GaN Network Lab 5

BGP fundamentals

1. Explain the role of BGP in the Internet routing infrastructure.
2. What is the role of AS path and local preference in BGP decision making?
3. Why can we say that BGP is “performance oblivious”? (i.e. network performances are not taken in account for route election)
4. What is the concept of route aggregation? Why does it play a central role in BGP?
5. Do all routers have a complete knowledge about the Internet routes? If a router does not know the route to a given prefix where is the traffic sent?
6. ASes exchange routes by connecting their routers via direct physical links. What network infrastructure is used to ease the interconnection of ASes?

We can retrieve BGP updates and information using the public BGP monitoring system:

- RIPE RIS: https://ris-live.ripe.net/
- Route Views: https://www.routeviews.org/routeviews/
- Looking glasses: https://bgp.he.net/super-lg/

Although looking glasses (BGP routers sharing their routes) are useful to consult information about a specific prefix, they cannot be used to monitor the Internet in real time. For that, researchers and operators rely on RIPE RIS and Route Views.

1. Explain briefly the architecture behind these BGP monitoring platforms.

CDNs and BGP

1. How do CDNs like Google or Cloudflare use BGP to optimize content delivery?
2. Why is a client redirected to a single destination while a CDN prefix can be announced from a different location?
3. Using Hurricane Electrics Looking glass (https://bgp.he.net/super-lg/), check the different route observed for the prefix 8.8.8.0/24. What can you say about the length of the observed AS path? What does it say about these CDNs' infrastructure?

Security in BGP

1. In its default version, what are the security mechanisms in place in BGP?
2. Define the concept of a BGP hijack and route poisoning.
3. What security mechanism was introduced to prevent BGP hijacks?

4. BGP is still very much unsecure, what is the limitation of the most used security mechanism in BGP?

Exercise:

The following update is being observed at a public monitor of RIPE RIS:


```
{
    "project": "RR",
    "timestamp": 1762194762.99,
    "peer": "193.203.0.63",
    "peer_asn": "6720",
    "collector": "rrc05.ripe.net",
    "type": "UPDATE",
    "path": [6720, 1853, 6939, 9434],
    "community": [[1120, 1]],
    "origin": "IGP",
    "next_hop": "193.203.0.63",
    "prefixes": ["147.28.10.0/23"]
}
```


1. From which AS is the update coming from?
2. To which organisation this AS belongs to? (check RIPE Stat)
3. How many ASes use this AS for transit? (check CAIDA AS ranking)
4. How many providers does this AS have?
5. What is the difference between a peer to peer link and a customer to provider link between two ASes?

You know receive this second announcement:


```
{
    "project": "RV",
    "timestamp": 1762196671.753521,
    "peer": "64.71.137.241",
    "peer_asn": 6939,
    "collector": "route-views2",
    "type": "UPDATE",
    "community": [],
    "path": [6447, 6939, 215011, 9434],
    "prefixes": ["147.28.11.0/24"],
    "next_hop": "64.71.137.241"
}
```


1. What changed compared to the previous update?
2. Compare the ranking (using CAIDA AS ranking) between the two ASes. The ranking is calculated using the number of providers, customers and peers. It is a metric to

evaluate the importance of an AS in the Internet infrastructure, the more customer and lesser provider, higher the rank.

3. Do you think this announcement is legitimate?
4. What is the valley-free rule in BGP? How far can the route propagate on the Internet?
5. Why are currently implemented security mechanisms insufficient to prevent this type of bogus route?