

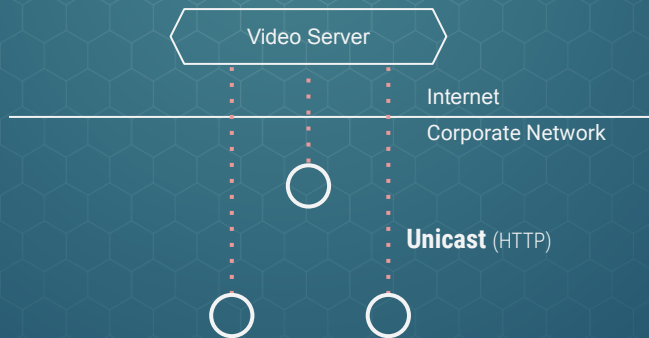


Web & Networks - eCDN

Stream video to any number of employees  
without breaking the corporate network

# Problem: streaming video at scale breaks corporate networks

- Streaming live video at scale behind the firewall creates **congestion**
- During large internal events, such as all-hands meetings, everyone watches at the same time, the network gets saturated and **video quality drops**. Other apps are impacted too.



# Intro: Streaming (HLS/DASH) vs Real Time Protocols

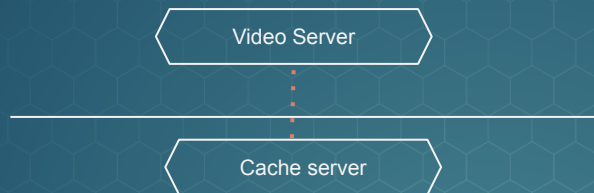
HTTP Streaming con: latency > 1 sec

HTTP Streaming pros:

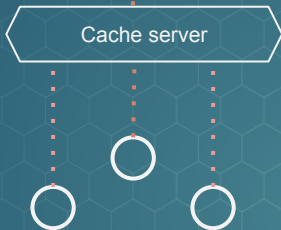
1. No packet drops and jittery video, since there's buffer on the client side
2. More efficient encoding which leads to better picture resolution on the same bitrate
3. Cheaper - simple *stateless* servers can cache video segments (CDN)
4. Standard and interoperable - play on *any* device without a client. Benefit from de facto industry libraries and open video players with features such as captioning, ABR, DVR, etc
5. Mitigate network congestion with peer assisted delivery

# Solution: eCDN technologies

1. Caching



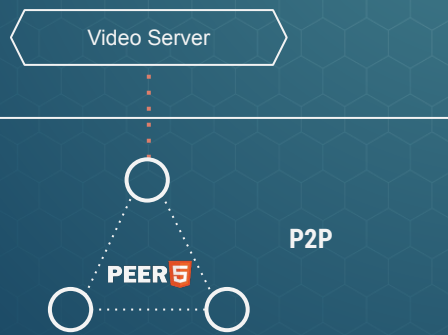
2. Multicast



Multicast router 1

Multicast router 2

3. P2P



# p2p technologies – no client implementation

1. Using WebRTC
2. Contained to the browser



# WebRTC P2P Challenges - I

**Offices segmentation problem** - keep traffic over “cheap” connections

- a. Office - to - office links are expensive
- b. Remote home - to - office (VPN) is expensive
- c. Identify the offices and keep traffic local

Solved problem using traceroute



# WebRTC P2P Challenges - I

**Standardization** - Allow network primitives from within the browser.

Traceroute problems:

1. Fingerprinting privacy aspect
2. ICMP attacks

Mitigation:

1. Create a flag or a policy to enable the API if desired on specific origins



# WebRTC P2P Challenges - II

## VPNs - don't p2p over virtual paths

Virtual paths are expensive and makes no sense to p2p over them.

While natively it's quite easy to understand if the device's routing is using a virtual NIC, inside the browser it's impossible

**Standardization** - Allow exposing the NICs used on the devices, and their type (loopback, ethernet, wifi, vpn).

problems:

1. Fingerprinting privacy aspect

Mitigation:

1. Create a flag or a policy to enable the API if desired on specific origins





# WebRTC P2P Challenges - II

**Standardization** - Allow network primitives from within the browser.

Traceroute problems:

1. Fingerprinting privacy aspect
2. ICMP attacks

Mitigation:

1. Create a flag or a policy to enable the API if desired on specific origins

