To: Fabio Massacci, Giorgio Di Tizio
From: Claudio Facchinetti
Subject: BGP Hijacking exercise
Date: October 27, 2021

1 First task

How many hops away is the ftp server from the client?
As we can see from the screnshot, the client is four hops away from the ftp server: the path from the client goes through, in order, `asn3`, `asn2` and finally reaches the server.

```
traceroute to 10.1.1.2 (10.1.1.2), 30 hops max, 60 byte packets
 1  10.5.0.1  0.332 ms  0.313 ms  0.273 ms
 2  10.3.0.2  0.943 ms  0.933 ms  0.922 ms
 3  10.2.0.1  1.342 ms  1.330 ms  1.308 ms
 4  10.1.1.2  1.207 ms  1.163 ms  1.136 ms
```

Figure 1: Traceruote for the first task

Explain what route is the client using to reach the server 10.1.1.2 In order to reach the server (`10.1.1.2`) the client is going to use the second route reported in the image below: in particular it is going to send the packets to 10.5.0.1, because the address `10.1.1.2` matches the destination `10.0.0.0` with netmask `255.0.0.0`.

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
0.0.0.0         192.168.1.254   0.0.0.0         UG        0 0          0 eth4
10.0.0.0        10.5.0.1        255.0.0.0       UG        0 0          0 eth2
10.5.0.0        0.0.0.0         255.255.255.0   U         0 0          0 eth2
192.168.0.0     0.0.0.0         255.255.252.0   U         0 0          0 eth4
192.168.1.254   0.0.0.0         255.255.255.255 UH        0 0          0 eth4
```

Figure 2: Netstat output for the first task

What does the README file say? The content of the README file is still the same: `AS1 owns the prefix for 10.1/16`

(ASN3) What is the AS path to reach 10.1/16? As we can see from the picture below the machine `asn3` is going to reach `10.1/16` by sending the traffic to `10.3.0.2`.

(ASN2) What is the AS path to reach 10.1/16? As we can see from the picture below the machine `asn2` is going to reach `10.1/16` by sending the traffic to `10.2.0.1`.

2 Second task

How many hops away is the ftp server from the client this time? Is there a difference in output from the same command in Part-1? As we can see from the picture the client

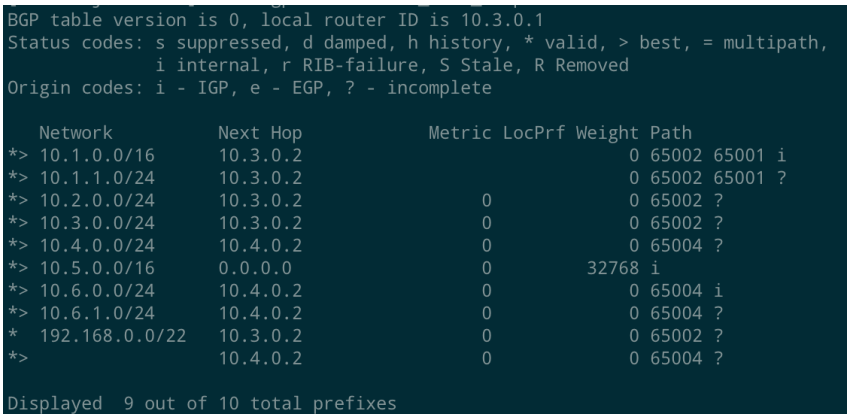

Figure 3: BGP routes for ASN3 for the first task

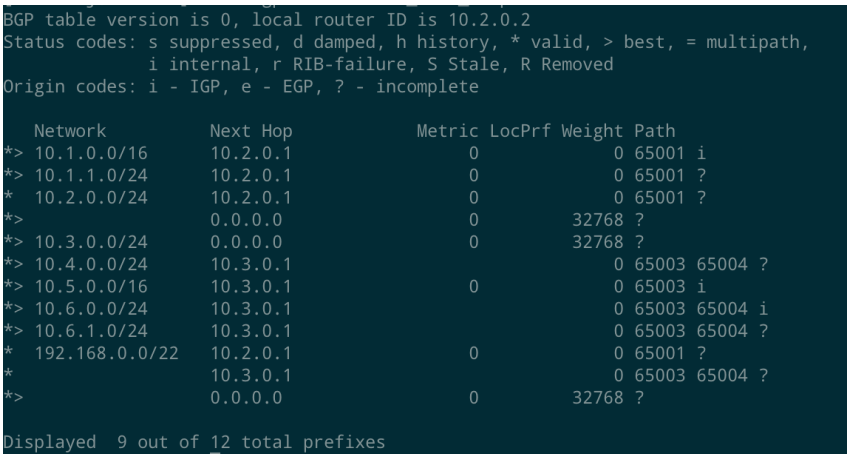

Figure 4: BGP routes for ASN2 for the first task

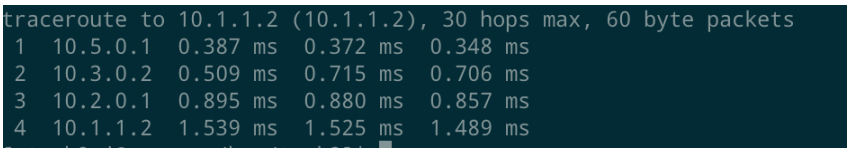

Figure 5: Traceroute output for the second task

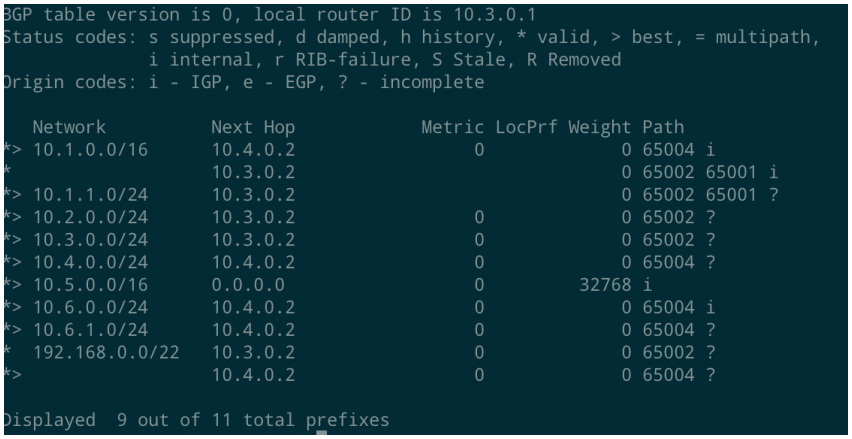

Figure 6: BGP routes of ASN3 for the second task

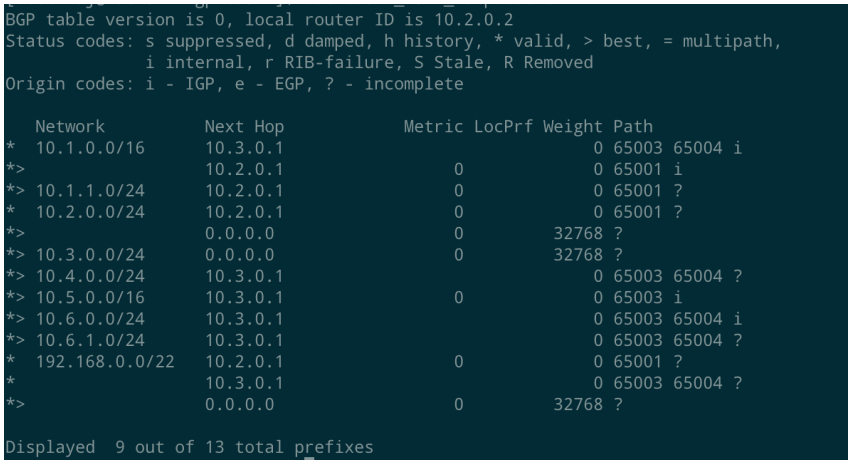

Figure 7: BGP routes of ASN2 for the second task

is still four hops away from the server and there has been no modifications from the previous task.

What does the README file say? Did the contents of README file differ from the output in Part-1? The content of the README file is still `AS1 owns the prefix for 10.1/16`: it did not change from the previous task.

(ASN3) What is the AS path to reach 10.1/16? Did the AS path differ from the last time? Taking a look at the BGP routes we can notice that the path to reach `10.1/16` is still the same, however we can notice that the BGP Hijacking was success: now the route to `10.0.0.0/16` is different as the traffic directed to that network now go through `asn4` instead of `asn2` as in the previous case

(ASN2) What AS path will be used to reach an IP address 10.1.1.2? What AS path will be used to reach an IP address 10.1.2.2? Taking a look at the BGP routes we can say that the traffic directed to `10.1.1.2` will go through the address `10.2.0.1` while the traffic for `10.1.2.2` will go through the `AS3` which will then be sent to the `AS4`. This happens because the `AS1` is publishing a shorter prefix which is able to catch the traffic directed to `10.1.0.0/16`.

```
traceroute to 10.1.1.2 (10.1.1.2), 30 hops max, 60 byte packets
 1  10.5.0.1  0.509 ms  0.494 ms  0.470 ms
 2  10.4.0.2  0.879 ms  0.863 ms  0.841 ms
 3  10.1.1.2  1.776 ms  1.755 ms  1.726 ms
```

Figure 8: Traceroute for the third task

```
BGP table version is 0, local router ID is 10.3.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
              i internal, r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.0.0/16      10.3.0.2                               0 65002 65001 i
*> 10.1.1.0/24      10.4.0.2                    0          0 65004 i
*                   10.3.0.2                               0 65002 65001 ?
*> 10.2.0.0/24      10.3.0.2                    0          0 65002 ?
*> 10.3.0.0/24      10.3.0.2                    0          0 65002 ?
*> 10.4.0.0/24      10.4.0.2                    0          0 65004 ?
*> 10.5.0.0/16      0.0.0.0                     0      32768 i
*> 10.6.0.0/24      10.4.0.2                    0          0 65004 i
*> 10.6.1.0/24      10.4.0.2                    0          0 65004 ?
*  192.168.0.0/22   10.3.0.2                    0          0 65002 ?
*>                  10.4.0.2                    0          0 65004 ?

Displayed  9 out of 11 total prefixes
```

Figure 9: BGP routes for ASN3 for the third task

3 Third task

How many hops away is the ftp server 10.1.1.2 from the client this time? Is there a difference in output from the same command in Part-2?

As we can see now the output of the command is different: the client machine traffic goes through `AS4` in order to reach the server, while it was not the case before. From this we can see that `asn4` successfully managed to hijack the prefix `10.1.0.0/16`.

Did the contents of README file differ from the output in Part-2? The content of the README file did actually change: before it was `AS1 owns the prefix for 10.1/16` while now it is `I just hijacked your BGP prefix!`.

(ASN3) What is the AS path to reach 10.1/16? Did the AS path differ from Part-2? What is the AS path to reach 10.1.1.0/24? Taking a look at the BGP routes for `asn3` we can see that both the routes to `10.1/16` and to `10.1.1.0/24` have changed since last part.
Since `asn4` stopped advertising the route for `10.1/16` now `asn3` will take use the same AS path as in task one to reach such destination. Now `asn4` also started advertising its route for `10.1.1/24`, therefore `asn3` will use that route as it is shorted in order to redirect traffic.

(ASN2) What AS path will be used to reach an IP address 10.1.1.2? What AS path will be used to reach an IP address 10.1.2.2? The machine `asn2` in to reach `10.1.1.2` it will send traffic to `asn3` while to reach `10.1.2.2` it will send traffic to `10.2.0.1`

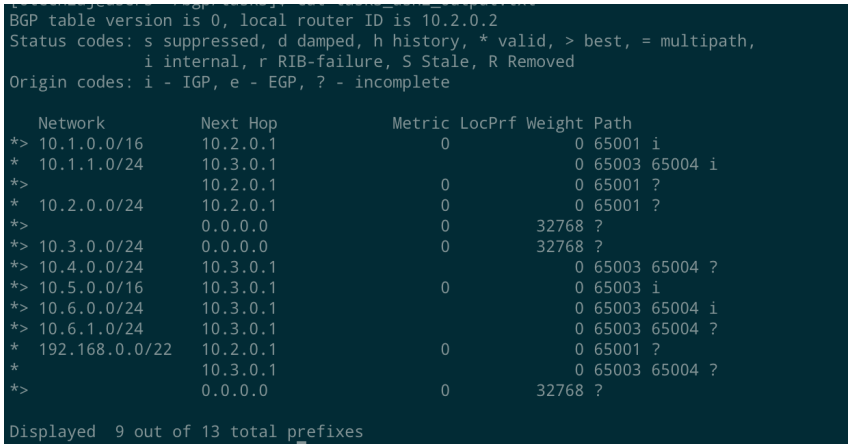

Figure 10: BGP routes for ASN2 for the third task