Attack on Finances (AoF)

You are a cybersecurity analyst for a large financial institution. One day, you receive an urgent message from your boss informing you that the company's payment processing system has been hacked. The hackers have stolen millions of dollars from the company's accounts, and they're threatening to leak sensitive customer information if their demands aren't met.

Your boss tells you that the company's IT team has identified the source of the attack as a group of hackers based in Eastern Europe. **They've traced the hackers' location to Bucharest in Romania**, but they don't have any other information about the group or their motives.

Your job is to work with the IT team to set up a network topology that will help you prevent them from accessing any more sensitive data. You'll need to set up a network that covers all of the company's branches across the world, as well as a secure connection to the Romanian clients.

The company's **headquarters is in Dhaka**, and they have **branches in California, Lisbon, Paris, Madrid and Tokyo**. The distance between each branch and the number of computer devices at each branch are listed below:

	Dhaka	California	Lisbon	Paris	Bucharest	Tokyo	Madrid
Dhaka (150)	0						
California (50)	1300	0					
Lisbon (11)	910	523	0				
Paris (20)	788	409	89	0			
Bucharest (30)	618	389	122	101	0		
Tokyo (40)	489	876	387	398	578	0	
Madrid (130)	863	329	102	177	212	476	0

*The numbers in brackets () specify the number of devices in the city and the values in the table specify the distance (in kilometers) between branches. *

Requirements:

While creating the network infrastructure, you were provided with certain restrictions and rules that you needed to follow:

- **Using the network address 192.128.0.0/10**, create subnets and assign to each branch with the least amount of waste.
- **Dhaka** being the headquarters is connected directly with each of the other cities.
- **California** and **Tokyo** will also have **two separate web servers**. The DNS server will be located in California. If anyone types the URL “www.california..gov” the web server located at California will handle the query and the user will see a webpage that says “Welcome to California!”. Similarly, the web server located in Tokyo will handle requests for “www.japan.com” and return “I love Anime!” when visited through the URL.
- **Dhaka** and **Bucharest** are the most important cities; for security, they will use static addressing while the other branches’ IP addresses will be assigned using DHCP and handled by their network’s DHCP server.
- **Dhaka** and **Bucharest** will be communicating a lot which is why they will require email servers to be set up so that they can exchange mail among themselves. Make sure the email configurations are all set up.
- Establish connections among all the branches with the shortest route possible. When establishing a connection, keep the following things in mind:
    - There has to exist at least one floating route among the branches.
- Showing **1 device** per 10 devices is enough to represent the full active computers in the departments.

- Configure at least one network to be routed dynamically and one to be routed statically.
- You have to remember the default route cannot be used while exchanging packets. Data will be delivered using static or dynamic routes only.
- You have to be able to ping from one city to another after all the setups are properly completed

Deliverables:

- The network mentioned above should be implemented in packet tracer, with the necessary devices and full configuration.
- After completion, you should be able to test the conditions imposed.
- You will have to submit the followings:
    - Network topology diagram with proper labels
    - The configuration commands of all the routers you have implemented.
    - VLSM tree
    - IP address table