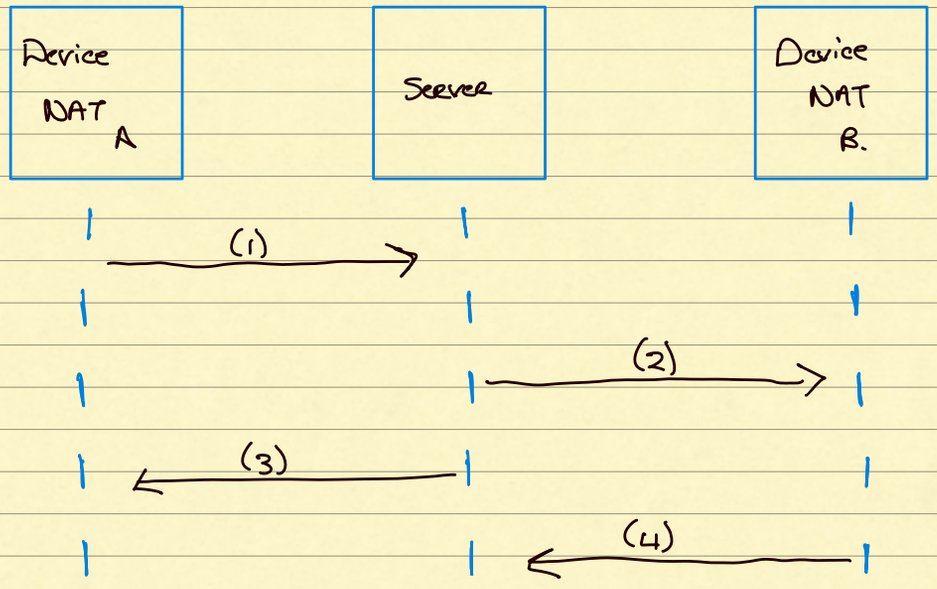
1.) In the Context of IP Restricted NAT devices, what does the hole-punching technique do? Describe this technique, using a diagram to aid your explanation if applicable.

Hole punching Technique is a technique used to establish a direct Connection between two devices behind different NATs, Without Requiring any intermediary Seevers.

The basic idea behind hole-punching is that both devices establish outbound Connections to a third party Seever that is accessable from both devices. This Seevee then Relays packets between the two devices allowing them to Communicate with each other directly.



- Devices A + B Establish an outbound Connection to the Seevee.
- Seever Relays IP address and port num of device B to device A. And Vice-Veesa.
- Once devices have obtained each others IP addresses and port, they Can Establish a direct Connection and Communicate with each other.

2.) In multiplayer online games, interest management Cuts down on bandwidth usage by filtering reelevant updates. Desceibe 2 Common techniques of interest management.

2 Common techniques of interest management would be Spatial partitioning & object Culling

Spatial partioning: With this technique, the game world is divided into Smallee Sections, and the Seever only Sends updates for the sections that are Relevant to the playee. Ex. In fps games the Seever would only Send updates for the area of the map that are Cureently Visible to the playee

This Reduces the amount of network teaffic as areas that arent Visible are reeelevant and not Sent.

Object Culling: In this technique, updates for objects that are currently visible or relevant to a player are not sent by the server. Ex. In Racing Games, the server may not send updates for cars that are too far away or behind a player, as they are not relevant to the players immediate interactions.

3.) Interest Management is important for good network performance on massively multiplayer games. What is a potentially visible set, and how does this approach differ from static zones. How do these interest management approaches benefit the game.

A potentially visible set, is a dynamic set of objects that are potentially visible to a players current position and view. The PVS is updated based on players movements and view, and only updates for objects within the PVS are sent to the 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 world. PVS approach can allow for complex game mechanics like dynamic events and quests that take place across multiple areas

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

4.) Describe one example for client-side attack and server-side, respectively. Please include details of how this attack works and how a mechanism to prevent it.

One Client side attack is a phishing attack. In a phishing attack, an attacker can create a fake website or email that looks like a legitimate one, such as a bank or social media website. The Attacker will send a link to this fake site, tricking them into entering their sensitive information like, passwords and credit card information.

To prevent this, users should be educated on how to identify phishing attempts. Such as checking the URL of a website and looking for secure connections. Also most modern browsers have anti-phishing mechanisms such as warning messages or blacklisting phishing websites

A Server-side attack might be a SQL injection. An attacker exploits a vulnerability in a web-apps

SQL database by inserting malicious code into a user input field. The attacker can execute SQL commands to retrieve sensitive data or deleting database entries.
To prevent attacks, Devs should parameterize queries. Which allow input to be treated as data rather than executable code.

5) Two methods of cheating in online games is through Aimbot & use of Wallhacks
Aimbot is a software that automatically aims and shoots at targets in the game. Giving the cheater an unfair advantage. Aimbot works by scanning for player models and automatically adjusting the cheaters aim to hit them.

To prevent this, devs can implement anti-cheat mechanisms, such as detecting abnormal patterns of movement or behaviour or monitoring player input to detect use of external software.

Another method of cheating is using Wallhacks, This gives the cheater a view of all players in a session through all walls and obstacles in the game. This can be prevented by also monitoring player behaviour and detecting abnormal patterns of movement.. Server-Side checks can also be implemented to check validity of player actions.