teórico para un paquete UDP.                                                                                                                                            |
| 8                 | c         | 8 bytes.<br>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         | Falso.<br>Es falso ya que UDP puede detectar errores, pero no los puede corregir.                                                                                                                                  |
| 10                | a         | Verdadero.<br>Esto es verdadero, ya que UDP sí puede detectar errores.                                                                                                                                             |

Ir a la  
autoevaluación



[Índice](#)[Primer bimestre](#)[Segundo bimestre](#)[Solucionario](#)[Referencias bibliográficas](#)

### Autoevaluación 11

| Pregunta | Respuesta | Retroalimentación                                                                                                                                                                                           |
|----------|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1        | d         | <p>El campo de suma de comprobación.</p> <p>La suma de comprobación permite comprobar que el datagrama llega a su destino sin haber sufrido ninguna alteración.</p>                                         |
| 2        | d         | <p>Número de secuencia.</p> <p>Este número de secuencia permite que las funciones de la capa de transporte reensamble los segmentos en el mismo orden en el que fueron transmitidos.</p>                    |
| 3        | a         | <p>Verdadero.</p> <p>Los paquetes se deben guardar en buffers según sea necesario, para entregarlos en orden a la capa superior.</p>                                                                        |
| 4        | b         | <p>En un campo de longitud fija de la cabecera del paquete.</p> <p>Las cabeceras tienen por defecto una longitud fija.</p>                                                                                  |
| 5        | d         | <p>Suceso de invocación, suceso de recepción, suceso de fin de temporización.</p> <p>Son los eventos que se dan del lado del emisor cuando se usa el protocolo GBN (Go-Back-N).</p>                         |
| 6        | a         | <p>Cuando no hay errores en los bits.</p> <p>La fiabilidad se refiere a la no pérdida, no alteración y/o no duplicación de datos.</p>                                                                       |
| 7        | b         | <p>Envío de paquetes con procesamiento en cadena.</p> <p>Mediante el pipeline el emisor permite el envío de múltiples paquetes a ser reconocidos.</p>                                                       |
| 8        | a         | <p>A la asignación de números de secuencia alternados entre 0 y 1.</p> <p>Este tipo de protocolos son necesarios para proporcionar una comunicación fiable en presencia de paquetes perdidos o dañados.</p> |
| 9        | b         | <p>Fluye en ambas direcciones.</p> <p>Esto se debe a que TCP ofrece una conexión full-dúplex.</p>                                                                                                           |



Índice

Primer bimestre

Segundo bimestre

Solucionario

Referencias bibliográficas

### Autoevaluación 11

| Pregunta | Respuesta | Retroalimentación                                                                                                                                                                                                                                                                                                                                 |
|----------|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 10       | a         | <p>[0, <math>2^k - 1</math>]</p> <p>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 <math>2^{32} - 1</math>.</p> |

Ir a la  
autoevaluación

[Índice](#)[Primer bimestre](#)[Segundo bimestre](#)[Solucionario](#)[Referencias bibliográficas](#)

### Autoevaluación 12

| Pregunta | Respuesta | Retroalimentación                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1        | d         | 160 bits.<br>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         | Falso.<br>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.<br>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.<br>El campo número de reconocimiento contiene el número de secuencia del siguiente octeto que el emisor de un reconocimiento espera recibir.                                        |
| 4        | b         | Paquetes ACK enviados por el receptor al emisor.<br>TCP proporciona un servicio de transmisión fiable, considerando toda la información intercambiada durante una conexión como un flujo continuo de bytes.<br>ACK es un campo significativo de acuse de recibo.                                                                                                                                                                                                                                  |
| 5        | b, c, d   | RST. Aborta una conexión, por motivos diversos.<br>SYN. Solicita la conexión.<br>FIN. Finaliza la conexión.<br>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"><li>▪ La aplicación remitente informa a TCP que los datos tienen que enviarse inmediatamente.</li><li>▪ Informa al receptor de que los datos deben de ser pasados inmediatamente a la aplicación destino.</li></ul> 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. |

[Índice](#)[Primer bimestre](#)[Segundo bimestre](#)[Solucionario](#)[Referencias bibliográficas](#)

| Autoevaluación 12 |           |                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Pregunta          | Respuesta | Retroalimentación                                                                                                                                                                                                                                                                                                                                                                                                 |
| 7                 | a         | Calcular un promedio de valores de RTTestimado<br>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         | MSS.<br>Es el tamaño más grande de datos, se especifica en bytes.                                                                                                                                                                                                                                                                                                                                                 |
| 9                 | a         | Verdadero<br>Recuerde que el tamaño de la ventana es un campo en el encabezado<br>TCP que permite la administración de datos perdidos y el control del flujo.                                                                                                                                                                                                                                                     |
| 10                | d         | 5 bits<br>El campo de opciones TCP permite añadir campos a la cabecera con el fin de realizar las siguientes operaciones: <ul style="list-style-type: none"><li>▪ Monitorear los retrasos que experimentan los segmentos desde el origen hasta el destino.</li><li>▪ Aumentar el tamaño de la ventana.</li><li>▪ Indicar el tamaño máximo del segmento (MSS) que el origen está preparado para recibir.</li></ul> |

[Ir a la autoevaluación](#)

| Autoevaluación 13 |           |                                                                                                                                                                                                                                                                                                                |
|-------------------|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Pregunta          | Respuesta | Retroalimentación                                                                                                                                                                                                                                                                                              |
| 1                 | d         | <p>65535 octetos.</p> <p>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.</p> |
| 2                 | a         | <p>De mayor tamaño.</p> <p>La opción de factor de escala de ventana que permite extender el tamaño de la ventana más allá del límite.</p>                                                                                                                                                                      |
| 3                 | a         | <p>Verdadero.</p> <p>Con el fin de poder detectar cualquier modificación de los datos durante su transmisión, TCP calcula un Checksum que incluye en la cabecera y que verifica la integridad del segmento.</p>                                                                                                |
| 4                 | b         | <p>Al primer octeto que espera recibir.</p> <p>En donde NSI corresponde al Número de Secuencia Inicial. NSI corresponde a el número de secuencia del primer octeto de datos enviado por el nodo.</p>                                                                                                           |
| 5                 | b         | <p>Falso.</p> <p>El segmento SYN consume un número de secuencia.</p>                                                                                                                                                                                                                                           |
| 6                 | a         | <p>Uno de los dos hosts decide terminar y termina la conexión en ambos sentidos.</p> <p>Ya que la en la conexión simétrica cada host corta la conexión únicamente en el sentido que emite datos.</p>                                                                                                           |
| 7                 | a         | <p>Verdadero.</p> <p>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.</p>                                                                                            |
| 8                 | a         | <p>Verdadero.</p> <p>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.</p>                                                |

Índice

Primer bimestre

Segundo bimestre

Solucionario

Referencias bibliográficas

| Autoevaluación 13 |           |                                                                                                                                                                                                                                                    |
|-------------------|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Pregunta          | Respuesta | Retroalimentación                                                                                                                                                                                                                                  |
| 9                 | a         | Un bit de control del segmento TCP.<br>Petición de sincronismo de números de secuencia para iniciar la conexión.                                                                                                                                   |
| 10                | c         | Adapta la velocidad de transmisión a la velocidad de lectura.<br>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

| <b>Autoevaluación 14</b> |           |                                                                                                                                                                                                                                                                                                                        |
|--------------------------|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Pregunta                 | Respuesta | Retroalimentación                                                                                                                                                                                                                                                                                                      |
| 1                        | a         | Arranque lento.<br>Por lo tanto, cuando la ventana de congestión alcanza un determinado umbral la fase de arranque lento finaliza.                                                                                                                                                                                     |
| 2                        | b         | Evitación de la congestión.<br>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         | A la mitad del valor de la ventana de congestión.<br>El recibir un triple ACK duplicado significa un evento de pérdida. Esto hace que TCP reduzca la ventana de congestión.                                                                                                                                            |
| 4                        | b         | 1 MSS.<br>Luego la ventaja crecerá exponencialmente hasta cierto umbral, luego de esto crecerá linealmente.                                                                                                                                                                                                            |
| 5                        | a         | Verdadero.<br>Esto indica que el procedimiento no es demasiado lento.                                                                                                                                                                                                                                                  |
| 6                        | b         | Como máximo el valor de la ventana de congestión.<br>Considerar que el incremento máximo en el tamaño de la ventana durante un RTT será de un segmento.                                                                                                                                                                |
| 7                        | a         | 64 Kbytes.<br>Se usa arranque lento hasta llegar al valor umbral. A partir de ahí, se incrementa linealmente la ventana de congestión.                                                                                                                                                                                 |
| 8                        | 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.<br>En el control de congestión terminal a terminal, la capa de red si proporciona soporte explícito a la capa de transporte para propósitos de control de congestión. |
| 9                        | a         | Verdadero.<br>El número máximo de bytes que puede enviar el emisor es el mínimo de ambos tamaños de ventana.                                                                                                                                                                                                           |

#### Autoevaluación 14

| Pregunta | Respuesta | Retroalimentación                                                                                       |
|----------|-----------|---------------------------------------------------------------------------------------------------------|
| 10       | a         | Del buffer del receptor.<br>Ya que Internet acepta el problema que existe en la capacidad del receptor. |

Ir a la  
autoevaluación

Índice

Primer  
bimestre

Segundo  
bimestre

Solucionario

Referencias  
bibliográficas



## 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* (7ma ed.). Pearson.

Kurose, & Ross. (2007). REDES DE COMPUTADORAS. Un enfoque descendente. In *PEARSON Educación* (4ta ed.). Pearson.

Salcedo, O., Hernández, C., & Manta, H. (2010). Análisis y evaluación del routing information protocol RIP. In *Tecnura* (Vol. 14, pp. 89–108). scieloco.