Lab 15

a) Smurf attack is a way of cheating in a video game. The smurf attack is based around when a machine is pinged it will respond. This can be exploited where you can have many different machines send ping requests to a client in a video game. With enough of these pings, it will cause an overload on the client, that could cause the client to slow down on their machine or worse. This is an issue with the Peer-to-Peer network game architecture. If this is a big issue for a game, there could be a change of architecture to a server architecture. Another form of cheating would be a SYN-attack. The idea of SYN-attack is where Client A would send Mutiple SYN messages to Client B from spoofed IP addresses fast before B can time out. A solution to this form of cheating would be the use of the client puzzle protocol. This protocol adds in a challenge response. This challenge response is sent when Client A is trying to overload Client B with SYN messages. So, if Client A doesn't answer the challenge within a time-limit, then the connection will drop, as this suggests that Client A is a spoofed IP. This protects Client B, as all of these SYN messages will be registered as spoofed IP's therefore stopping the cheating attempt.

b) Potentially visible sets are an algorithm to accelerate the rendering of 3D environments. This is a form of occlusion culling where a client would set visible polygons are pre-computed. Then they are indexed at run-time to quickly get an idea of the visible geometry the client can see. This pre-computation will occur on the server side and be sent out to all clients on the network that are connected. Static zones differ as the geometry is static, it does not need to be pre-calculated. interest management helps the game a lot, as it will filter out unneeded updates that will speed up the game for all the clients.