November 2020

Real-time IP Detection To Dynamically Apply Concurrency Constraints On Streaming

Stephen Lau

Janani Krishnaswamy

Follow this and additional works at: https://www.tdcommons.org/dpubs_series

Real-time IP Detection To Dynamically Apply Concurrency Constraints On Streaming

<u>ABSTRACT</u>

Streaming content providers offer a variety of subscription plans that differ on the number of users that can be created within an account and the number of devices that can concurrently receive streaming content at the same time. Some content providers offer family plans that allow users to stream unlimited concurrent streams within their physical household. It is important to accurately define a household for the family for the successful implementation of such plans. This disclosure describes the use of real-time IP address detection to dynamically define a household for a subscription account. The techniques do not store any information such as MAC address, DMA code etc. and are also tolerant of IP address changes and household moves/changes.

<u>KEYWORDS</u>

- IP address detection
- Content streaming
- Video streaming
- Audio streaming
- Streaming session
- Concurrent session
- Family plan

<u>BACKGROUND</u>

Streaming content providers offer a variety of subscription plans that differ on the number of users that can be created within an account and the number of devices that can receive streaming content at the same time. For example, family plans typically allow the creation of 4 to

6 family members and 2 to 3 concurrent streams within a single account. Some content providers offer family plans that allow users to stream unlimited concurrent streams within their physical household. It is important to accurately define a household for the family for the successful implementation of such plans.

There are multiple possible approaches to establish the household for a subscription. One approach is to utilize (with user permission) the combination of router MAC address, SSID name and IP address to designate the home location. With user permission, this combination can be stored on the content provider's server. Playback of streaming content is then allowed on any device that connects through this home location. Another approach can include the creation of a geofence using location data such as from a GPS and/or local radio frequency identifiers such as Wi-Fi nodes or Bluetooth beacons.

While these approaches make cheating (e.g., where more than the permitted number of streams are utilized simultaneously) unlikely, these involve steps that can be difficult for a non-technical user. Further, these approaches require obtaining user permission, and upon receipt of such permission, storing personally-identifiable information (PII) such as GPS coordinates, router MAC address etc. on the streaming content provider's server, which is often infeasible. Geofencing-based approaches do not work when there are client devices that view streaming content but are not compatible with the required technology.

DESCRIPTION

The techniques described in this disclosure use real-time IP detection to dynamically define a household within which unlimited streaming connections are allowed. The real-time IP detection is performed upon specific user permission. Utilizing these techniques, a streaming content provider that offers a family plan that allows N simultaneous streaming connections, can

allow N-1 IP addresses to have a single streaming connection and a single IP address (e.g., that associated with a router within the household) an unlimited number of streaming connections. The process, implemented with specific user permission to utilize IP address data is described with reference to Fig. 1 below.
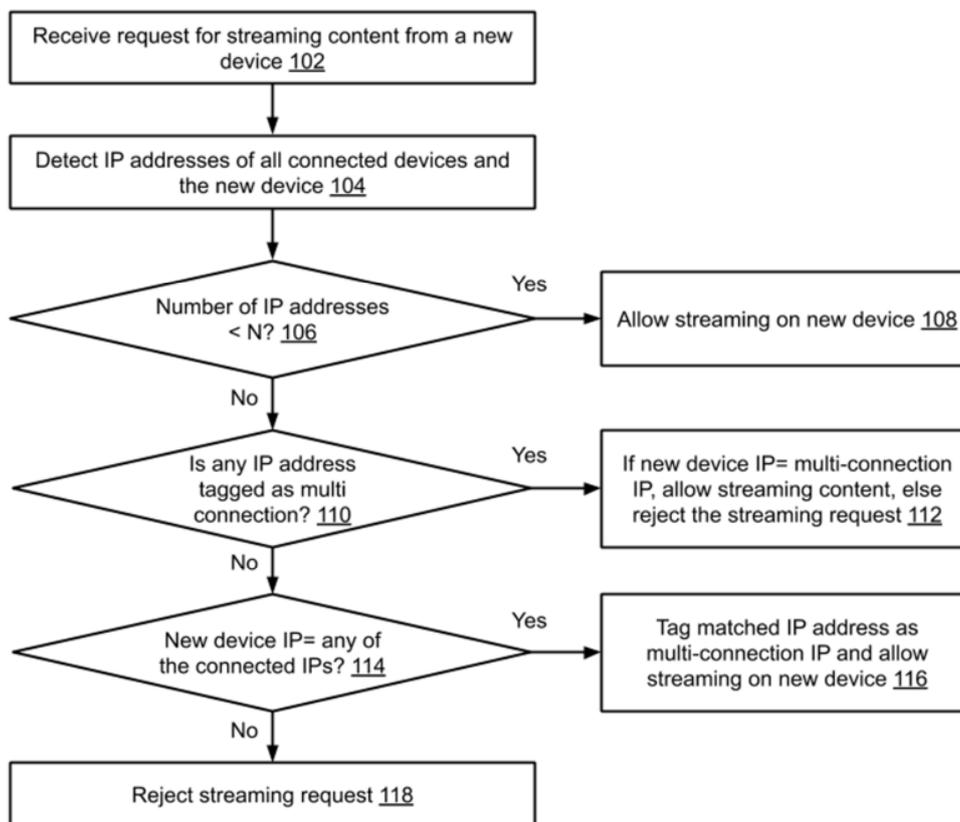

Fig. 1: Example process to dynamically define a household

When a streaming content request is received (102) from a new device, it is determined whether to approve or reject the streaming request based on the following process.

IP addresses of each connected device (linked to the account) that is already streaming content is detected. The IP address of the new device that is requesting streaming content is also detected (104). The number of distinct IP addresses is compared with N, which is the limit for simultaneous connections permitted per the subscription plan (106).

If the number of IP addresses is less than N, the streaming content is allowed on the new device (108). If the number of distinct IP addresses across the connected devices equals N, it is checked whether any of the detected IP addresses is tagged as a multi-connection IP address (110). If at least one IP address is tagged as a multi-connection IP address, streaming content is allowed only if the IP address of the new device matches with the multi-connection IP. If the IP address of the new device does not match with the multi-connection IP, the streaming content request is rejected (112).

If no IP address is tagged as a multi-connection IP, the IP address of the incoming device is compared with the IP addresses of the connected devices (114). If the IP address of the new device matches with one of the connected devices, the IP address is registered as a multi-connection IP address and streaming content is allowed on the new device (116). If the IP address of the incoming device does not match with that of any other device that is already streaming content, the new streaming request is rejected (118) as exceeding the number of simultaneous connections permitted per the subscription plan. Further, the multi-connection IP tag is dropped if the number of connected devices on the multi-connection IP address drops to 1. This enables dynamic reassignment of the multi-connection IP.

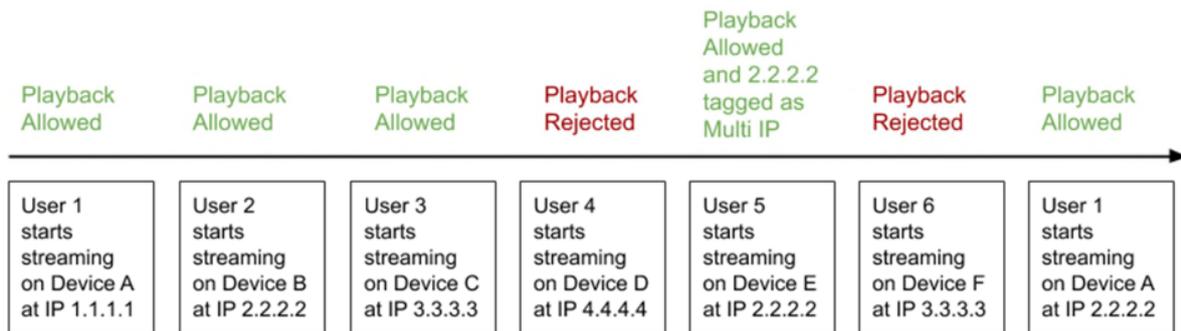A scenario involving a family plan that allows for 3 simultaneous connections (N=3) is illustrated in Fig. 2 below.

Fig. 2: Scenario with 3 simultaneous connections

1. User 1 starts streaming on device A at IP address 1.1.1.1. Playback is allowed to commence, since the number of connected IP addresses is less than 3.

2. User 2 starts streaming on device B at IP address 2.2.2.2. Playback is allowed to commence, since the number of connected IP addresses is less than 3.

3. User 3 starts streaming on device C at IP address 3.3.3.3. Playback is allowed to commence, since the number of connected IP addresses does not exceed 3.

4. User 4 attempts to start streaming on device D at IP address 4.4.4.4. Playback is rejected, since the number of IP addresses exceeds 3.

5. User 5 starts streaming on device E at IP address 2.2.2.2. Playback is allowed to commence and 2.2.2.2 is designated as the dynamic household where unlimited connections are allowed.

6. User 6 attempts to start streaming on device F at IP address 3.3.3.3. Playback is rejected, since the IP address of the new device does not match with the household IP (2.2.2.2).

7. User 1 starts streaming on device G at IP address 2.2.2.2. Playback is allowed to commence, as 2.2.2.2 is the household IP that is allowed unlimited concurrent connections.

The techniques described in this disclosure use real-time IP detection to enable the implementation of a content streaming plan that allows for unlimited streaming connections on one IP address (referred to as multi-connection IP address) and a single streaming connection on the remaining IP addresses. These techniques, implemented with user permission to detect IP address and compare it with other active IP addresses on the same account, do not require storage of information such as MAC address, DMA code etc. on the streaming content provider's server. The techniques are also more tolerant of IP address changes and household moves/changes, and do not require any user action when such changes take place.

CONCLUSION

Streaming content providers offer a variety of subscription plans that differ on the number of users that can be created within an account and the number of devices that can concurrently receive streaming content at the same time. Some content providers offer family plans that allow users to stream unlimited concurrent streams within their physical household. It is important to accurately define a household for the family for the successful implementation of such plans. This disclosure describes the use of real-time IP address detection to dynamically define a household for a subscription account. The techniques do not store any information such as MAC address, DMA code etc. and are also tolerant of IP address changes and household moves/changes.

REFERENCES

1. https://www.independent.co.uk/life-style/gadgets-and-tech/netflix-password-sharing-account-rules-friends-family-a9166316.html accessed 21 Sep 2020.