GaN Network Lab 4

Exercise 1: Network Analysis

As a network engineer, responsible for the service's quality experienced by your clients accessing your organization's Web server. In order to estimate the ability of your organization to deliver content to your clients, you implemented a monitoring software checking (among possible metrics):

- the latency experienced by your clients
- server allocation result (Note: could include Anycast vs. Unicast here)
- number of clients connected at any time to your server
- etc…

More precisely, your focus is directed on the Latency experienced by the client while interacting with the network infrastructure. Indeed, studies show that a user experiencing between 50ms to Xms is Y% more likely to leave your website []. With that in mind you set strict constraints on latency and procedures to act whenever you detect inflated latency[1] towards one of your clients[2].

[1] : inflated latency means that the time for a user's request to reach your server and send back the response is abnormally long (hundreds of milliseconds is already too long).
[2]: a client usually refers to a large cluster of users (i.e. prefixes, identifying for thousands of users).

For this first part, we will discuss the procedure you could use to estimate latencies experienced by your clients and how to detect if we are indeed in case of path inflation.

1) First of all, we would like you to propose an idea on how you could estimate the RTT for every client requesting services from one of your servers. (Hint: for a Web server, before sending HTTPS data, you need to establish a TCP connection).

2) Three clients established a connection with your server, your monitoring software outputs you these value:

Clients prefix	P1	P2	P3
RTT (ms)	12	23	156

As you can see here, latency experienced by clients belonging to prefix P3 is significantly higher than the rest of estimated RTT. As the network engineer of your company, you are in charge of **a)** identifying the nature of the event, **b)** locating precisely where the problem is coming from.

a) Give at least three potential events on the network that could explain the inflated latency towards clients belonging to prefix P3

b) List tools you could use to troubleshoot the problem you have with prefix P3

You assume that client prefix P3 is allocated to the best server (i.e. in terms of geolocalisation, network perspective, etc.). From that, you assume that the problem is coming from the network itself and start troubleshooting.

As we mentioned, you trust your infrastructure (memory, database, etc.) and assume that the problem is coming from the network. Moreover, you only see path inflation towards prefix P3 and not for your other client, implying the presence of a point of failure on the network path between your server and clients belonging to prefix P3.

1) In order to start your investigation, you run traceroute towards your client **using TCP**. Draw the resulting path you obtain (route is composed of 4 routers):

2) here are the RTT estimation you get while probing:

Router	R1	R2	R3	R4	Client
RTT (ms)	10	15	23	30	156

How do you interpret these results? Are you able to identify the point of failure using them?

3) Give an example on how traceroute can lead to false link discovery. Justify your answer and draw a schema.

4) Considering that no per-packet load-balancing is present on the path, how can you ensure that the route we obtained shows actual router physical links? (hint: think about flow-id definition and remember that we are probing using TCP).

5) As you haven't discovered any useful information about the point of failure, you assume that your knowledge about the topology is incomplete. Which strategy would you use, to discover other potential routes? (hint: think about how packets are routed depending on flow-id value).

6) After a couple of trial and error, you are able to discover a new route and obtain the resulting metrics:

Router	R1	R5	R6	R4	Client
RTT (ms)	10	15	23	140	156

How do you ensure that this route is not the same as before? (remember that we only get IP addresses from traceroute). How do you interpret these results? Are you able to make a guess about where the point of failure is located? Justify your answer.

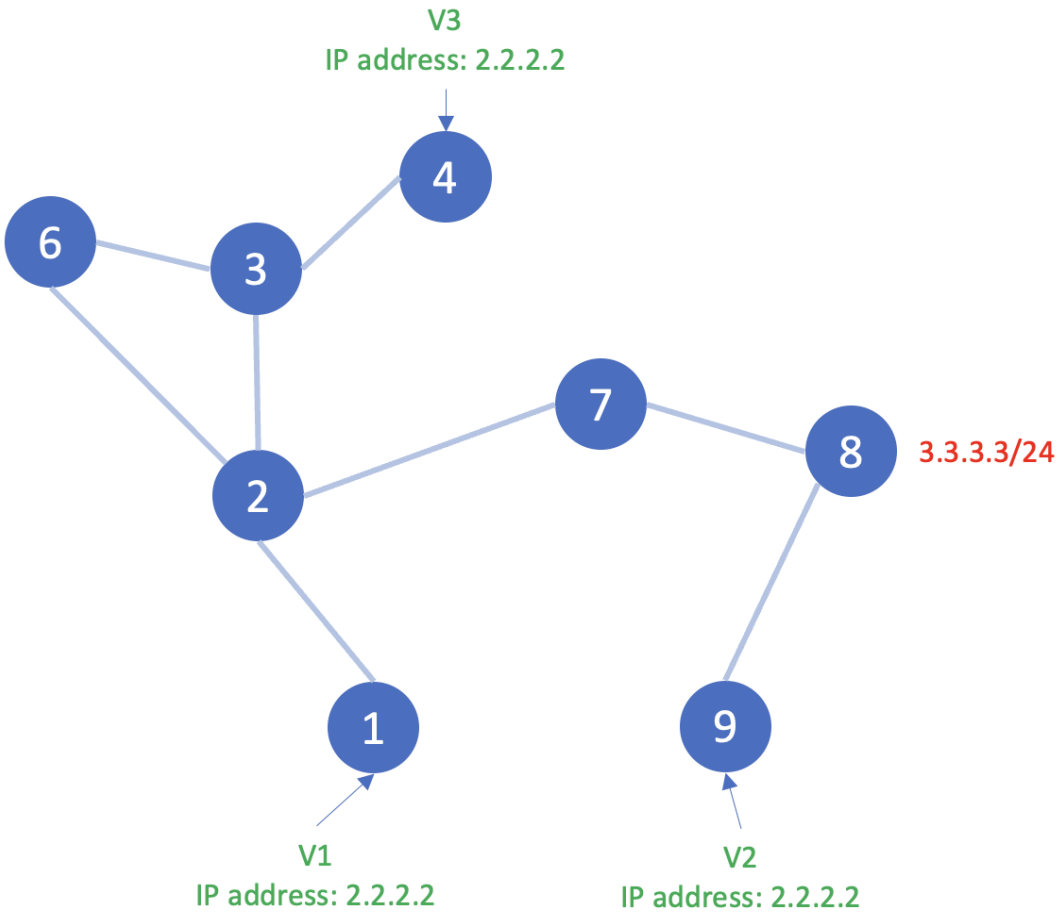
7) Imagine now that even after discovering the complete topology from the server to the client you do not see any path inflation, except when probing the client's prefix (case question 2)). How would you explain the situation? Which tool could you use to verify your assumption?

Exercise 2: Using BGP for Anycast detection

Course question:

What are the different types of messages exchanged in BGP?

What are the main organisations used to monitor BGP traffics? What is the fundamental limitation of monitoring BGP using these platforms?



You have the following scenario:

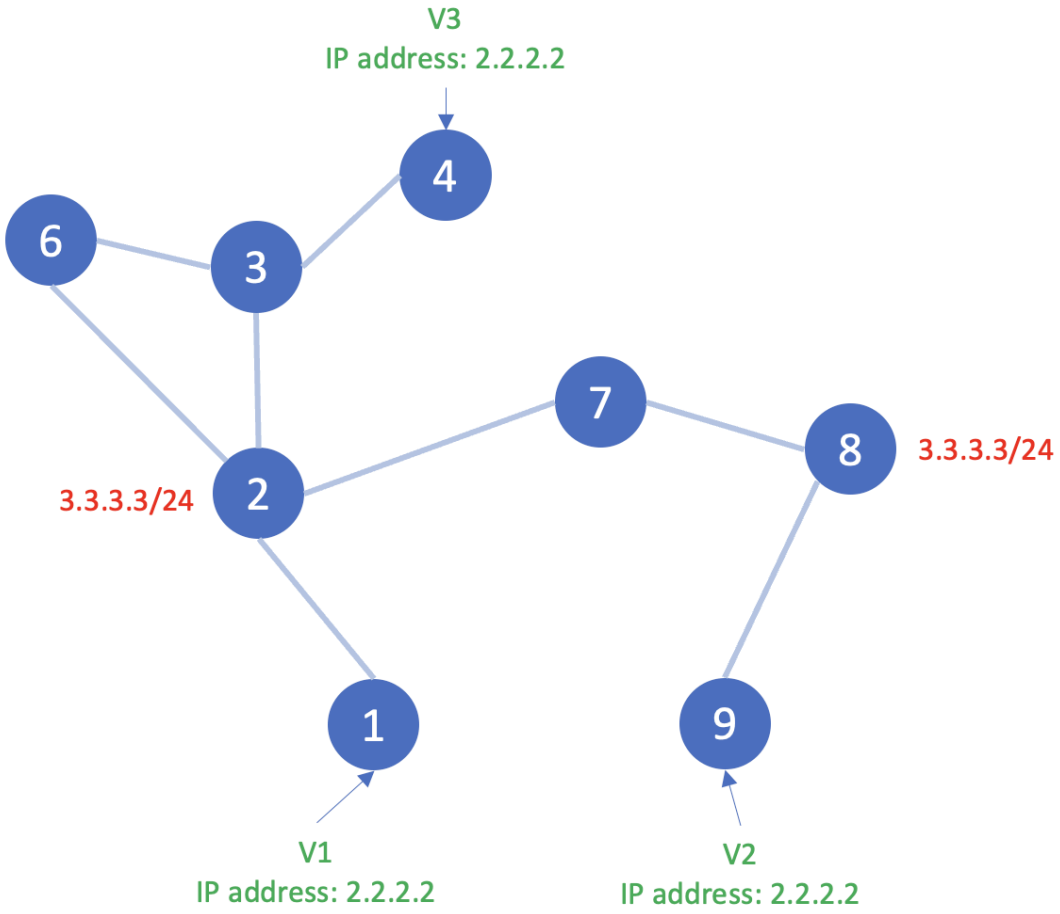
- Each blue circle represents an AS.
- You dispose of three vantage points (VPs): V1 (AS1), V2(AS9) and V3(AS4).
- All the VPs have the same **Anycast IP address**: 2.2.2.2
- We can make ping from the VPs

Our objective is to detect if the prefix `3.3.3.3/24` is Anycast or not. We already know that we can detect Anycast with latency based measurements (question 11). Problem: making pings to all /24 prefixes is costly, we want to craft another solution.
For the remainder of the exercise, we consider the shortest AS path is elected by each AS (i.e. we ignore local preference consideration).

We first consider that `3.3.3.3/24` is an **Unicast** prefix (only AS 8 advertise the prefix):

1°) Draw the **forward path** of a ping packet from each VP **to the prefix** 3.3.3.3/24.

2°) Draw the **backward path** (i.e. the ping response from AS 8). How is the response routed back? (again, considering the VPs have an Anycast prefix).



Consider now the figure above. that the prefix `3.3.3.3/24` is also announced by the AS 2 (**i.e. the prefix is Anycast**).

1°) What will be the path from each VP to the prefix?

2°) What about the backward path?

3°) Can you craft an Anycast detection based on the difference observed between the two scenarios?