
Apuntes de redes Documentation

Versión 1.0

Oscar G. G.

01 de noviembre de 2021

1. Caracterización de redes	1
1.1. Terminología: redes LAN, MAN y WAN, topologías, arquitecturas, protocolos.	1
1.2. Sistemas de numeración decimal, binario y hexadecimal.	1
1.2.1. Ejercicio: convertir a binario	1
1.2.2. Ejercicio: convertir a hexadecimal	2
1.3. Conversión entre sistemas.	2
1.4. Arquitectura de redes.	2
1.5. Encapsulamiento de la información.	2
1.6. El modelo OSI.El modelo TCP/IP.	2
1.7. Las tecnologías «Ethernet».	2
1.8. El protocolo ARP	2
1.9. El modelo OSI y «Ethernet».	3
1.10. Tipos de cableado «Ethernet».	3
1.11. Cableado estructurado: subsistemas troncales y horizontales.	3
1.12. Algoritmo de acceso al medio CSMA/CD.	3
1.13. Estructura de la trama «Ethernet».	3
2. Integración de elementos en una red	5
2.1. Los medios físicos.	5
2.1.1. Los cables metálicos (coaxial, STP y UTP).	5
2.1.2. Fibra óptica y tipos de fibra.	5
2.2. Ancho de banda y tasa de transferencia.	5
2.2.1. Analógico vs digital	6
2.2.2. Parámetros de una señal.	6
2.2.3. Modulación	6
2.2.4. Medidas	6
2.3. Factores físicos que afectan a la transmisión.	7
2.4. La conexión inalámbrica.	7
2.5. Los espectros de onda de microondas y radio.	7
2.6. Topologías.	7
2.7. Asociación y autenticación en la WLAN.	8
2.8. Dispositivos hardware en redes: hubs, APs, switches y routers	8
2.8.1. Hub	8
2.8.2. Switch	8
2.8.3. Ejemplo de simulación con switch	9
2.9. Direccionamiento.	10

2.10. Dominios de colisión y de «broadcast»	10
2.11. Direcciones IPv4 y máscaras de red.	11
2.12. Protocolos de resolución de direcciones ARP, RARP.	11
2.13. Direcciones IPv6	11
2.13.1. Representación de direcciones	11
2.13.2. Tipos de direcciones	12
2.14. Conjuntos de protocolos IPv6	13
2.15. Túneles IPv6	13
2.16. Direccionamiento dinámico (DHCP).	13
2.17. Adaptadores.	13
2.18. Adaptadores alámbricos: instalación y configuración. Adaptadores inalámbricos: instalación y configuración.	13
2.19. Monitorización de la red mediante aplicaciones que usan el protocolo SNMP.	13
2.20. Anexo: Ejercicios sobre compresión de direcciones IPv6	13
2.20.1. Soluciones a compresión de direcciones IPv6	15
2.21. Anexo: ejercicios sobre clasificación de direcciones IPv6	17
2.21.1. Soluciones a la clasificaciones de direcciones IPv6	19
3. Configuración y administración de conmutadores	21
4. Configuración y administración básica de routers	23
5. Configuración de redes virtuales VLAN	25
6. Configuración y administración de protocolos dinámicos	27
7. Configuración del acceso a Internet desde una LAN	29
8. Ejercicios propuestos para el tema 1	31
8.1. Conversión de números	31
9. Soluciones a ejercicios seleccionados	33

Caracterización de redes

1.1 Terminología: redes LAN, MAN y WAN, topologías, arquitecturas, protocolos.

Apartados 1.2.2.2 hasta 1.2.3.2

1.2 Sistemas de numeración decimal, binario y hexadecimal.

Apartado 8.1.1.5

1.2.1 Ejercicio: convertir a binario

Convertir a binario:

- 43
- 67
- 95
- 121
- 193
- 217
- 675

1.2.2 Ejercicio: convertir a hexadecimal

- 5191
- 2193
- 21430
- 39810
- 46712

1.3 Conversión entre sistemas.

Apartado 8.1.1.5

1.4 Arquitectura de redes.

Apartados 1.3.1.1 hasta 1.3.2.4

1.5 Encapsulamiento de la información.

Apartado 3.1.14

1.6 El modelo OSI.El modelo TCP/IP.

Apartado 3.2.4.2

1.7 Las tecnologías «Ethernet».

Apartados 5.1.1.1 hasta 5.3.1.2 Apartados 3.3.2.3

1.8 El protocolo ARP

Tenemos esta situación:

- Un ordenador tiene la IP 192.168.1.10
- Otro ordenador tiene la IP 192.168.1.11
- Se desea enviar un bloque de datos desde el 192.168.1.10 hacia el 192.168.1.11

Los bloques de datos **NO SE PUEDEN ENVIAR DIRECTAMENTE DE UNA IP A OTRA IP**. El ordenador 192.168.1.10 no puede enviar directamente a ese ordenador que le han dicho. PRIMERO HAY QUE AVERIGUAR LA DIRECCIÓN ETHERNET DEL 192.168.1.11.

Podrían pasar dos cosas 1. El ordenador 192.168.1.10 ya sabía de alguna manera la MAC del 192.168.1.11 2. Si no la sabe TIENE QUE PREGUNTAR.

Al protocolo que hace preguntas y respuestas traduciendo de direcciones IP a MACs se le llama **protocolo ARP (Address Resolution Protocol)**

ARP funciona así:

1. El ordenador 192.168.1.10 envía los datos a su capa Ethernet. Esta capa no sabe cuál es la MAC de ese destinatario 192.168.1.11, así que **GENERA UN PAQUETE CON UNA PREGUNTA EN LA QUE PONE ESTO**
Dirección origen: La MAC del 192.168.1.10 (por ejemplo 00-01-96-cc-59-43) Dirección destino: FF-FF-FF-FF-FF-FF
2. El paquete llega a todo el mundo, y por supuesto también al 192.168.1.11, que lo abre, ve la pregunta y por tanto construye la respuesta:
Dirección de origen: La MAC del 192.168.1.11 (por ejemplo 00.30.f2.d.6e.34) Dirección de destino: La MAC del 192.168.1.10 (00-01-96-cc-59-43)
3. El paquete de respuesta llega al que preguntó, el cual ya puede enviar los datos a la dirección Ethernet correcta.

1.9 El modelo OSI y «Ethernet».

Apartado 3.2.4.4 página 142

1.10 Tipos de cableado «Ethernet».

Cable UTP: apartado 4.2.1.3 Cable STP: apartado 4.2.1.4

1.11 Cableado estructurado: subsistemas troncales y horizontales.

1.12 Algoritmo de acceso al medio CSMA/CD.

Apartado 4.4.3.3 página 198

1.13 Estructura de la trama «Ethernet».

Apartado 4.4.4.6, página 209

2.1 Los medios físicos.

Apartado 1.2.1.4 Página 29

2.1.1 Los cables metálicos (coaxial, STP y UTP).

- Cable coaxial: apartado 4.2.1.5, página 168.
- Cable UTP: apartado 4.2.2.1, página 170.
- Cable STP: apartado 4.2.1.4, página 167.

2.1.2 Fibra óptica y tipos de fibra.

Apartado 4.2.3.3, página 176.

2.2 Ancho de banda y tasa de transferencia.

Apartado 4.1.3.2 página 162

En realidad antes de comprender el ancho de banda necesitamos comprender algunos conceptos básicos y que indicamos en los siguientes apartados

2.2.1 Analógico vs digital

- Una señal analógica es una señal en la que aceptamos cualquier valor.
- Una señal digital es una en la que solo se aceptan ciertos valores.

2.2.2 Parámetros de una señal.

- Se llama amplitud a la altura de una onda. Cabe destacar que por altura nos referimos a la distancia entre el punto más alto y más bajo de una señal.
- Se llama longitud de onda a la distancia que recorre una señal entera. Se mide en metros (o mm, o hasta nanómetros)
- Se llama fase al punto donde empieza y acaba la onda, que no tiene por qué ser siempre el punto 0 o el punto más alto.

2.2.3 Modulación

Modificar parámetros de una señal para enviar 0 y 1. Si combinamos la modificación de muchos parámetros conseguiremos enviar más bits por segundo, pero la recepción se vuelve algo muy complejo.

2.2.4 Medidas

En informática, en general $1K=1024$. Sin embargo, en redes, las medidas como $1=1000$. Por tanto si nos hablan de una conexión de 300Mbps, se refieren a $300 \cdot 10^6$. Además se debe recordar que:

- «b» (en minúscula) se refiere a *bits*.
- «B» (en mayúscula) se refiere a *bytes*.

Pero ¿entonces qué es el ancho de banda? Se define como la diferencia entre la frecuencia máxima que se acepta y la frecuencia mínima. Cuanto más ancha sea esa banda, más datos podremos meter. No es lo mismo que la *velocidad*.

La diferencia entre el ancho de banda y la velocidad, es lo que llamamos *rendimiento*, que se mide en porcentaje y nunca es del 100 %

- Si tenemos una fibra de 600Mbps, y perdemos el 8 % en protocolos, ¿a qué velocidad nos descargaremos un archivo?

Si pierdo el 8 %, conservamos el 92, es decir $0.92 \cdot 600 = 552$ Mbps. Si un archivo ocupa 400MB, entonces ocupa $400 \cdot 8$ Mb, es decir 3200Mb, que en realidad es $3200 \cdot 1024$ Kb, o lo que es lo mismo $3200 \cdot 1024 \cdot 1024$ bits, o sea 3.355.443.200 bits. Si queremos descargar esos 3.355.443.200 bits en una fibra de 552Mbps, aún tendremos que convertir 552 «medidas estándar», es decir 552.000.000 bits por segundo.

Conclusión: si dividimos 3.355.443.200 bits por 552.000.000 obtenemos 6,078 segundos.

2.3 Factores físicos que afectan a la transmisión.

2.4 La conexión inalámbrica.

Se han popularizado mucho por ofrecer una ventaja inexistente en otros medios: la movilidad. Las redes Wifi usan el estándar 802.11, del cual ha habido muchas variantes:

- 802.11a), fue el primero, que ofrecía un máximo de 11Mbps, un alcance de unos pocos metros.
- 802.11n) ofrece mucha más velocidad y alcance.

Aparte de eso, las redes Wifi son más inseguras.

Un detalle muy sutil es que en ocasiones los usuarios usan la clave correcta en la red equivocada.

Si nuestro portátil tiene una tarjeta WiFi 802.11n) y nuestro router wifi resulta ser 802.11 a) ambos dispositivos cambian automáticamente al protocolo más compatible, que será el más lento.

Toda red Wifi tiene un identificador llamado SSID. La costumbre es que los nodos difundan el nombre. Sin embargo no es obligatorio, puede activarse una opción con un nombre parecido a este «Not broadcast SSID»

Hay muchos tipos de conexiones:

- Wifi: conexión doméstica, con alcance alto y una velocidad alta.
- Bluetooth: punto a punto, velocidad baja y un alcance bajo, consume muy poca energía.
- 4G, 5G.

2.5 Los espectros de onda de microondas y radio.

Apartado...

2.6 Topologías.

- Bus: los equipos forman una línea y cada equipo tiene que averiguar al principio qué ordenadores están a su izquierda y cuales a su derecha. **Obsoleto**
- Anillo: antiguo, los equipos se conectaban en círculo y había un sentido de giro en el envío de paquetes, el sistema era un poco mejor, pero los cortes en el cable producían errores en toda la red. **Muy improbable que sigan usándose.**
- Estrella: la conexión de los cables implica conectar todos los dispositivos a un punto central que retransmite los datos el equipo correcto. **Es prácticamente el único sistema que queda en uso**

2.7 Asociación y autenticación en la WLAN.

Se llama «autenticación» al proceso seguido por un punto de acceso para ver si un equipo va a tener permiso para enviar y recibir datos a través de ese punto de acceso.

Se llama «asociación» al proceso por el cual un dispositivo utiliza el permiso concedido en el punto anterior para enviar y recibir datos.

Dentro de los sistemas de autenticación:

- Deshabilitado: cualquier puede asociarse al punto de acceso y transmitir y recibir.
- WEP (Wire Equivalent Privacy) usa un sistema de cifrado y un sistema de claves. Quien proporcione la clave correcta podrá asociarse al punto de acceso y enviar y recibir datos cifrados con una clave del router.
- WPA: usa un cifrado más potente y mucho más difícil de romper que WEP.
- WPA2: va aún más lejos y ofrece una seguridad mucho mayor.

WEP, WPA y WPA2 suelen basarse un sistema llamado PSK (Pre-Shared Key o clave pre-compartida). En estos casos ponemos una clave en los router/puntos de acceso que luego también pondremos en los ordenadores. Estos sistemas suelen llamarse WPA-PSK y WPA2-PSK.

Existe una variante: WPA, WPA2 usan un tercer equipo que actúa de servidor de autenticación.

En todos los sistemas de autenticación ocurre lo siguiente: * Los sistemas de cifrado pueden ser más potentes o más débiles. Los más potentes implican velocidades más lentas al gastar más tiempo en el cifrado y descifrado. * Una vez que un dispositivo envía una petición de conexión el router/punto de acceso envía una petición de clave. * Si el dispositivo envía una clave correcta, el router envía una clave de cifrado que se usará durante toda la sesión.

2.8 Dispositivos hardware en redes: hubs, APs, switches y routers

Dispositivos hay muchos, pero no todos ellos trabajan en la misma capa de red.

2.8.1 Hub

Un hub o concentrador es un dispositivo «tonto», cualquier paquete que reciba lo difunde por todos los puertos Ethernet. Por lo tanto es un dispositivo de capa de enlace.

2.8.2 Switch

Un switch es un dispositivo con un software incorporado que ejecuta un programa que apoyándose en una memoria RAM interna consigue enviar los paquetes **solo al destinatario correcto**. En un pequeño número sí generará colisiones, pero su número es muchísimo menor que el de un hub.

2.8.3 Ejemplo de simulación con switch

Supongamos que tenemos un switch. Supongamos que tenemos tres ordenadores:

- Ordenador con IP 192.168.1.20 con MAC 0A conectado al puerto 2 del switch.
- Ordenador con IP 192.168.1.21 con MAC 0B conectado al puerto 5 del switch.
- Ordenador con IP 192.168.1.22 con MAC 0C conectado al puerto 9 del switch.

Al principio la tabla del switch está en este estado:

Puerto	Mac
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	

Ahora supongamos que en el 192.168.1.20 envía un ping al 192.168.1.22. El 192.168.1.20 mete el mensaje (que llevará la MAC de origen 0A dentro) en su cable que llega al switch.

El switch se encuentra con dos cosas:

1. No sabe en qué puerto está el ordenador 0C que es el destinatario final: **no tendrá más remedio que enviar ese paquete por todos los puertos menos por donde vino**
2. El switch acaba de aprender y apuntar en su tabla que el ordenador con la MAC 0A está en el puerto 2, así que ahora la tabla del switch queda como sigue:

Puerto	Mac
0	
1	
2	0A
3	
4	
5	
6	
7	
8	
9	

El mensaje llegará a todos los ordenadores y casi todos lo descartarán pero el «ping» llegará correctamente al 0C el cual enviará un mensaje de respuesta usando como MAC de origen 0C. Ese mensaje llega al switch que ahora se encuentra con dos cosas:

1. El ordenador con la MAC 0C está conectado al puerto 9, así que ese conocimiento nuevo se apunta en la tabla quedará como sigue:

Puerto	Mac
0	
1	
2	0A
3	
4	
5	
6	
7	
8	
9	0C

2. El switch sabe que tiene que enviar un paquete al 0A así que analiza su tabla de direcciones. Al analizar su tabla y observar que tiene apunta que ese destinatario 0A está en el puerto 2 **EL PAQUETE SE ENVÍA SOLO POR EL PUERTO CORRECTO** sin generar colisiones en otros puntos de la red.

2.9 Direccionamiento.

Hasta ahora hemos visto que hay muchas capas de red: enlace, red, transporte, aplicación. Cada capa tiene su propio sistema de direcciones:

- En Ethernet hemos aprendido que las direcciones son de 48 bits, que se escriben como parejas de números hexadecimales, por ejemplo 3a:d1:f3:55:a8:10. Se debe recordar que hay una dirección Ethernet especial llamada «dirección de broadcast» o «dirección de difusión». Cuando un dispositivo quiere enviar un mensaje a toda la red, pone la dirección ff:ff:ff:ff:ff:ff como dirección de destino. Esto se hace por ejemplo en ARP cuando un ordenador quiere averiguar la MAC teniendo solo su IP. Los switches SIEMPRE OBEDECEN ESAS DIFUSIONES.
- Si hay muchos sistemas de direcciones siempre va a ser necesario «traducir entre ellos». Y por ejemplo ya conocemos ARP (Address Resolution Protocol), el cual dada una IP usa difusiones para averiguar la MAC de dicho ordenador con esa IP.

Ethernet en realidad divide la MAC en dos partes: los tres primeros pares son el código de fabricante. Los tres últimos son el número de la tarjeta.

2.10 Dominios de colisión y de «broadcast».

- Se llama «dominio de colisión» al conjunto de equipos que son susceptibles de provocarse colisiones mutuamente. En general es mucho mejor para el rendimiento el tener muchos dominios pequeños en lugar de uno grande.
- Dominio de broadcast o dominio de difusión es el conjunto de ordenadores que reciben las difusiones de un ordenador.

Un dominio de difusión **NO TIENE POR QUÉ COINCIDIR** con el dominio de colisiones en una red.

2.11 Direcciones IPv4 y máscaras de red.

Las direcciones IP son las direcciones de la capa software de red más extendida. La capa de red va a ser capaz de enviar datos a sitios remotos. Las direcciones IP están pensadas para poder distinguir un dispositivo cualquiera de cualquier otro del mundo.

Las direcciones IP son software, son un parámetro de configuración. La capa de red sirve como «abstracción» de la capa de enlace Ethernet.

En esencia una dirección IP es una secuencia binaria de 32 bits, como esta:

10010000.11110001.01110011.10101011

Como son muy poco prácticas de manejar y recordar, se suele permitir el escribirlas como números en decimal separados por un punto.

- El primer byte de la dirección dada es 10010000, que en decimal es 144.
- El segundo byte es 11110001, que en decimal es 241.
- El tercer byte es 01110011, que en decimal es 115.
- El cuarto byte es 10101011, que en decimal es 171.

Por tanto esa IP era 144.241.115.171.

La idea original era que con 32 bits se podrían tener 2 a la 32 equipos, es decir 4.294.967.296 ordenadores.

Como aparentemente había direcciones de sobra, se decidió asignarlas en bloques. Como una IP debe servir para poner número a las redes, y dentro de las redes poner número a cada equipo de esa red, se decidió utilizar siempre una secuencia llamada máscara para poder distinguir cual es el número de red y cual es el número de host.

Supongamos que en un cierto sitio se tiene una red. Si en un ordenador nos han dado una secuencia de bits como la de arriba 10010000.11110001.01110011.10101011 (que en decimal era 144.241.115.171) ¿como saber cual es la parte de red y la parte de host. La clave es mirar ese parámetro llamado máscara. Supongamos que esa máscara es 255.0.0.0. Si la pasamos a binario sale que la máscara es 11111111.00000000.00000000.00000000.

Num de red	Número de host
10010000	11110001.01110011.10101011

2.12 Protocolos de resolución de direcciones ARP, RARP.

2.13 Direcciones IPv6

2.13.1 Representación de direcciones

Dadas las limitaciones en las direcciones IPv4 se diseñó un nuevo formato de direcciones en el que hubiera muchas más posibilidades: **IPv6** En IPv6 hay *128 bits para direcciones* lo que supone un espacio de direcciones de 2 elevado a 128, un número realmente grande. Las direcciones IPv6 se escriben como secuencias de 8 grupos de 4 hexadecimales separadas por dos puntos, a continuación vemos algunos ejemplos:

```
fe80:a13d:d3d6:a190:31d2:a216:3261:1800
3410:0000:0000:0000:0000:0000:0000:2900
```

El segundo ejemplo muestra algo interesante y además muy habitual: **la mayor parte de las veces una dirección IPv6 tendrá muchos ceros consecutivos**. En ese caso, se puede abreviar esa dirección eliminando las secuencias de

ceros **pero dejando un «doble dos puntos»** para indicar que hemos recortado una IPv6, así tendríamos que la última dirección la podemos escribir así:

```
3410:0000:0000:0000:0000:0000:2900 (sin abreviar)
3410::2900 (abreviada)
```

Pero ¡cuidado! esta abreviatura debe hacerse con cuidado. Supongamos una IPv6 como esta:

```
5199:0000:0000:1767:0000:0000:00a5
```

Obsérvese que tenemos dos secuencias de ceros. Una de 8 ceros y otra de 12 ceros. La pregunta típica es ¿puedo abreviar ambos bloques? La respuesta es **NO**. Si escribiéramos la IPv6 así:

```
5199::1767::00a5
```

entonces ocurriría que **la máquina no podría nunca saber cuantos ceros hay en cada bloque abreviado**. Por ello haremos lo siguiente:

1. El bloque más grande de ceros, lo eliminaremos y pondremos el «doble dos puntos».
2. El bloque de ceros más pequeño se «recorta» dejándolo con un solo cero por bloque.
3. Si algun bloque tiene ceros por la izquierda se pueden eliminar (igual que en la vida real da igual escribir 15 que 0015)

Así la dirección IPv6 5199:0000:0000:1767:0000:0000:00a5

1. Se recorta primero por el bloque de ceros de la derecha y queda 5199:0000:0000:1767::00a5
2. Y el 5199:0000:0000:1767::00a5 se recorta de nuevo en los ceros de la izquierda para quedar como 5199:0:0:1767::00a5
3. Por último observamos que en el bloque final hay un 00a5 que se puede escribir como a5, así que nuestra dirección queda finalmente como 5199:0:0:1767::a5

2.13.2 Tipos de direcciones

Hay tres tipos básicos de direcciones IPv6: unicast, anycast y multicast.

- Las direcciones unicast son direcciones que indican una única conexión en todo Internet. Son las direcciones más comunes
- Las direcciones anycast se usan por lo administradores para «formar grupos». En anycast habrá muchas máquinas con la mismo IPv6 anycast pero cuando se envíe algo a esa dirección anycast **solo se enviará a uno de ellos**. Los router se encargarán de entregarlo a la máquina más cerca que tenga esa dirección anycast.
- Las direcciones multicast se usan en casos en los que varios nodos van a tener una misma IPv6 y cuando se envíe algo a esa IPv6 **todos la recibirán**.

Las direcciones reservadas por el IETF son las siguientes:

Uso	Prefijo	Primera IPv6	Última IPv6	Fracción que ocupa
Unicast global	2000::/3	2000::/3	3fff::/3	1/8
Unicast local único	fc00::/7	fc00::/7	fdff::/7	1/128
Unicast local en enlace	fe80::/10	fe80::/10	febf::/10	1/1024
Multicast	ff00::/8	ff00::/8	ffff::/8	1/256

2.14 Conjuntos de protocolos IPv6

2.15 Túneles IPv6

2.16 Direccionamiento dinámico (DHCP).

2.17 Adaptadores.

2.18 Adaptadores alámbricos: instalación y configuración. Adaptadores inalámbricos: instalación y configuración.

2.19 Monitorización de la red mediante aplicaciones que usan el protocolo SNMP.

2.20 Anexo: Ejercicios sobre compresión de direcciones IPv6

Comprimir las direcciones IPv6 siguientes según las reglas de compresión del protocolo (las soluciones aparecen al final):

Tabla 1: Ejercicios propuestos IPv6

Num ejercicio	IPv6
1	e9f9:ba67:0000:f4e8:0000:b344:0000:77ce
2	1105:9002:08f6:d492:0000:810e:6fe2:26e9
3	0000:7cec:7cf3:0000:8874:0000:4df7:0000
4	3539:0000:0000:0000:0000:1001:0000:0000
5	0000:0000:942c:238f:0000:0000:5457:911e
6	0000:ec1b:1252:bc77:a392:364b:5d89:938b
7	84c1:79a9:2635:0000:0000:0000:0000:0000
8	0000:0000:0000:1f29:0348:0000:af6c:9306
9	3261:0000:77be:4c86:b322:0000:0000:5c8b
10	2749:0000:0000:0000:0000:03bb:df01:0000
11	0000:0000:b753:0000:0000:0000:0000:ec7f
12	0000:dd97:0000:2c00:0000:8ac8:0000:b783
13	0000:0000:0000:0000:b4aa:12c0:47a0:0000
14	f310:0000:0000:0000:0000:b63a:0000:0000
15	0000:0000:412a:0000:0000:2403:0000:3a00
16	0000:67fa:bd62:c27c:0000:0000:0000:f1af
17	0000:0000:5211:9028:0000:b9d0:b78b:0000
18	0000:3d58:0000:aa0a:7371:0000:0000:c0a6
19	45a2:e709:0000:0000:7373:746b:0000:dc24
20	9c47:0000:0000:0000:6413:3ed8:0000:0000
21	d43e:0000:0000:4de7:0000:754c:d79b:0000
22	3e9f:0000:0000:0000:0000:db5f:0000:0000
23	dab7:0000:b129:4837:0000:e8bb:cd1d:235c
24	ec0c:48b6:0000:0000:0000:0000:0000:0000

continué en la próxima página

Tabla 1 – proviene de la página anterior

Num ejercicio	IPv6
25	3633:8915:39f5:0000:0000:0d82:0000:0000
26	0000:af51:13a0:0000:fc84:f114:9af0:b988
27	73b6:55f0:0000:0000:0000:0000:0000:b887
28	0663:0000:4704:3132:0000:2f36:0000:d0ca
29	0000:0000:f66d:0000:b973:0000:0f5c:0000
30	cda2:0000:7f62:07fa:c569:0000:ee8f:740c
31	e75a:0000:f7cc:a6ca:5b28:0000:8d59:0000
32	c449:ea16:8e11:7d22:0000:0000:0000:5fa8
33	0000:0000:9a7a:d7a3:1b61:0000:0000:cd22
34	0000:0000:8b6c:293f:0000:0000:0000:d90c
35	f8d4:0000:0000:4fd3:0000:0000:1837:0000
36	0000:fb07:0000:0000:0000:d783:a576:f695
37	0000:0000:4cc9:fb0c:0000:0000:0000:3bd9
38	60fe:0000:0000:7c56:0000:0000:c619:0000
39	ccb3:0000:c821:0000:0000:0000:0000:c74c
40	0000:0000:0b95:21ea:0000:0000:0000:0000
41	0000:0000:c009:0000:4f26:0000:affb:53f3
42	0000:dcd2:71be:0000:734d:2e61:0000:9881
43	bae4:eb02:0000:f41a:145d:bb47:0000:0000
44	0000:0000:0000:0000:0000:740c:0000:1741
45	0000:0000:0000:0000:7cd8:1e15:c90f:ae1b
46	241c:8bb2:a902:dc92:1333:4bfb:0000:56c3
47	ec1f:2794:38cd:0000:e5f8:0000:c2cc:898c
48	86a3:f3ec:0000:0000:0000:c93a:b47c:0000
49	0000:c570:e19b:681a:0615:0000:0000:0000
50	0000:dc4e:0000:0000:0000:0000:0000:8ffd
51	4ecb:68e9:e08d:a371:0000:0000:0000:0000
52	0000:0000:0000:64b2:0000:7e75:8bb1:ec30
53	a7e1:6747:0bb4:0000:0000:0000:5bd7:0000
54	1803:0000:0000:0000:33e5:4828:0000:e00c
55	0000:e083:0000:df9f:4d92:0000:0000:477d
56	2001:0000:0000:f007:781f:0000:c2d5:a767
57	0000:94e8:0000:5a26:a616:b790:0000:d238
58	0000:1a4b:fd0e:0000:0000:e929:0000:0000
59	5c77:da9a:3305:39eb:0000:ade2:0750:7450
60	7d09:0000:9d50:0000:33dc:0000:0000:445b
61	4b1a:0000:fd0b:f0c5:86be:0000:551c:0000
62	589e:0000:53c7:93e3:0000:0000:12e9:093c
63	0000:3616:0000:8509:368f:6ffa:0000:0000
64	78cc:20e9:00e5:f0a9:eac3:0000:0000:0000
65	0000:0000:4d06:0000:0000:0000:b1dd:0000
66	0000:0000:0000:e4bf:0d24:d134:0b2a:100a
67	0000:0000:0000:0000:0000:0000:9159:8768
68	0000:0000:0000:d4b0:bea8:0000:abdb:f2f7
69	dc62:0000:5b76:0000:01e3:77fb:0000:0000
70	0000:c781:0000:f950:0000:2451:7b8a:0000
71	4deb:e14c:c9b0:e65c:2265:0000:0000:29b3
72	0000:3ebe:5d28:0000:7697:0000:0000:1708
73	0000:0000:0000:f141:0000:215a:0000:0000

continué en la próxima página

Tabla 1 – proviene de la página anterior

Num ejercicio	IPv6
74	e64a:ff9f:eb7c:923b:3a5f:0000:0000:0000
75	36a8:58be:9b67:be76:66c3:0000:90a5:0000
76	b096:0000:0000:0000:7291:0000:eeef:0000
77	0000:0000:036c:0000:e583:d41a:956c:394f
78	79e4:8350:0000:6d5b:cac2:0000:dd6b:e62a
79	34f5:0000:2ecb:0000:0000:27c6:0000:0000
80	b2d2:b338:0000:0000:3160:20bc:f4e6:5878
81	0000:0000:0000:4ddc:0000:1646:d72c:0000
82	0000:e0bb:111c:0000:0000:6fd4:0000:8891
83	c04b:0000:0000:bac7:0000:e028:0000:c8e5
84	f680:0000:0000:0000:0000:0000:dfa9:0000
85	e19b:0000:101a:3fcc:ae97:0000:7970:f214
86	50c1:9e9c:0000:0000:ed17:0000:8e99:0000
87	0000:ab50:4066:2809:f314:0000:92da:0000
88	ff48:0000:0000:22e7:9656:0000:0000:0000
89	0000:0000:0000:0000:0000:0000:14a5:0000
90	8d13:0000:237a:c4d7:0000:0000:4df0:c8d0
91	4a7e:caaa:0000:0000:ec08:ce1f:0000:0000
92	1c21:0000:0000:0000:0000:0000:e5c0:fc84
93	0000:0000:32da:419f:0000:5b69:dad0:bc58
94	e73c:b036:3efd:0000:0000:0d87:0000:6197
95	0000:0000:0000:5bb0:bf99:0000:a21e:0000
96	0000:9a47:5197:a901:0000:0000:3ac3:39c8
97	0000:14e3:0000:0000:06d0:e328:20a4:ea05
98	d9b4:e5de:7478:a8ac:2a19:3ef6:a970:0000
99	dcd1:0000:a0df:0000:0000:f58a:0000:f323
100	0000:021d:64f1:df12:e8ac:0000:489f:75a0

2.20.1 Soluciones a compresión de direcciones IPv6

A continuación se muestran las soluciones a los ejercicios propuestos:

Tabla 2: Ejercicios resueltos IPv6

Num ejercicio	IPv6	Comprimida
1	e9f9:ba67:0000:f4e8:0000:b344:0000:77ce	e9f9:ba67:0:f4e8:0:b344:0:77ce
2	1105:9002:08f6:d492:0000:810e:6fe2:26e9	1105:9002:8f6:d492:0:810e:6fe2:26e9
3	0000:7cec:7cf3:0000:8874:0000:4df7:0000	0:7cec:7cf3:0:8874:0:4df7:0
4	3539:0000:0000:0000:0000:1001:0000:0000	3539::1001:0:0
5	0000:0000:942c:238f:0000:0000:5457:911e	::942c:238f:0:0:5457:911e
6	0000:ec1b:1252:bc77:a392:364b:5d89:938b	0:ec1b:1252:bc77:a392:364b:5d89:938b
7	84c1:79a9:2635:0000:0000:0000:0000:0000	84c1:79a9:2635::
8	0000:0000:0000:1f29:0348:0000:af6c:9306	::1f29:348:0:af6c:9306
9	3261:0000:77be:4c86:b322:0000:0000:5c8b	3261:0:77be:4c86:b322::5c8b
10	2749:0000:0000:0000:0000:03bb:df01:0000	2749::3bb:df01:0
11	0000:0000:b753:0000:0000:0000:0000:ec7f	0:0:b753::ec7f
12	0000:dd97:0000:2c00:0000:8ac8:0000:b783	0:dd97:0:2c00:0:8ac8:0:b783
13	0000:0000:0000:0000:b4aa:12c0:47a0:0000	::b4aa:12c0:47a0:0
14	f310:0000:0000:0000:0000:b63a:0000:0000	f310::b63a:0:0

continué en la próxima página

Tabla 2 – proviene de la página anterior

Num ejercicio	IPv6	Comprimida
15	0000:0000:412a:0000:0000:2403:0000:3a00	::412a:0:0:2403:0:3a00
16	0000:67fa:bd62:c27c:0000:0000:0000:f1af	0:67fa:bd62:c27c::f1af
17	0000:0000:5211:9028:0000:b9d0:b78b:0000	::5211:9028:0:b9d0:b78b:0
18	0000:3d58:0000:aa0a:7371:0000:0000:c0a6	0:3d58:0:aa0a:7371::c0a6
19	45a2:e709:0000:0000:7373:746b:0000:dc24	45a2:e709::7373:746b:0:dc24
20	9c47:0000:0000:0000:6413:3ed8:0000:0000	9c47::6413:3ed8:0:0
21	d43e:0000:0000:4de7:0000:754c:d79b:0000	d43e::4de7:0:754c:d79b:0
22	3e9f:0000:0000:0000:0000:db5f:0000:0000	3e9f::db5f:0:0
23	dab7:0000:b129:4837:0000:e8bb:cd1d:235c	dab7:0:b129:4837:0:e8bb:cd1d:235c
24	ec0c:48b6:0000:0000:0000:0000:0000:0000	ec0c:48b6::
25	3633:8915:39f5:0000:0000:0d82:0000:0000	3633:8915:39f5::d82:0:0
26	0000:af51:13a0:0000:fc84:f114:9af0:b988	0:af51:13a0:0:fc84:f114:9af0:b988
27	73b6:55f0:0000:0000:0000:0000:0000:b887	73b6:55f0::b887
28	0663:0000:4704:3132:0000:2f36:0000:d0ca	663:0:4704:3132:0:2f36:0:d0ca
29	0000:0000:f66d:0000:b973:0000:0f5c:0000	::f66d:0:b973:0:f5c:0
30	cda2:0000:7f62:07fa:c569:0000:ee8f:740c	cda2:0:7f62:7fa:c569:0:ee8f:740c
31	e75a:0000:f7cc:a6ca:5b28:0000:8d59:0000	e75a:0:f7cc:a6ca:5b28:0:8d59:0
32	c449:ea16:8e11:7d22:0000:0000:0000:5fa8	c449:ea16:8e11:7d22::5fa8
33	0000:0000:9a7a:d7a3:1b61:0000:0000:cd22	::9a7a:d7a3:1b61:0:0:cd22
34	0000:0000:8b6c:293f:0000:0000:0000:d90c	0:0:8b6c:293f::d90c
35	f8d4:0000:0000:4fd3:0000:0000:1837:0000	f8d4::4fd3:0:0:1837:0
36	0000:fb07:0000:0000:0000:d783:a576:f695	0:fb07::d783:a576:f695
37	0000:0000:4cc9:fb0c:0000:0000:0000:3bd9	0:0:4cc9:fb0c::3bd9
38	60fe:0000:0000:7c56:0000:0000:c619:0000	60fe::7c56:0:0:c619:0
39	ccb3:0000:c821:0000:0000:0000:0000:c74c	ccb3:0:c821::c74c
40	0000:0000:0b95:21ea:0000:0000:0000:0000	0:0:b95:21ea::
41	0000:0000:c009:0000:4f26:0000:affb:53f3	::c009:0:4f26:0:affb:53f3
42	0000:dcd2:71be:0000:734d:2e61:0000:9881	0:dcd2:71be:0:734d:2e61:0:9881
43	bae4:eb02:0000:f41a:145d:bb47:0000:0000	bae4:eb02:0:f41a:145d:bb47::
44	0000:0000:0000:0000:0000:740c:0000:1741	::740c:0:1741
45	0000:0000:0000:0000:7cd8:1e15:c90f:ae1b	::7cd8:1e15:c90f:ae1b
46	241c:8bb2:a902:dc92:1333:4bfb:0000:56c3	241c:8bb2:a902:dc92:1333:4bfb:0:56c3
47	ec1f:2794:38cd:0000:e5f8:0000:c2cc:898c	ec1f:2794:38cd:0:e5f8:0:c2cc:898c
48	86a3:f3ec:0000:0000:0000:c93a:b47c:0000	86a3:f3ec::c93a:b47c:0
49	0000:c570:e19b:681a:0615:0000:0000:0000	0:c570:e19b:681a:615::
50	0000:dc4e:0000:0000:0000:0000:0000:8ffd	0:dc4e::8ffd
51	4ecb:68e9:e08d:a371:0000:0000:0000:0000	4ecb:68e9:e08d:a371::
52	0000:0000:0000:64b2:0000:7e75:8bb1:ec30	::64b2:0:7e75:8bb1:ec30
53	a7e1:6747:0bb4:0000:0000:0000:5bd7:0000	a7e1:6747:bb4::5bd7:0
54	1803:0000:0000:0000:33e5:4828:0000:e00c	1803::33e5:4828:0:e00c
55	0000:e083:0000:df9f:4d92:0000:0000:477d	0:e083:0:df9f:4d92::477d
56	2001:0000:0000:f007:781f:0000:c2d5:a767	2001::f007:781f:0:c2d5:a767
57	0000:94e8:0000:5a26:a616:b790:0000:d238	0:94e8:0:5a26:a616:b790:0:d238
58	0000:1a4b:fd0e:0000:0000:e929:0000:0000	0:1a4b:fd0e::e929:0:0
59	5c77:da9a:3305:39eb:0000:ade2:0750:7450	5c77:da9a:3305:39eb:0:ade2:750:7450
60	7d09:0000:9d50:0000:33dc:0000:0000:445b	7d09:0:9d50:0:33dc::445b
61	4b1a:0000:fd0b:f0c5:86be:0000:551c:0000	4b1a:0:fd0b:f0c5:86be:0:551c:0
62	589e:0000:53c7:93e3:0000:0000:12e9:093c	589e:0:53c7:93e3::12e9:93c
63	0000:3616:0000:8509:368f:6ffa:0000:0000	0:3616:0:8509:368f:6ffa::

continué en la próxima página

Tabla 2 – proviene de la página anterior

Num ejercicio	IPv6	Comprimida
64	78cc:20e9:00e5:f0a9:eac3:0000:0000:0000	78cc:20e9:e5:f0a9:eac3::
65	0000:0000:4d06:0000:0000:0000:b1dd:0000	0:0:4d06::b1dd:0
66	0000:0000:0000:e4bf:0d24:d134:0b2a:100a	::e4bf:d24:d134:b2a:100a
67	0000:0000:0000:0000:0000:0000:9159:8768	::9159:8768
68	0000:0000:0000:d4b0:bea8:0000:abdb:f2f7	::d4b0:bea8:0:abdb:f2f7
69	dc62:0000:5b76:0000:01e3:77fb:0000:0000	dc62:0:5b76:0:1e3:77fb::
70	0000:c781:0000:f950:0000:2451:7b8a:0000	0:c781:0:f950:0:2451:7b8a:0
71	4deb:e14c:c9b0:e65c:2265:0000:0000:29b3	4deb:e14c:c9b0:e65c:2265::29b3
72	0000:3ebe:5d28:0000:7697:0000:0000:1708	0:3ebe:5d28:0:7697::1708
73	0000:0000:0000:f141:0000:215a:0000:0000	::f141:0:215a:0:0
74	e64a:ff9f:eb7c:923b:3a5f:0000:0000:0000	e64a:ff9f:eb7c:923b:3a5f::
75	36a8:58be:9b67:be76:66c3:0000:90a5:0000	36a8:58be:9b67:be76:66c3:0:90a5:0
76	b096:0000:0000:0000:7291:0000:eefd:0000	b096::7291:0:eefd:0
77	0000:0000:036c:0000:e583:d41a:956c:394f	::36c:0:e583:d41a:956c:394f
78	79e4:8350:0000:6d5b:cac2:0000:dd6b:e62a	79e4:8350:0:6d5b:cac2:0:dd6b:e62a
79	34f5:0000:2ecb:0000:0000:27c6:0000:0000	34f5:0:2ecb::27c6:0:0
80	b2d2:b338:0000:0000:3160:20bc:f4e6:5878	b2d2:b338::3160:20bc:f4e6:5878
81	0000:0000:0000:4ddc:0000:1646:d72c:0000	::4ddc:0:1646:d72c:0
82	0000:e0bb:111c:0000:0000:6fd4:0000:8891	0:e0bb:111c::6fd4:0:8891
83	c04b:0000:0000:bac7:0000:e028:0000:c8e5	c04b::bac7:0:e028:0:c8e5
84	f680:0000:0000:0000:0000:0000:dfa9:0000	f680::dfa9:0
85	e19b:0000:101a:3fcc:ae97:0000:7970:f214	e19b:0:101a:3fcc:ae97:0:7970:f214
86	50c1:9e9c:0000:0000:ed17:0000:8e99:0000	50c1:9e9c::ed17:0:8e99:0
87	0000:ab50:4066:2809:f314:0000:92da:0000	0:ab50:4066:2809:f314:0:92da:0
88	ff48:0000:0000:22e7:9656:0000:0000:0000	ff48:0:0:22e7:9656::
89	0000:0000:0000:0000:0000:0000:14a5:0000	::14a5:0
90	8d13:0000:237a:c4d7:0000:0000:4df0:c8d0	8d13:0:237a:c4d7::4df0:c8d0
91	4a7e:caaa:0000:0000:ec08:ce1f:0000:0000	4a7e:caaa::ec08:ce1f:0:0
92	1c21:0000:0000:0000:0000:0000:e5c0:fc84	1c21::e5c0:fc84
93	0000:0000:32da:419f:0000:5b69:dad0:bc58	::32da:419f:0:5b69:dad0:bc58
94	e73c:b036:3efd:0000:0000:0d87:0000:6197	e73c:b036:3efd::d87:0:6197
95	0000:0000:0000:5bb0:bf99:0000:a21e:0000	::5bb0:bf99:0:a21e:0
96	0000:9a47:5197:a901:0000:0000:3ac3:39c8	0:9a47:5197:a901::3ac3:39c8
97	0000:14e3:0000:0000:06d0:e328:20a4:ea05	0:14e3::6d0:e328:20a4:ea05
98	d9b4:e5de:7478:a8ac:2a19:3ef6:a970:0000	d9b4:e5de:7478:a8ac:2a19:3ef6:a970:0
99	dcd1:0000:a0df:0000:0000:f58a:0000:f323	dcd1:0:a0df::f58a:0:f323
100	0000:021d:64f1:df12:e8ac:0000:489f:75a0	0:21d:64f1:df12:e8ac:0:489f:75a0

2.21 Anexo: ejercicios sobre clasificación de direcciones IPv6

Dadas las siguientes direcciones IPv6 indica de qué tipo son:

1. feab:e7b8:6626:0:a16e:0:6efe:995f
2. fdf6:22e5:e01:0:9af6::
3. fd53:a56e:0:950d:4bc::3c92
4. ff22:a6f1::933c:ff7b:f150
5. fea3:0:d97a::eac:bbb1:c90b

6. fd67:0:3456:e82b:4617:138d:936:3834
7. fdfb:1935::25cf:4987:0:0
8. 2277:2700:2b57:0:4d38::
9. ffad:bdd2:3e17:0:98f7:7f6b::
10. 3415::
11. ff6d:0:6a25:df12:88d:5fa6::
12. ff22::71ac:0:aca
13. fc0a:0:cbf3:70ae:e72c:0:c4db:0
14. 26bc:0:49e::5f84:d8c5:0
15. fe90:af2c:c2d6:195e:bc86:0:4f08:f7ca
16. 2537:5b85:8e74:b4d0:b2fc::
17. fe96::b88b:32f8:0:d025:0
18. 3170::98dc:d2c0:c886:0:0
19. 29ae:0:243:0:d814:1b69:f171:0
20. 274d:d1e0:19f2:0:fa26:fb94:529e:1378
21. 3c9e:6c30::71e3:0:0:8f68
22. fd9b::a80f
23. feb6:0:6c6d:c6dd:454c:4ea:d71e:cee
24. fea1:e171:60e7:d8e7:4d43::df9
25. fc98::67d0:0:68a5:0:0
26. fea6:791a:c569:86a1:bf71:adcb:11:fe15
27. fdfd:9440:8179:7eef:0:a606:0:1fe7
28. 3b2f:90fa:0:bb9e:13b:ab79::
29. fea9:1415:0:e7bc:0:fbcd::
30. ff5e:0:336f:0:7f53::
31. fe83:dd6c:0:9584:3367:b654:75b3:0
32. fc58:0:bc51:10a3::
33. ff3a:e8a3::3c07:5a1e:0
34. feae::2230:0:e8b
35. ffcd:0:6ecc:9718:0:c20e::
36. ff9e:0:246f:0:ed59::7fb4
37. ff68:0:e756:95e1::67f1:0
38. fc5e:d122:7da3:896e:626c::
39. 3bc1:0:ab12:85bf:2274::
40. ff09:7ffd:d25c:2e26:aeac:3a45:0:f1e
41. fd03:0:5db4:d114:2972:0:c484:0

42. feac:cfe9::e3c9:0
43. ff05::9c60:0:0:4b4a
44. 2499:0:aeac:0:12e:cbdf:7b95:0
45. ff9f::5cc0
46. fdc5:289e:0:c613::7add:6ea5
47. ff79:8c::ece7:0:0
48. fd16:8393:2506::9bb4:75be:0
49. ff9c:875b:3f71:0:299e::
50. fddd::1d58:0:bfa5:f060:0

2.21.1 Soluciones a la clasificaciones de direcciones IPv6

1. feab:e7b8:6626:0:a16e:0:6efe:995f es de tipo unicast local en enlace
2. fdf6:22e5:e01:0:9af6:: es de tipo unicast local único
3. fd53:a56e:0:950d:4bc::3c92 es de tipo unicast local único
4. ff22:a6f1::933c:ff7b:f150 es de tipo multicast
5. fea3:0:d97a::eac:bbb1:c90b es de tipo unicast local en enlace
6. fd67:0:3456:e82b:4617:138d:936:3834 es de tipo unicast local único
7. fdfb:1935::25cf:4987:0:0 es de tipo unicast local único
8. 2277:2700:2b57:0:4d38:: es de tipo unicast global
9. ffad:bdd2:3e17:0:98f7:7f6b:: es de tipo multicast
10. 3415:: es de tipo unicast global
11. ff6d:0:6a25:df12:88d:5fa6:: es de tipo multicast
12. ff22::71ac:0:aca es de tipo multicast
13. fc0a:0:cbf3:70ae:e72c:0:c4db:0 es de tipo unicast local único
14. 26bc:0:49e::5f84:d8c5:0 es de tipo unicast global
15. fe90:af2c:c2d6:195e:bc86:0:4f08:f7ca es de tipo unicast local en enlace
16. 2537:5b85:8e74:b4d0:b2fc:: es de tipo unicast global
17. fe96::b88b:32f8:0:d025:0 es de tipo unicast local en enlace
18. 3170::98dc:d2c0:c886:0:0 es de tipo unicast global
19. 29ae:0:243:0:d814:1b69:f171:0 es de tipo unicast global
20. 274d:d1e0:19f2:0:fa26:fb94:529e:1378 es de tipo unicast global
21. 3c9e:6c30::71e3:0:0:8f68 es de tipo unicast global
22. fd9b::a80f es de tipo unicast local único
23. feb6:0:6c6d:c6dd:454c:4ea:d71e:cee es de tipo unicast local en enlace
24. fea1:e171:60e7:d8e7:4d43::df9 es de tipo unicast local en enlace
25. fc98::67d0:0:68a5:0:0 es de tipo unicast local único

26. fea6:791a:c569:86a1:bf71:adcb:11:fe15 es de tipo unicast local en enlace
27. fdfd:9440:8179:7eef:0:a606:0:1fe7 es de tipo unicast local único
28. 3b2f:90fa:0:bb9e:13b:ab79:: es de tipo unicast global
29. fea9:1415:0:e7bc:0:fbcd:: es de tipo unicast local en enlace
30. ff5e:0:336f:0:7f53:: es de tipo multicast
31. fe83:dd6c:0:9584:3367:b654:75b3:0 es de tipo unicast local en enlace
32. fc58:0:bc51:10a3:: es de tipo unicast local único
33. ff3a:e8a3::3c07:5a1e:0 es de tipo multicast
34. feae::2230:0:e8b es de tipo unicast local en enlace
35. ffcd:0:6ecc:9718:0:c20e:: es de tipo multicast
36. ff9e:0:246f:0:ed59::7fb4 es de tipo multicast
37. ff68:0:e756:95e1::67f1:0 es de tipo multicast
38. fc5e:d122:7da3:896e:626c:: es de tipo unicast local único
39. 3bc1:0:ab12:85bf:2274:: es de tipo unicast global
40. ff09:7ffd:d25c:2e26:aeac:3a45:0:f1e es de tipo multicast
41. fd03:0:5db4:d114:2972:0:c484:0 es de tipo unicast local único
42. feac:cfe9::e3c9:0 es de tipo unicast local en enlace
43. ff05::9c60:0:0:4b4a es de tipo multicast
44. 2499:0:aeac:0:12e:cbdf:7b95:0 es de tipo unicast global
45. ff9f::5cc0 es de tipo multicast
46. fdc5:289e:0:c613::7add:6ea5 es de tipo unicast local único
47. ff79:8c::ece7:0:0 es de tipo multicast
48. fd16:8393:2506::9bb4:75be:0 es de tipo unicast local único
49. ff9c:875b:3f71:0:299e:: es de tipo multicast
50. fddd::1d58:0:bfa5:f060:0 es de tipo unicast local único

Configuración y administración de conmutadores

Segmentación de la red. Ventajas que presenta. Conmutadores y dominios de colisión y «broadcast». Segmentación de redes. Formas de conexión al conmutador para su configuración. Configuración del conmutador. Configuración estática y dinámica de la tabla de direcciones MAC. Diagnóstico de incidencias del conmutador. Las tormentas de «broadcast». El protocolo Spanning-Tree.

Configuración y administración básica de routers

Los «routers» en las LAN y en las WAN. Componentes del router. Formas de conexión al router para su configuración inicial. Comandos para configuración del router. Comandos para administración del router. Configuración del enrutamiento estático. Definición y ubicación de listas de control de acceso (ACLs).

Configuración de redes virtuales VLAN

El diseño de redes locales a tres capas (núcleo, distribución y acceso). Implantación y configuración de redes virtuales. Diagnóstico de incidencias en redes virtuales. Definición de enlaces troncales en los conmutadores y routers. El protocolo IEEE802.1Q Protocolos para la administración centralizada de redes virtuales; el protocolo VTP

Configuración y administración de protocolos dinámicos

Protocolos enrutables y protocolos de enrutamiento. Protocolos de enrutamiento interior y exterior. El enrutamiento sin clase. La subdivisión de redes y el uso de máscaras de longitud variable (VLSM). El protocolo RIPv2; comparación con RIPv1. Configuración y administración de RIPv1. Configuración y administración de RIPv2. Diagnóstico de incidencias en RIPv2. Los protocolos de enrutamiento estado-enlace Configuración y administración en OSPF. Diagnóstico de incidencias en OSPF. Configuración y administración de protocolos de enrutamiento propietarios.

Configuración del acceso a Internet desde una LAN

Direccionamiento interno y direccionamiento externo. NAT origen y NAT destino. NAT estático, dinámico, de sobrecarga (PAT) e inverso. Configuración de NAT. Diagnóstico de incidencias de NAT. Configuración de PAT. Diagnóstico de fallos de PAT. Introducción a las tecnologías WAN: Frame Relay, RDSI, ADSL. Las tecnologías Wifi y Wimax. Las tecnologías UMTS y HSDPA. Tecnologías emergentes basadas en cable e inalámbricas.

Ejercicios propuestos para el tema 1

8.1 Conversión de números

Convertir a binarios los siguientes números:

- 43
- 67
- 95
- 121
- 193
- 217
- 675

Soluciones a ejercicios seleccionados

Convertir a binarios los siguientes números:

- 43: debe salir 0010.1011
- 67: debe salir 0100.0011
- 95: debe salir 0101.1111
- 121: debe salir 0111.1001
- 193: debe salir 1100.0001
- 217: debe salir 1101.1001
- 675: debe salir 0010.1010.0011