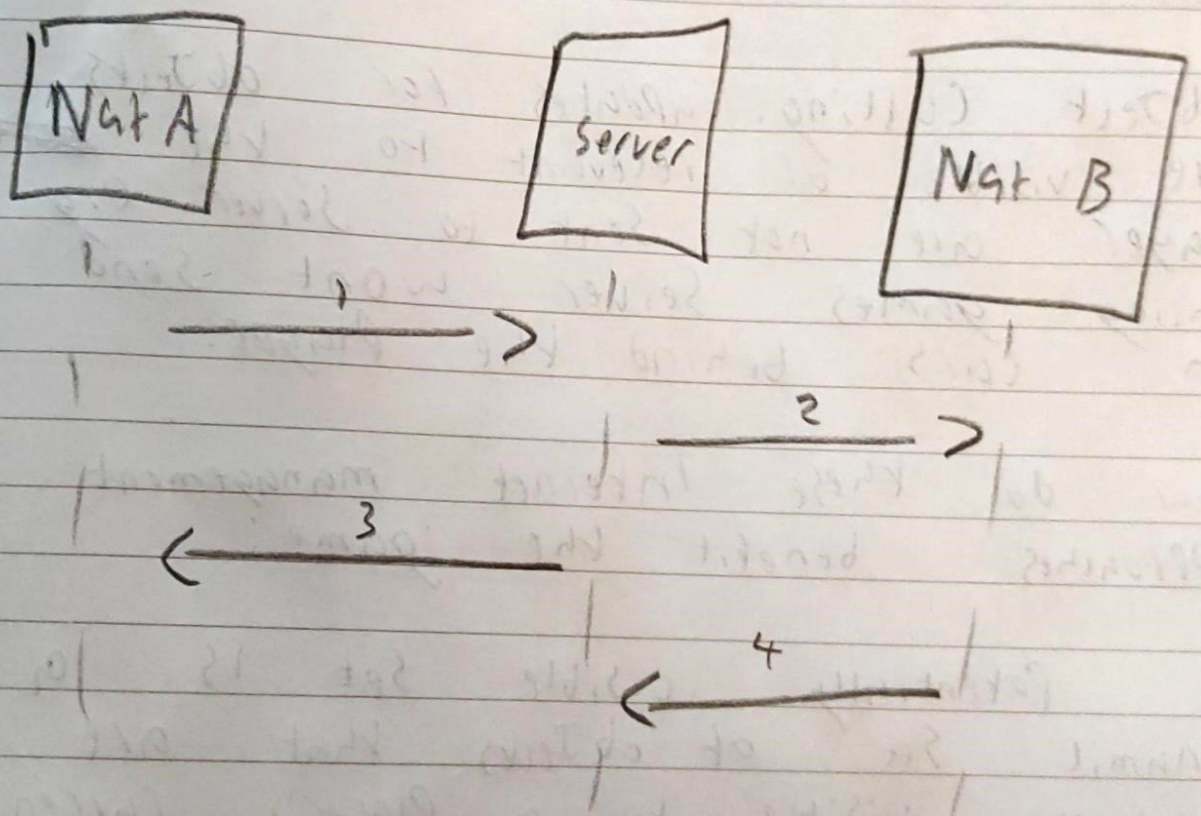
Final lab

1) Hole Punching technique:

The hole Punching technique is used to establish a direct connection between 2 devices behind 2 different network address translations (NAT) devices with needing any intermediary servers. Hole Punching basically both devices establish outbound connections to a third party server that is accessible from both devices. This server relays packets between the two devices allowing them to communicate with each other directly



A to B establish an outbound connection to Server.

Server relays IP address and Port num of devile B to devile A. repeats in reverse

When devices have IP, they can communicate with each other.

2) 2 techniques of interest management in games

Spatial Partitioning: Game world is divided into smaller sections and server only sends updates for the sections related to player. e.g only send updates for areas of map visible by player. This reduces the amount of network traffic as non visible areas are not sent.

Object Culling: updates for objects that are visible or relevant to the player are not sent to server. e.g racing games server wont send updates on cars behind the player.

3) how do these internet management approaches benefit the game:

a potentially visible set is a dynamic set of objects that are potentially visible to a player's current position and view. the PVS is updated based on player's client. This differs from static zones, which divide the game into static areas or zones and only updates for objects within the players current zone are sent

PVS benefits the game in several ways. first it reduces bandwidth used by filtering out objects that are not relevant to the player. This allows for a more dynamic and immersive game. PVS approach can allow for complex game mechanics like dynamic events and quests that take place across multiple areas.

Static zones are much simpler to implement and can provide a more structured and predictable gameplay experience. they can also allow for easier management of server resources as updates for objects outside the player's zone can be delayed or batched to reduce server load.

4) one client-side attack is a phishing attack: an attacker can create a fake website or email that looks like a real one. These sites will ask for sensitive information. prevention: user should educated to spot them such as checking urls

serverside attack could be an SQL injection. attacker executes SQL commands in input field to retrieve sensitive data.

5) 2. methods of cheating are aimbot and wallhacks. Aimbot is software that aims and shoots at other players. Scans for player models and automatically adjusting aim. To prevent this, devs can add anti-cheat mechanisms such as detecting abnormal patterns of monitoring player input.

wallhacks makes player models be visible through walls. Server side checks can be implemented to check validity of player actions, also monitoring player behaviour.