

Práctica 1.5. RIP y BGP

Objetivos

En esta práctica se afianzan los conceptos elementales del encaminamiento. En particular, se estudia un protocolo de encaminamiento interior y otro exterior: RIP (*Routing Information Protocol*) y BGP (*Border Gateway Protocol*).

Existen muchas implementaciones de los protocolos de encaminamiento. En esta práctica vamos a utilizar Quagga, que actualmente implementa RIP (versiones 1 y 2), RIPng, OSPF, OSPFv3, IS-IS y BGP. Quagga está estructurado en diferentes servicios (uno para cada protocolo) controlados por un servicio central (Zebra) que hace de interfaz entre la tabla de reenvío del *kernel* y las tabla de encaminamiento de cada protocolo.

Todos los ficheros de configuración han de almacenarse en el directorio `/etc/quagga`. La sintaxis de estos ficheros es sencilla y está disponible en <http://quagga.net>. Revisar especialmente la correspondiente a RIP y BGP en <https://www.quagga.net/docs/quagga.html>. Además, en `/usr/share/doc/quagga-0.99.22.4` hay ficheros de ejemplo.



Activar el **portapapeles bidireccional** (menú Dispositivos) en las máquinas virtuales.

Usar la opción de Virtualbox (menú Ver) para realizar **capturas de pantalla**.

La **contraseña** del usuario `cursoresdes` es `cursoresdes`.

Contenidos

Parte I. Protocolo interior: RIP

- Preparación del entorno

- Configuración del protocolo RIP

Parte II. Protocolo exterior: BGP

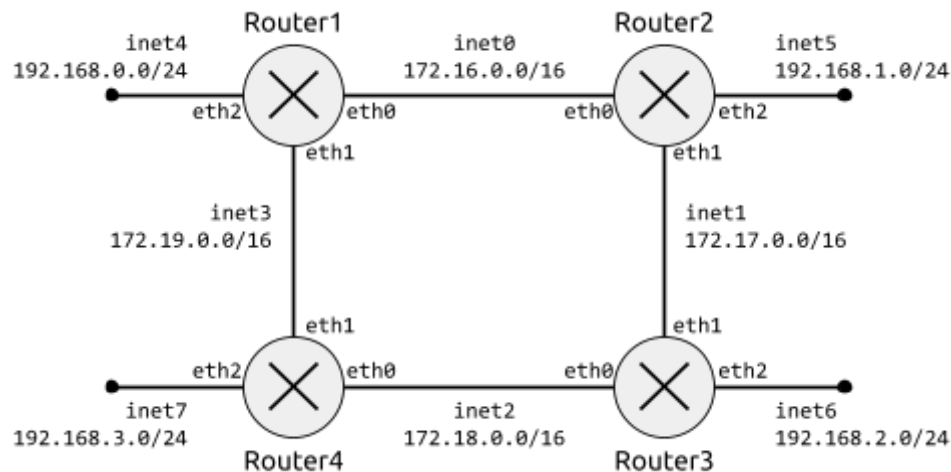
- Preparación del entorno

- Configuración del protocolo BGP

Parte I. Protocolo interior: RIP

Preparación del entorno

Configuraremos la topología de red que se muestra en la siguiente figura, donde cada encaminador (Router1...Router4) tiene tres interfaces, cada uno conectado a una red diferente.:



Al igual que en prácticas anteriores, usaremos la herramienta vtopo1 para construir automáticamente esta topología. A continuación se muestra el contenido del fichero de configuración de la topología:

```
netprefix inet
machine 1 0 0 1 3 2 4
machine 2 0 0 1 1 2 5
machine 3 0 2 1 1 2 6
machine 4 0 2 1 3 2 7
```

Para facilitar la configuración de las máquinas, la siguiente tabla muestra las direcciones de cada uno de los interfaces de los encaminadores:

Máquina virtual	Interfaz	Dirección de red	Dirección IP
Router1	eth0	172.16.0.0/16	172.16.0.1
	eth1	172.19.0.0/16	172.19.0.1
	eth2	192.168.0.0/24	192.168.0.1
Router2	eth0	172.16.0.0/16	172.16.0.2
	eth1	172.17.0.0/16	172.17.0.2
	eth2	192.168.1.0/24	192.168.1.2
Router3	eth0	172.18.0.0/16	172.18.0.3
	eth1	172.17.0.0/16	172.17.0.3
	eth2	192.168.2.0/24	192.168.2.3
Router4	eth0	172.18.0.0/16	172.18.0.4
	eth1	172.19.0.0/16	172.19.0.4
	eth2	192.168.3.0/24	192.168.3.4

Configurar todos los encaminadores según la figura y tabla anterior. Además, activar el reenvío de paquetes IPv4 igual que en la práctica 1.1. Después, comprobar:

- Que los encaminadores adyacentes son alcanzables, por ejemplo, Router1 puede hacer *ping* a Router2 y Router4.
- Que la tabla de reenvío de cada encaminador es la correcta e incluye una entrada para cada una de las tres redes a las que está conectado.

Configuración del protocolo RIP

Ejercicio 1. Configurar RIP en todos los encaminadores para que intercambien información:

- Crear un fichero `ripd.conf` en `/etc/quagga` con el contenido que se muestra a continuación.
- Iniciar el servicio RIP (y Zebra) con `service ripd start`.

Contenido del fichero `/etc/quagga/ripd.conf`:

```
# Activar el encaminamiento por RIP
router rip
# Definir la versión del protocolo que se usará
version 2
# Habilitar información de encaminamiento en redes asociadas a los interfaces
network eth0
network eth1
network eth2
```

Ejercicio 2. Consultar la tabla de encaminamiento de RIP y de Zebra en cada encaminador con el comando `vttysh` (`sudo vtysh -c "show ip rip"` y `sudo vtysh -c "show ip route"`). Comprobar también la tabla de reenvío de IPv4 con el comando `ip (ip route)`.

```
[VM1]
sudo vtysh -c "show ip rip"
Codes: R - RIP, C - connected, S - Static, O - OSPF, B - BGP
Sub-codes:
  (n) - normal, (s) - static, (d) - default, (r) - redistribute,
  (i) - interface

  Network      Next Hop      Metric From      Tag Time
C(i) 172.16.0.0/16  0.0.0.0        1 self          0
R(n) 172.17.0.0/16  172.16.0.2      2 172.16.0.2     0 02:35
R(n) 172.18.0.0/16  172.19.0.4      2 172.19.0.4     0 02:58
C(i) 172.19.0.0/16  0.0.0.0        1 self          0
C(i) 192.168.0.0/24 0.0.0.0        1 self          0
R(n) 192.168.1.0/24  172.16.0.2      2 172.16.0.2     0 02:35
R(n) 192.168.2.0/24  172.16.0.2      3 172.16.0.2     0 02:35
R(n) 192.168.3.0/24  172.19.0.4      2 172.19.0.4     0 02:58

sudo vtysh -c "show ip route"
Codes: K - kernel route, C - connected, S - static, R - RIP,
      O - OSPF, I - IS-IS, B - BGP, A - Babel,
      > - selected route, * - FIB route

C>* 127.0.0.0/8 is directly connected, lo
C>* 172.16.0.0/16 is directly connected, eth0
R>* 172.17.0.0/16 [120/2] via 172.16.0.2, eth0, 00:02:29
R>* 172.18.0.0/16 [120/2] via 172.19.0.4, eth1, 00:01:07
C>* 172.19.0.0/16 is directly connected, eth1
C>* 192.168.0.0/24 is directly connected, eth2
R>* 192.168.1.0/24 [120/2] via 172.16.0.2, eth0, 00:02:29
R>* 192.168.2.0/24 [120/3] via 172.16.0.2, eth0, 00:01:17
R>* 192.168.3.0/24 [120/2] via 172.19.0.4, eth1, 00:01:07
```

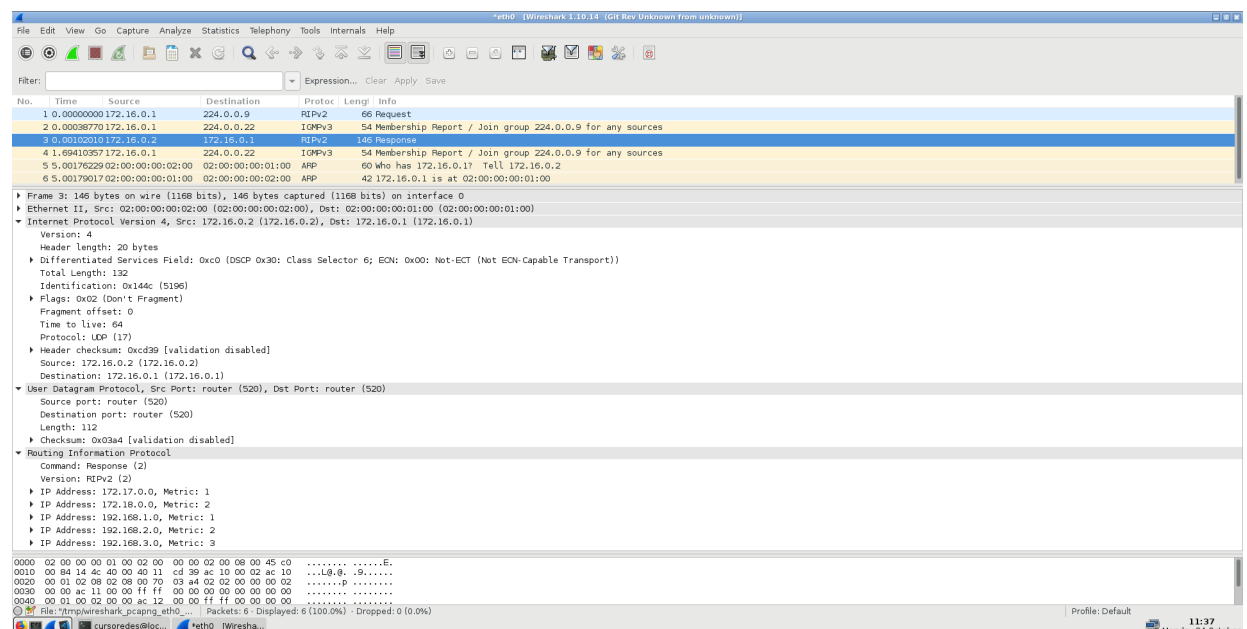
ip route

```
172.16.0.0/16 dev eth0 proto kernel scope link src 172.16.0.1
172.17.0.0/16 via 172.16.0.2 dev eth0 proto zebra metric 2
172.18.0.0/16 via 172.19.0.4 dev eth1 proto zebra metric 2
172.19.0.0/16 dev eth1 proto kernel scope link src 172.19.0.1
192.168.0.0/24 dev eth2 proto kernel scope link src 192.168.0.1
192.168.1.0/24 via 172.16.0.2 dev eth0 proto zebra metric 2
192.168.2.0/24 via 172.16.0.2 dev eth0 proto zebra metric 3
192.168.3.0/24 via 172.19.0.4 dev eth1 proto zebra metric 2
```

Ejercicio 3. Con la herramienta wireshark, estudiar los mensajes RIP intercambiados, en particular:

- Encapsulado.
- Direcciones origen y destino.
- Campo de versión.
- Información para cada ruta: dirección de red, máscara de red, siguiente salto y distancia.

Copia una captura de pantalla de Wireshark con mensajes RIP que muestre el formato de un mensaje Response.



- *Encapsulado:* UDP, puerto 520
- *Direcciones*
 - *Origen:* 172.16.0.2
 - *Destino:* 172.16.0.1
- *Versión:* RIPv2
- *Ruta:*
 - *Dirección de red:* 172.17.0.0
 - *Máscara de red:* 255.255.0.0
 - *Siguiente salto:* 0.0.0.0
 - *Distancia:* 1

Ejercicio 4. Eliminar el enlace entre Router1 y Router4 (por ejemplo, desactivando el interfaz eth1 en Router4). Comprobar que Router1 deja de recibir los anuncios de Router4 y que, pasados aproximadamente 3 minutos (valor de *timeout* por defecto para las rutas), ha reajustado su tabla.

```
[VM4]
sudo ip link set dev eth0 down
```

```
[VM1]
sudo vtysh -c "show ip rip"
Codes: R - RIP, C - connected, S - Static, O - OSPF, B - BGP
Sub-codes:
  (n) - normal, (s) - static, (d) - default, (r) - redistribute,
  (i) - interface
```

Network	Next Hop	Metric	From	Tag	Time
C(i) 172.16.0.0/16	0.0.0.0	1	self	0	
R(n) 172.17.0.0/16	172.16.0.2	2	172.16.0.2	0	02:42
R(n) 172.18.0.0/16	172.16.0.2	3	172.16.0.2	0	02:42
C(i) 172.19.0.0/16	0.0.0.0	1	self	0	
C(i) 192.168.0.0/24	0.0.0.0	1	self	0	
R(n) 192.168.1.0/24	172.16.0.2	2	172.16.0.2	0	02:42
R(n) 192.168.2.0/24	172.16.0.2	3	172.16.0.2	0	02:42
R(n) 192.168.3.0/24	172.16.0.2	4	172.16.0.2	0	02:42

Ejercicio 5. Los servicios de Quagga pueden configurarse de forma interactiva mediante un interfaz VTY (Virtual Teletype), de forma similar a los encaminadores comerciales. Para activar el interfaz VTY, hay que añadir el comando password al fichero de configuración del servicio deseado. Configurar ripd vía VTY:

- Añadir "password asor" al fichero ripd.conf, desactivar el protocolo (no router rip) y comentar el resto de entradas. Una vez cambiado el fichero, reiniciar el servicio.
- Conectar al interfaz VTY de ripd con telnet y configurarlo. Teclea '?' para mostrar la ayuda asociada.

Ejemplo de sesión:

```
$ telnet 127.0.0.1 ripd
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.

Hello, this is Quagga (version 0.99.20.1)
Copyright © 1996-2005 Kunihiro Ishiguro, et al.
User Access Verification

Password: asor
localhost.localdomain> ?
  echo      Echo a message back to the vty
  enable    Turn on privileged mode command
  exit      Exit current mode and down to previous mode
  help      Description of the interactive help system
  list      Print command list
  quit      Exit current mode and down to previous mode
  show      Show running system information
  terminal   Set terminal line parameters
  who       Display who is on vty
localhost.localdomain> enable
localhost.localdomain# configure terminal
```

```
localhost.localdomain(config)# router rip
localhost.localdomain(config-router)# version 2
localhost.localdomain(config-router)# network eth0
localhost.localdomain(config-router)# exit
localhost.localdomain(config)# exit
localhost.localdomain# show running-config
```

Current configuration:

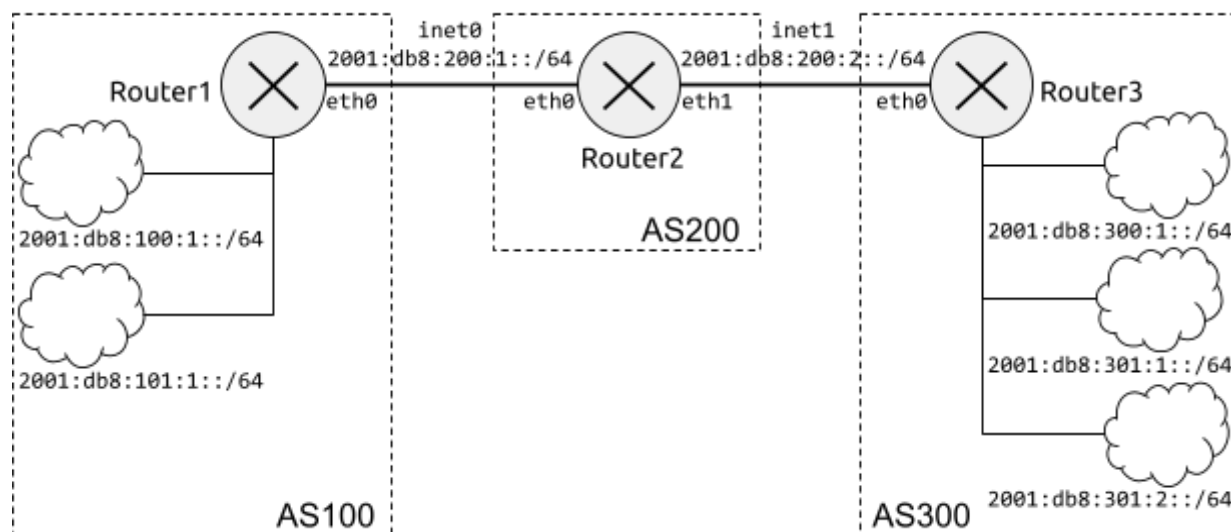
```
!
password asor
!
router rip
 version 2
 network eth0
!
line vty
!
end
localhost.localdomain# write
Configuration saved to /etc/quagga/ripd.conf
localhost.localdomain# exit
Connection closed by foreign host.
$ _
```

Nota: Para poder escribir la configuración en ripd.conf, el usuario quagga debe tener los permisos adecuados sobre el fichero. Para cambiar el propietario del fichero, ejecutar el comando `chown quagga:quagga /etc/quagga/ripd.conf`.

Parte II. Protocolo exterior: BGP

Preparación del entorno

Configuraremos la topología de red con 3 AS, siendo uno de ellos el proveedor de los otros dos:



Nota: El prefijo 2001:db8::/32 está reservado para documentación y ejemplos (RFC 3849).

Crearemos esta topología (sin las redes internas de los AS) con la herramienta vtopo1 y el siguiente

fichero:

```
netprefix inet
machine 1 0 0
machine 2 0 0 1 1
machine 3 0 1
```

Para facilitar la configuración de las máquinas, la siguiente tabla muestra las direcciones de cada uno de los interfaces de los encaminadores:

Máquina virtual	Interfaz	Dirección de red	Dirección IP
Router1	eth0	2001:db8:200:1::/64	2001:db8:200:1::1
Router2	eth0	2001:db8:200:1::/64	2001:db8:200:1::2
	eth1	2001:db8:200:2::/64	2001:db8:200:2::2
Router3	eth0	2001:db8:200:2::/64	2001:db8:200:2::3

Configurar los encaminadores según se muestra en la figura anterior. Debe comprobarse la conectividad entre máquinas adyacentes.

Configuración del protocolo BGP

Ejercicio 6. Consultar la documentación de las clases de teoría para determinar el tipo de AS (*stub*, *multihomed* o *transit*) y los prefijos de red que debe anunciar. Recordar que el prefijo global de encaminamiento es de 48 bits y que los prefijos anunciados deben agregarse al máximo.

Número de AS	Tipo	Prefijos agregados
100	stub	2001:db8:100::/47
200	transit	
300	stub	2001:db8:300::/47

Ejercicio 7. Configurar BGP en los encaminadores para que intercambien información:

- Crear un fichero `bgpd.conf` en `/etc/quagga` usando como referencia el que se muestra a continuación.
- Iniciar el servicio BGP (y Zebra) con `service bgpd start`.

Por ejemplo, el contenido del fichero `/etc/quagga/bgpd.conf` de Router1 en el AS 100 sería:

```
[VM1]
# Activar el encaminamiento BGP en el AS 100
router bgp 100
# Establecer el identificador de encaminador BGP
bgp router-id 0.0.0.1
# Añadir el encaminador BGP vecino en el AS 200
neighbor 2001:db8:200:1::2 remote-as 200
# Empezar a trabajar con direcciones IPv6
address-family ipv6
# Anunciar un prefijo de red agregado
network 2001:db8:100::/47
# Activar IPv6 en el encaminador BGP vecino
```

```
neighbor 2001:db8:200:1::2 activate
# Dejar de trabajar con direcciones IPv6
exit-address-family
```

[VM2]

```
# Activar el encaminamiento BGP en el AS 100
router bgp 200
# Establecer el identificador de encaminador BGP
bgp router-id 0.0.0.2
# Añadir el encaminador BGP vecino en el AS 100
neighbor 2001:db8:200:1::1 remote-as 100
neighbor 2001:db8:200:2::3 remote-as 300
# Empezar a trabajar con direcciones IPv6
address-family ipv6
# Activar IPv6 en el encaminador BGP vecino
neighbor 2001:db8:200:1::1 activate
neighbor 2001:db8:200:2::3 activate

# Dejar de trabajar con direcciones IPv6
exit-address-family
```

[VM3]

```
# Activar el encaminamiento BGP en el AS 300
router bgp 300
# Establecer el identificador de encaminador BGP
bgp router-id 0.0.0.3
# Añadir el encaminador BGP vecino en el AS 200
neighbor 2001:db8:200:2::2 remote-as 200
# Empezar a trabajar con direcciones IPv6
address-family ipv6
# Anunciar un prefijo de red agregado
network 2001:db8:300::/47
# Activar IPv6 en el encaminador BGP vecino
neighbor 2001:db8:200:2::2 activate
# Dejar de trabajar con direcciones IPv6
exit-address-family
```

Ejercicio 8. Consultar la tabla de encaminamiento de BGP y de Zebra en cada encaminador con el comando vtysh (sudo vtysh -c "show ipv6 bgp" y sudo vtysh -c "show ipv6 route"). Comprobar también la tabla de reenvío de IPv6 con el comando ip (ip -6 route).

Copia los comandos usados y su salida.

[VM2]

```
sudo vtysh -c "show ipv6 bgp"
```

BGP table version is 0, local router ID is 0.0.0.2

Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, R Removed

Origin codes: i - IGP, e - EGP, ? - incomplete

Network	Next Hop	Metric	LocPrf	Weight	Path
---------	----------	--------	--------	--------	------

```
*> 2001:db8:100::/47
```

```
2001:db8:200:1::1
```

```
0
```

```
0 100 i
```



```
*> 2001:db8:300::/47
      2001:db8:200:2::3
          0          0 300 i
```

Total number of prefixes 2

sudo vtysh -c "show ipv6 route"

*Codes: K - kernel route, C - connected, S - static, R - RIPng,
O - OSPFv6, I - IS-IS, B - BGP, A - Babel,
> - selected route, * - FIB route*

```
C>* ::1/128 is directly connected, lo
B>* 2001:db8:100::/47 [20/0] via fe80::ff:fe00:100, eth0, 00:03:06
C>* 2001:db8:200:1::/64 is directly connected, eth0
C>* 2001:db8:200:2::/64 is directly connected, eth1
B>* 2001:db8:300::/47 [20/0] via fe80::ff:fe00:300, eth1, 00:01:20
C * fe80::/64 is directly connected, eth1
C>* fe80::/64 is directly connected, eth0
```

ip -6 route

```
unreachable ::/96 dev lo metric 1024 error -113 pref medium
unreachable ::ffff:0.0.0.0/96 dev lo metric 1024 error -113 pref medium
2001:db8:100::/47 via fe80::ff:fe00:100 dev eth0 proto zebra metric 1024 pref medium
2001:db8:200:1::/64 dev eth0 proto kernel metric 256 pref medium
2001:db8:200:2::/64 dev eth1 proto kernel metric 256 pref medium
2001:db8:300::/47 via fe80::ff:fe00:300 dev eth1 proto zebra metric 1024 pref medium
unreachable 2002:a00::/24 dev lo metric 1024 error -113 pref medium
unreachable 2002:7f00::/24 dev lo metric 1024 error -113 pref medium
unreachable 2002:a9fe::/32 dev lo metric 1024 error -113 pref medium
unreachable 2002:ac10::/28 dev lo metric 1024 error -113 pref medium
unreachable 2002:c0a8::/32 dev lo metric 1024 error -113 pref medium
unreachable 2002:e000::/19 dev lo metric 1024 error -113 pref medium
unreachable 3ffe:ffff::/32 dev lo metric 1024 error -113 pref medium
fe80::/64 dev eth0 proto kernel metric 256 pref medium
fe80::/64 dev eth1 proto kernel metric 256 pref medium
```

Ejercicio 9. Con ayuda de la herramienta wireshark, estudiar los mensajes BGP intercambiados (OPEN, KEEPALIVE y UPDATE).

Copia una captura de pantalla de Wireshark con mensajes BGP que muestre el formato de un mensaje UPDATE.

Wireshark 1.10.14 interface showing network traffic capture from eth0. The top pane displays a list of captured packets, including BGP KEEPALIVE and Neighbor Solicitation messages. The middle pane shows the details of the selected packet (Frame 1: 105 bytes on wire), identifying it as a BGP KEEPALIVE Message. The bottom pane displays the raw packet data in hexadecimal and ASCII format.

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protoc	Length	Info
1	0.00000000	2001:db8:200:1::2	2001:db8:200:1::1	BGP	105	KEEPALIVE Message
2	0.00060543	2001:db8:200:1::1	2001:db8:200:1::2	BGP	105	KEEPALIVE Message
3	0.00061531	2001:db8:200:1::1	2001:db8:200:1::1	TCP	86	49310 > bgp [ACK] Seq=20 Ack=20 Win=225 Len=0 TSval=1316917 TSecr=1317820
4	5.00296624	fe80::ff:fe00:200	2001:db8:200:1::1	ICMPv6	86	Neighbor Solicitation for 2001:db8:200:1::1 from 02:00:00:00:02:00
5	5.00319244	2001:db8:200:1::1	fe80::ff:fe00:200	ICMPv6	78	Neighbor Advertisement 2001:db8:200:1::1 (sol)
6	5.01220001	fe80::ff:fe00:100	2001:db8:200:1::2	ICMPv6	86	Neighbor Solicitation for 2001:db8:200:1::2 from 02:00:00:00:01:00
7	5.01220915	2001:db8:200:1::2	fe80::ff:fe00:100	ICMPv6	78	Neighbor Advertisement 2001:db8:200:1::2 (sol)

Frame 1: 105 bytes on wire (840 bits), 105 bytes captured (840 bits) on interface 0

Ethernet II, Src: 02:00:00:00:02:00 (02:00:00:00:02:00), Dst: 02:00:00:00:01:00 (02:00:00:00:01:00)

Internet Protocol Version 6, Src: 2001:db8:200:1::2 (2001:db8:200:1::2), Dst: 2001:db8:200:1::1 (2001:db8:200:1::1)

Transmission Control Protocol, Src Port: 49310 (49310), Dst Port: bgp (179), Seq: 1, Ack: 1, Len: 19

Border Gateway Protocol - KEEPALIVE Message

Marker: ffffffff

Length: 19

Type: KEEPALIVE Message (4)

0030 00 00 00 00 01 c0 9e 00 b3 dc 25 26 a5 4e 1a%&.N.

0040 03 d3 80 18 00 e1 5f b0 00 00 01 01 08 0a 00 14S..1X.....

0050 18 35 00 13 31 58 ff ff ff ff ff ff ff ff

0060 ff ff ff ff ff ff 00 13 04

Border Gateway Protocol (bgp). 19 ... Packets: 11 · Displayed: 11 (100.0%)

Profile: Default

12:32 Monday 24 October

Filter: Expression... Clear Apply Save

Open the "Display Filter" dialog to edit/apply filters

No.	Time	Source	Destination	Protoc	Length	Info
27	123.020917	2001:db8:200:1::1	2001:db8:200:1::2	TCP	86	49310 > bgp [ACK] Seq=61 Ack=40 Win=225 Len=0 TSval=1424937 TSecr=1425840
28	123.020938	2001:db8:200:1::2	2001:db8:200:1::1	TCP	94	54524 > bgp [SYN] Seq=0 Win=28800 Len=0 MSS=1440 SACK_PERM=1 TSval=1440840 TSecr=0 WS=1
29	130.191512	2001:db8:200:1::2	2001:db8:200:1::1	TCP	74	bgp > 54524 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
30	130.191500	2001:db8:200:1::1	2001:db8:200:1::2	TCP	94	49314 > bgp [SYN] Seq=0 Win=28800 Len=0 MSS=1440 SACK_PERM=1 TSval=1447108 TSecr=0 WS=1
31	130.191965	2001:db8:200:1::2	2001:db8:200:1::1	TCP	94	bgp > 49314 [SYN, ACK] Seq=0 Ack=1 Win=28560 Len=0 MSS=1440 SACK_PERM=1 TSval=1448011 TSecr=0 WS=1
32	130.192105	2001:db8:200:1::2	2001:db8:200:1::1	TCP	86	49314 > bgp [ACK] Seq=1 Ack=1 Win=28800 Len=0 TSval=1447109 TSecr=1448011
33	130.192325	2001:db8:200:1::1	2001:db8:200:1::2	TCP	86	bgp > 49314 [ACK] Seq=1 Ack=62 Win=28672 Len=0 TSval=1448012 TSecr=1447109
34	130.192626	2001:db8:200:1::1	2001:db8:200:1::2	BGP	166	OPEN Message, KEEPALIVE Message
35	130.192634	2001:db8:200:1::2	2001:db8:200:1::1	TCP	86	49314 > bgp [ACK] Seq=62 Ack=81 Win=28800 Len=0 TSval=1447109 TSecr=1448012
36	130.192771	2001:db8:200:1::2	2001:db8:200:1::1	BGP	124	KEEPALIVE Message, KEEPALIVE Message
37	130.193159	2001:db8:200:1::1	2001:db8:200:1::2	BGP	105	KEEPALIVE Message
38	130.233133	2001:db8:200:1::2	2001:db8:200:1::1	TCP	86	49314 > bgp [ACK] Seq=100 Ack=100 Win=28800 Len=0 TSval=1447150 TSecr=1448013
39	131.194945	2001:db8:200:1::1	2001:db8:200:1::2	BGP	177	UPDATE Message
40	131.194990	2001:db8:200:1::2	2001:db8:200:1::1	TCP	86	49314 > bgp [ACK] Seq=100 Ack=191 Win=28800 Len=0 TSval=1448112 TSecr=1449014

Border Gateway Protocol - UPDATE Message

Marker: ffffffff

Length: 91

Type: UPDATE Message (2)

Unfeasible routes length: 0 bytes

Total path attribute length: 68 bytes

Path attributes

0000 02 00 00 00 02 00 02 00 00 00 01 00 86 dd 6c 00l

0010 00 00 00 7b 06 01 20 01 0d b8 02 00 00 01 00 00 ...f.....

0020 00 00 00 00 00 01 20 01 0d b8 02 00 00 01 00 00>

0030 00 00 00 00 00 02 00 b3 c0 a2 12 a0 dc 3e dd 75>.u

0040 30 23 80 18 00 e0 7b 06 00 00 01 01 08 0a 00 16 0#.....

Frame (frame). 177 bytes Packets: 40 · Displayed: 40 (100.0%) · Dropped: 0 (0.0%)

Profile: Default

12:34 Monday 24 October