Question 1
What phases can be distinguished in the lifecycle of a bot?

Answer
Infection (system receives and executes bot malware), rallying (bot announce its presence to C&C server and establishes C&C channel), passive (bot waits for commands from C&C server), active (bot performs malicious activity). In parallel with passive and active phases, a bot may propagate malware and infect other systems or receive updates from the C&C server.

Question 2
What is the purpose of fast flux?

Answer
Botmasters utilize fast flux to frequently change the IP address associated with the domain name of its C&C server (or proxy bots in front of the C&C server). This helps in evading IP based blacklisting and blocking.

Question 3
What is the purpose of DGA?

Answer
Botnets apply a DGA (domain generation algorithm) to generate a large amount of pseudo-random domain names for contacting the C&C server. Most of those domain names are not registered, and only a few actually correspond to a C&C server. The purpose is to hide the domain name of the C&C server.

Question 4
Do botmasters prefer a botnet with a central or hybrid topology?

Answer
The goal of botmasters typically is to earn the most money with the least effort. In this philosophy, a simple botnet with central topology is preferred. However, if the botmaster wants to reduce the chance of being arrested and make the botnet more robust, then a more advanced, decentralized (or even hybrid) topology is preferred.