UNIVERSITY OF CALGARY

Packet-Level Analysis of Zoom Performance Anomalies

Mehdi Karamollahi, Carey Williamson, and Martin Arlitt

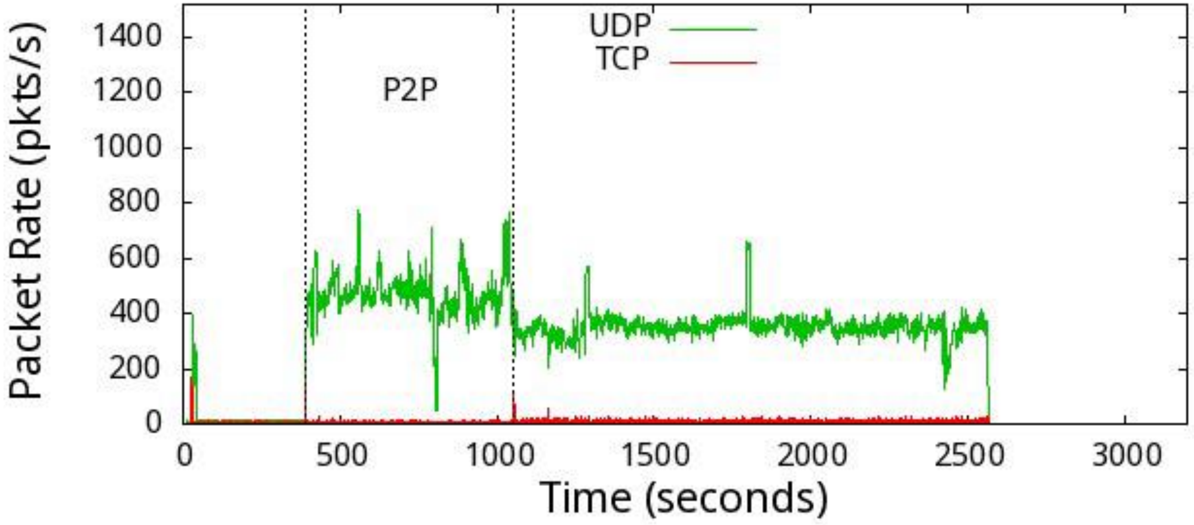
ACM/SPEC ICPE 2023

Coimbra, Portugal

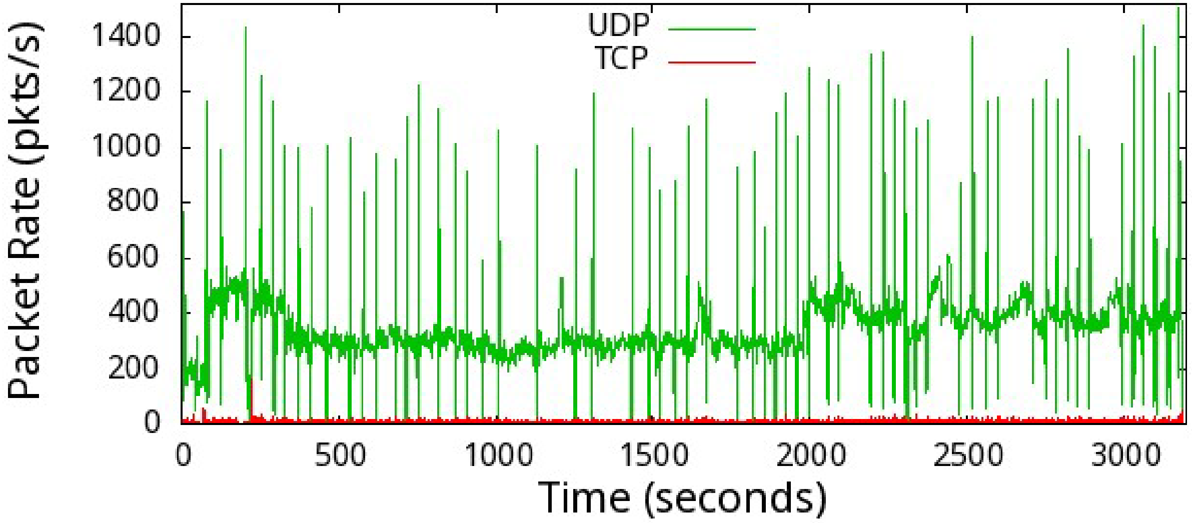
Motivation

Many Zoom performance problems on our campus network during the Fall 2021 semester:

Trace A (August 31, 2021)



Trace B (October 6, 2021)



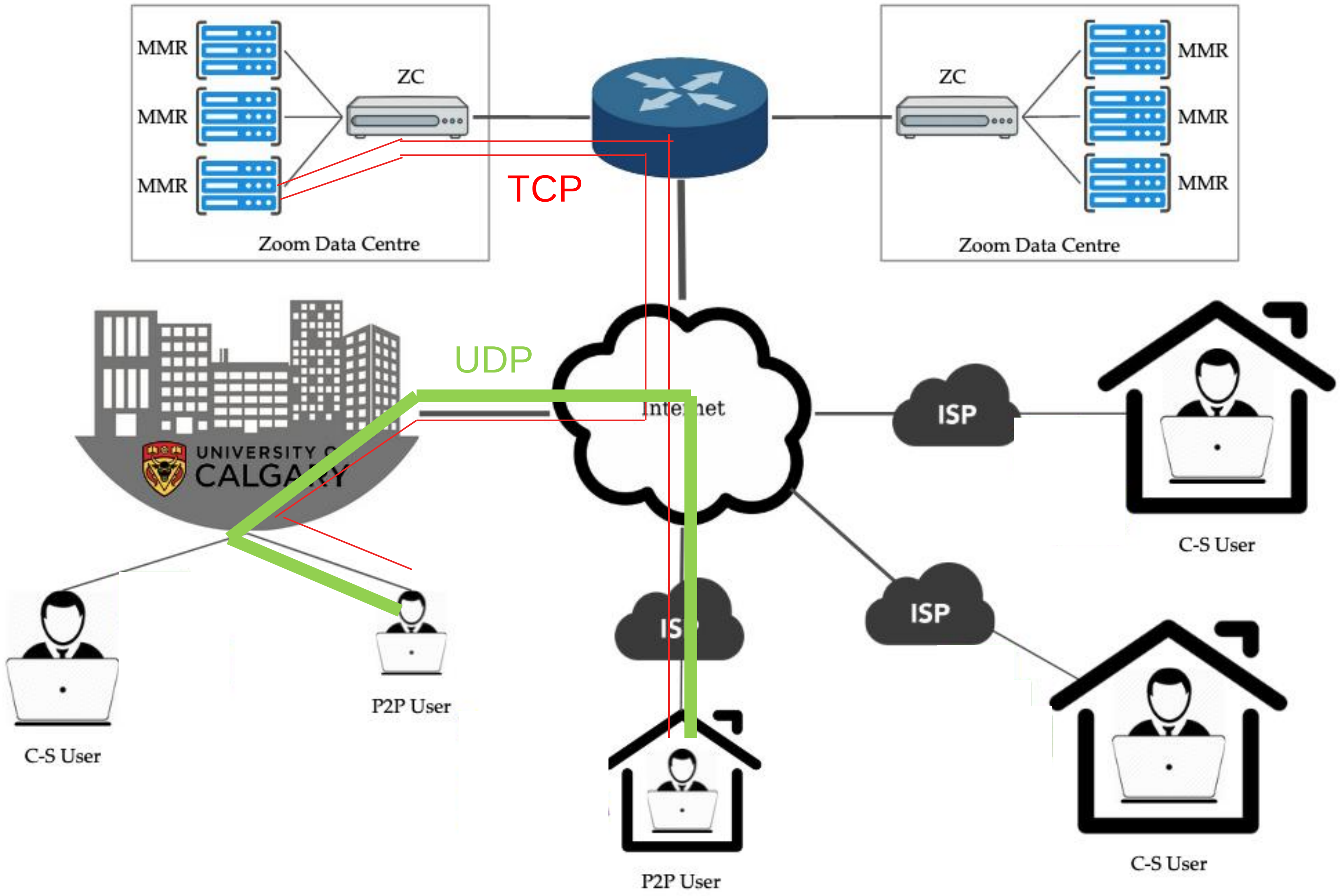
Why?

Objectives

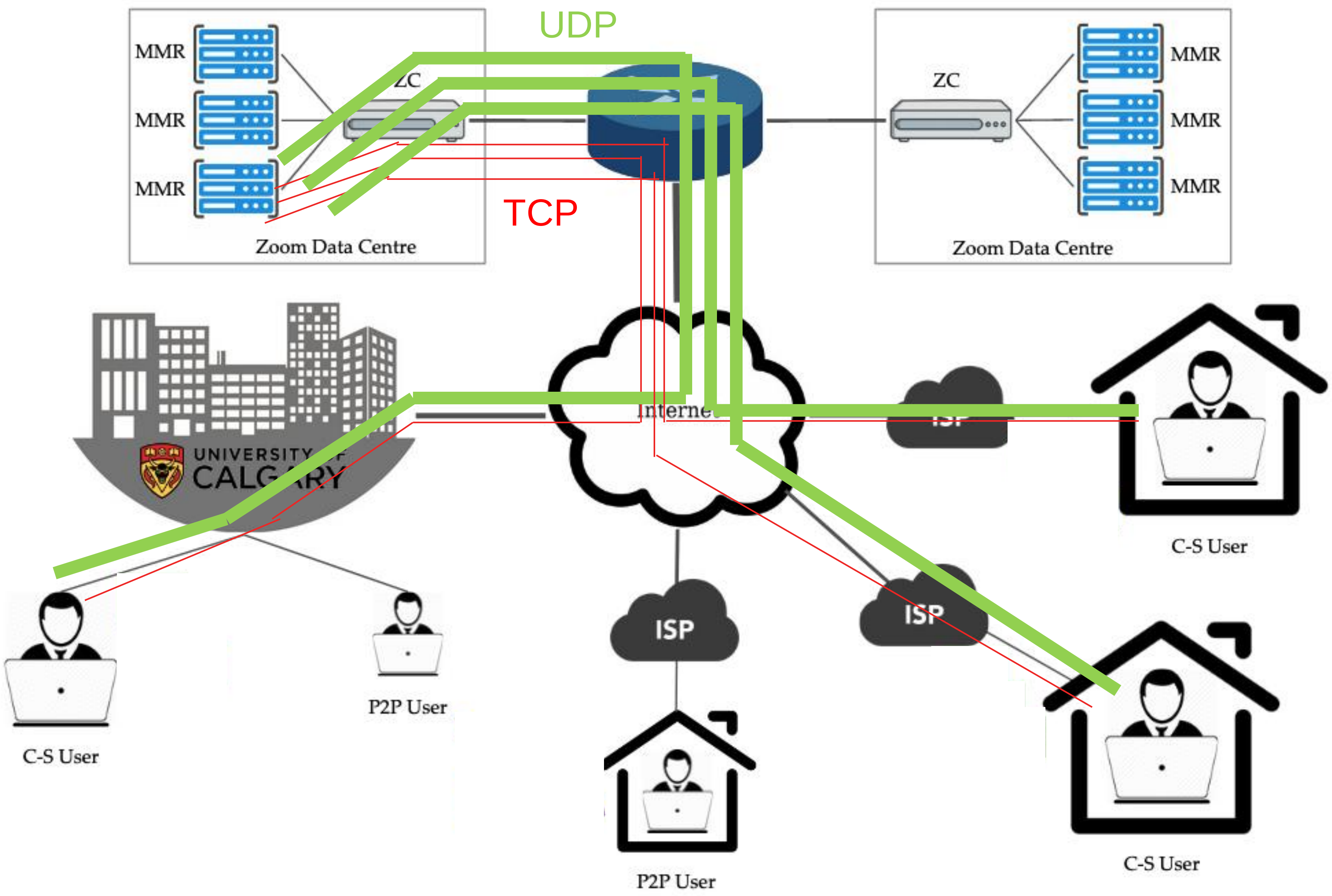
- To understand the structural properties of Zoom traffic
- To determine why these Zoom performance anomalies occurred
- To provide recommendations to improve Zoom performance on enterprise-level networks like our campus network

Approach: Packet-level analysis of Wireshark traces of Zoom test sessions (see appendix of paper for Wireshark basics and a link to a video demo)

Zoom Overview: Peer-to-Peer (P2P) Mode

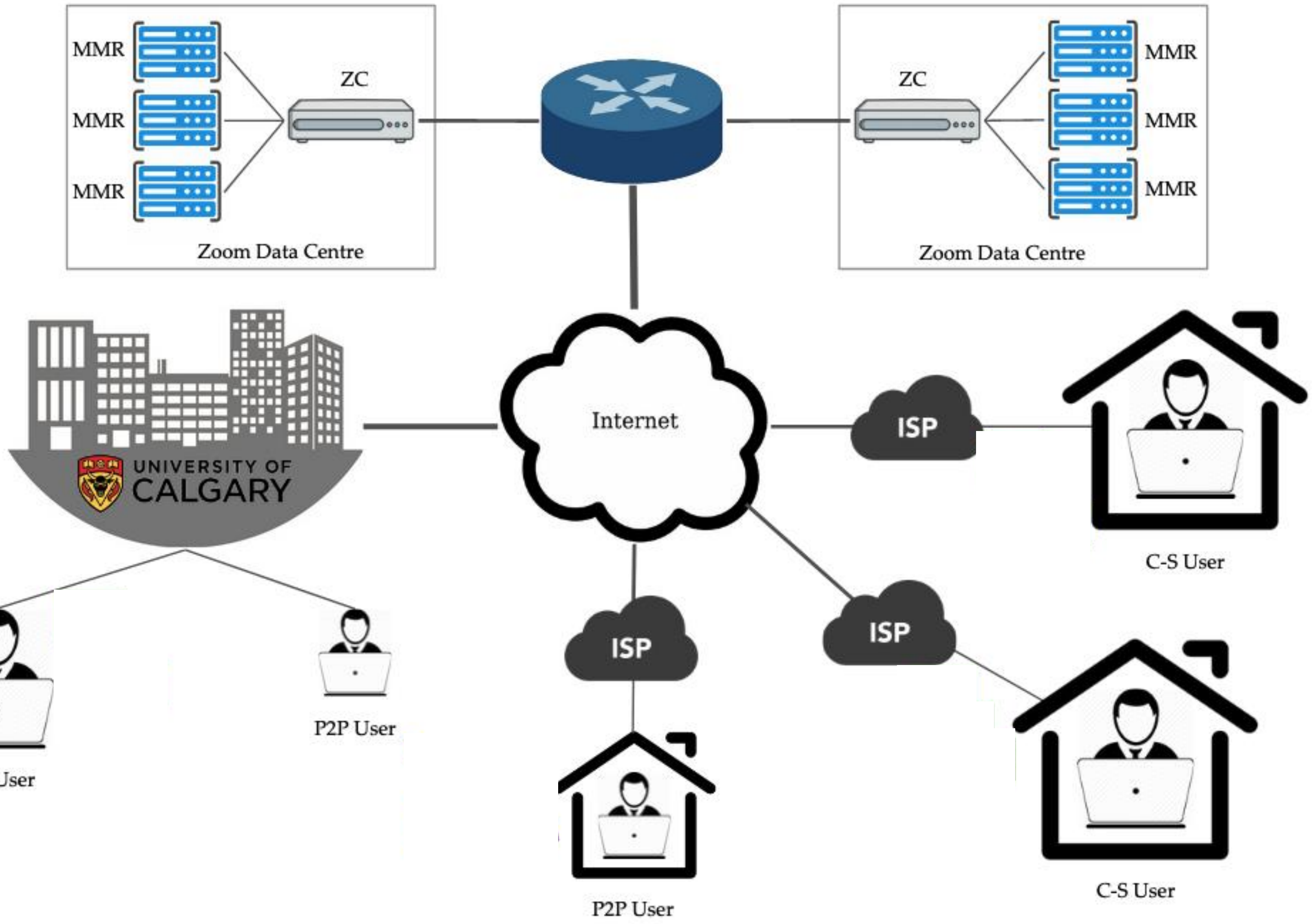


Zoom Overview: Client-Server Mode



Answer: The Perfect Storm

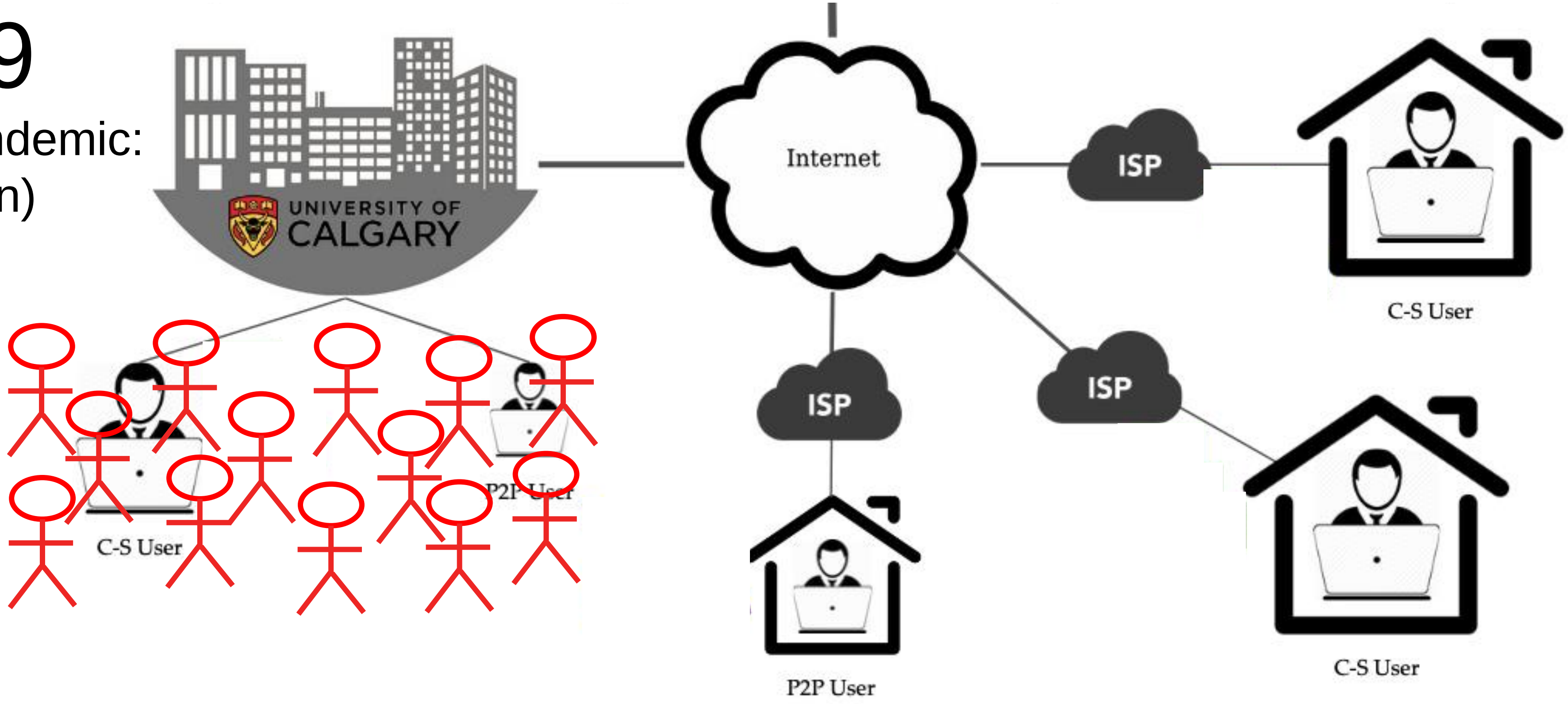
People
Protocols
Patterns
Policies
Performance
Peculiarities



The Perfect Storm: People

2019

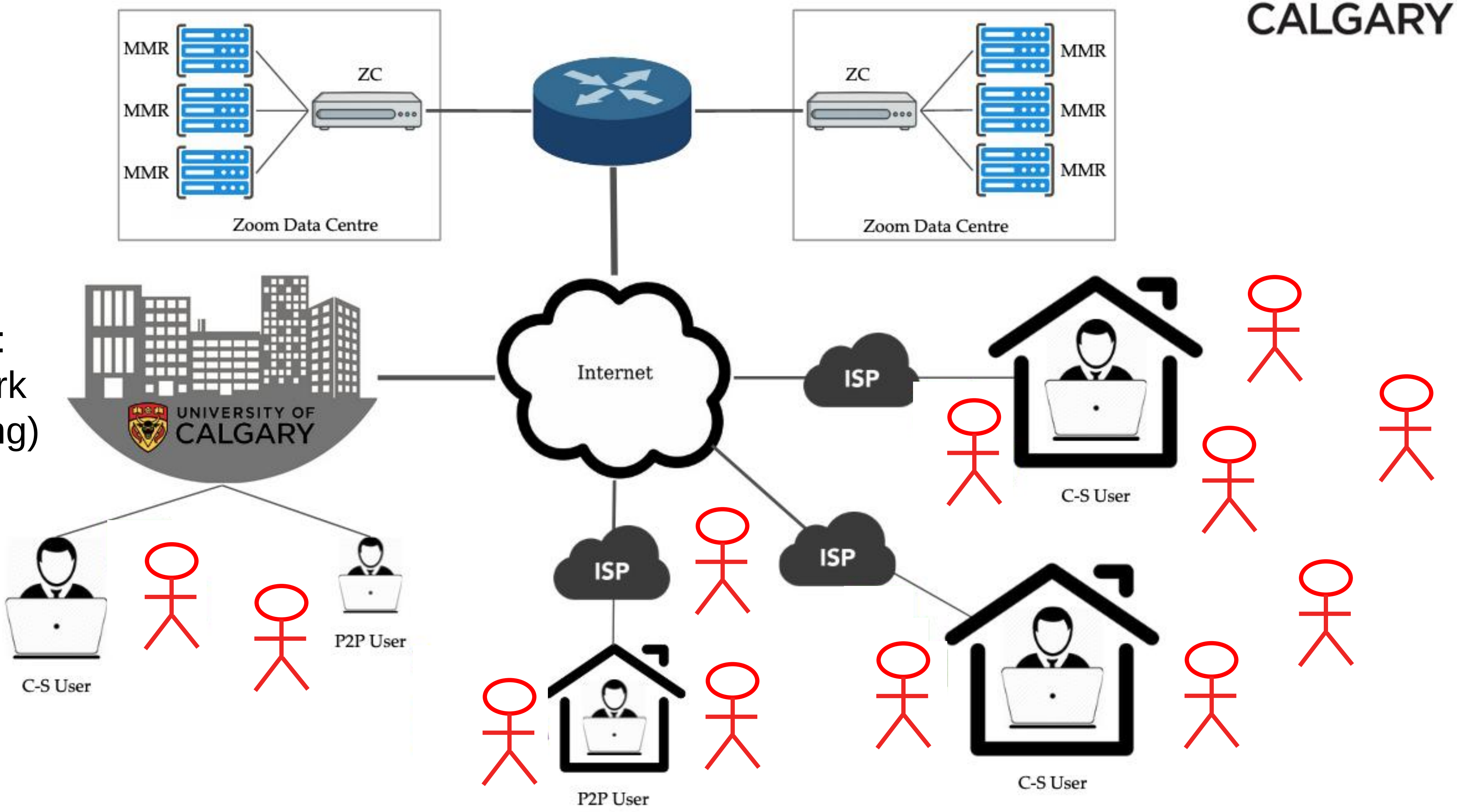
(pre-pandemic: in person)



The Perfect Storm: People

2020

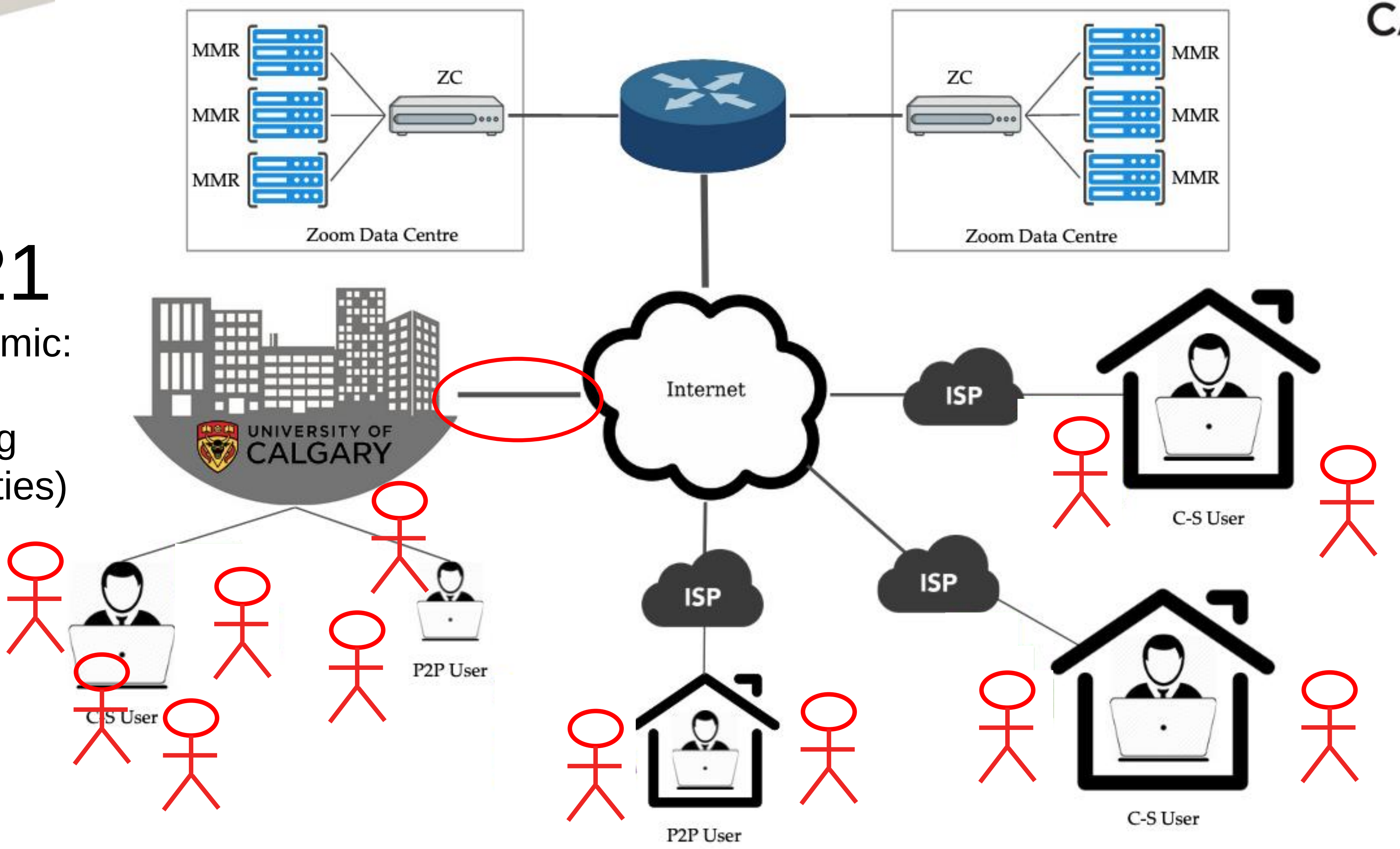
(pandemic: remote work and learning)



The Perfect Storm: People

2021

(pandemic: hybrid learning modalities)

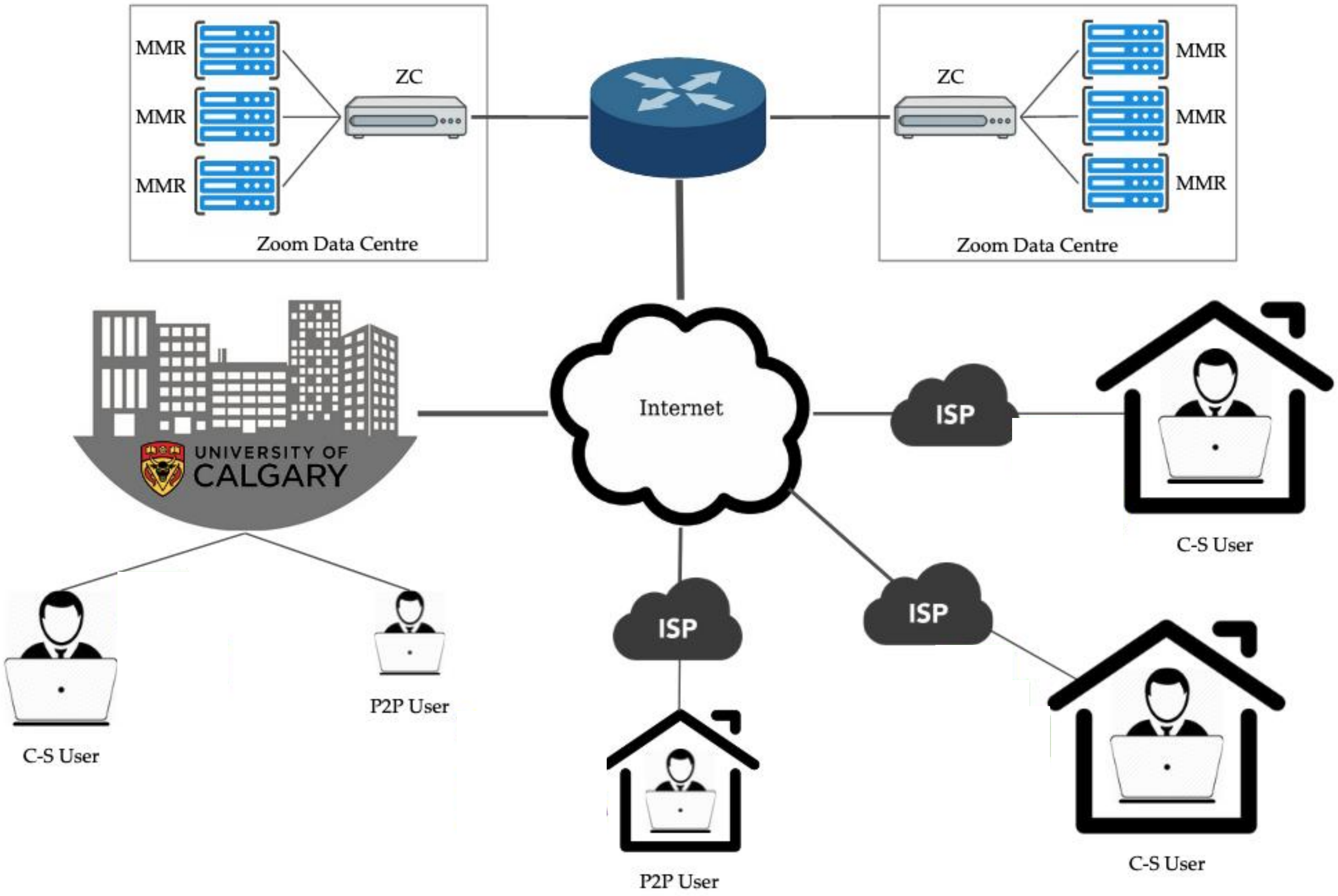


The Perfect Storm: Protocols

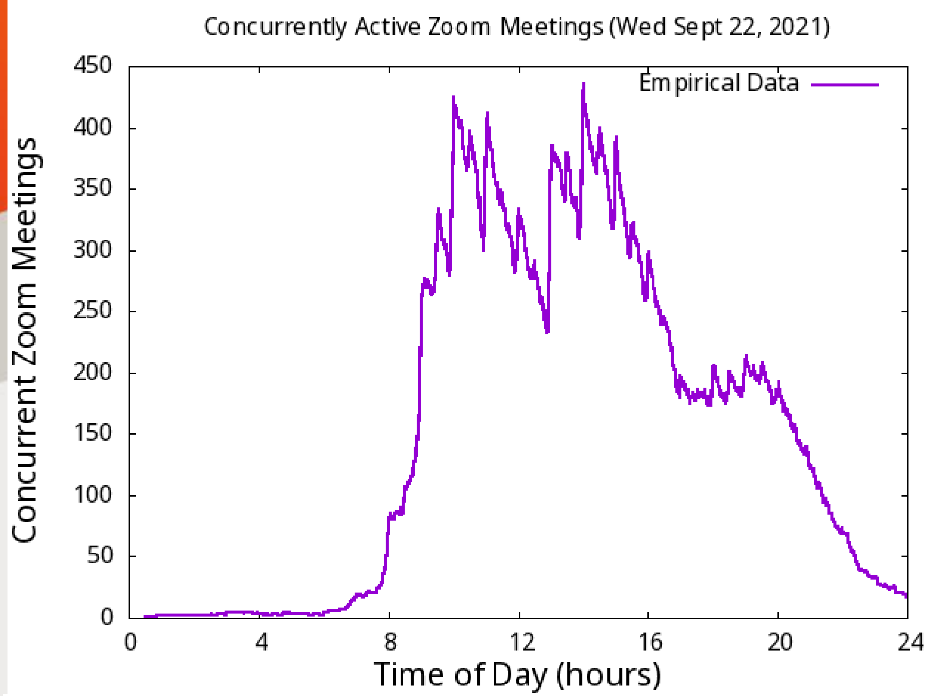
Zoom uses both TCP and UDP

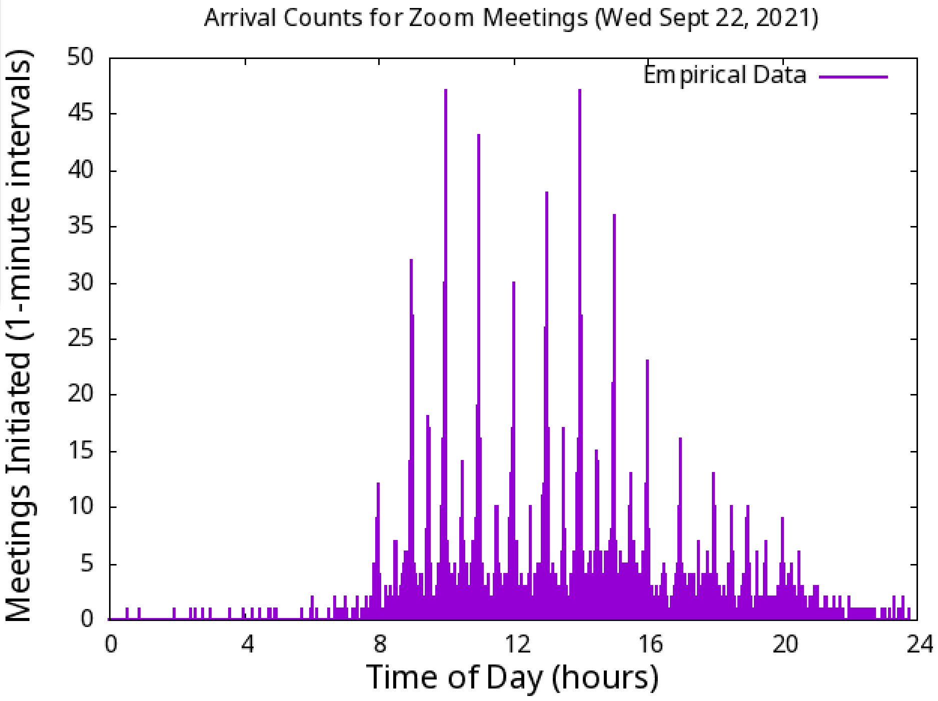
TCP uses congestion control

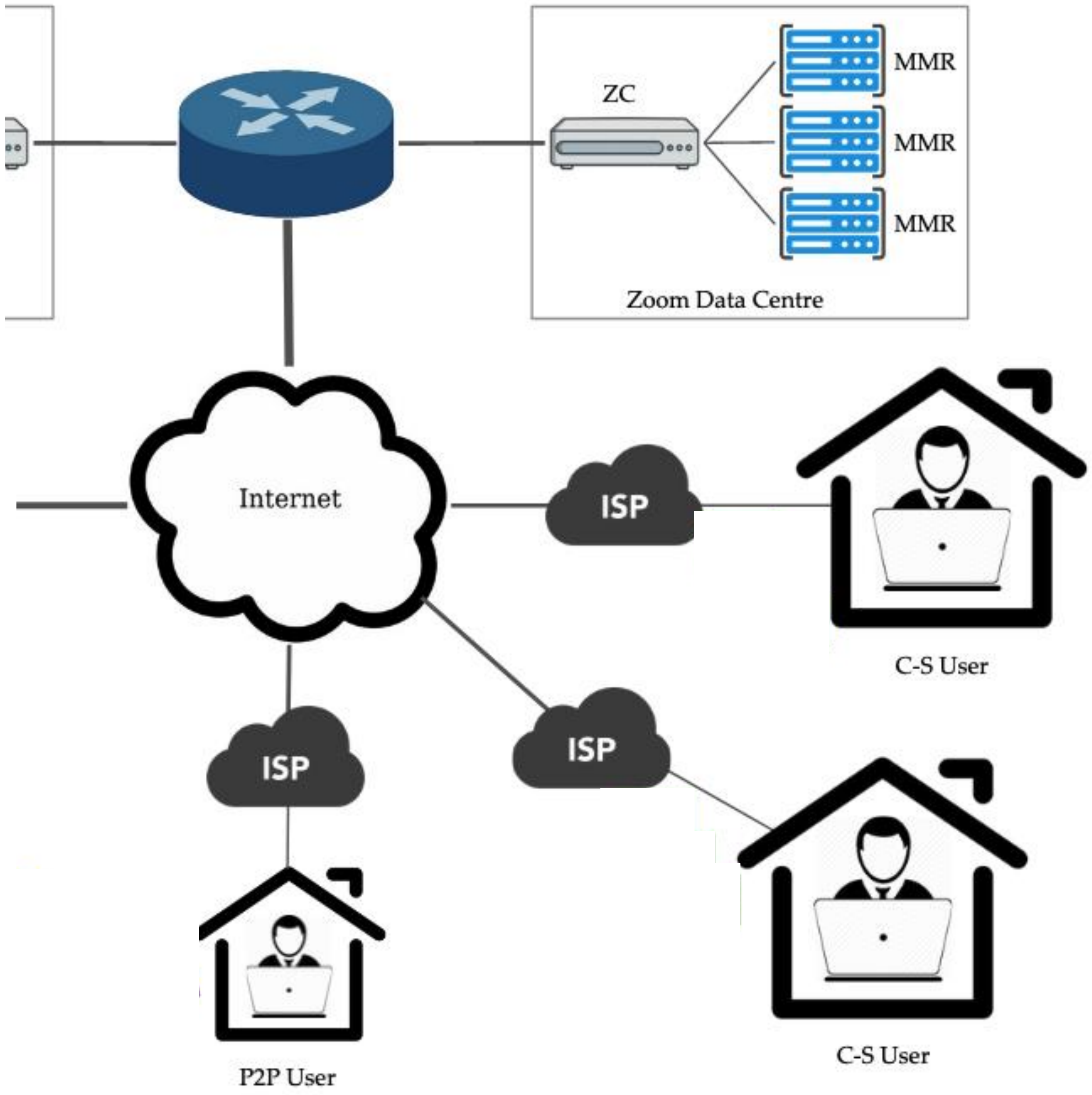
UDP does not



…rfect Storm: Patterns







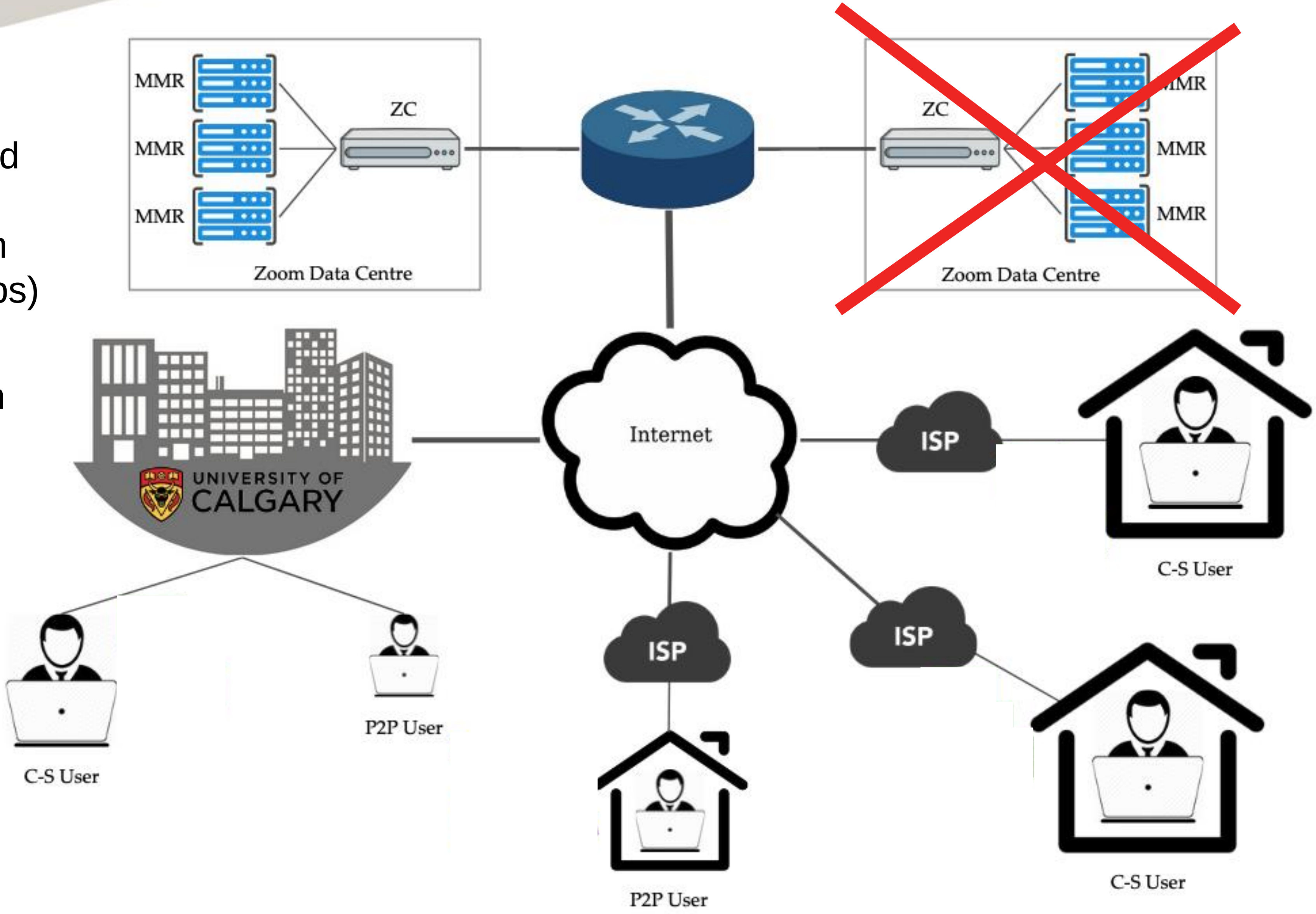
Zoom traffic is non-stationary with distinct spikes at class start times (high demand)

The Perfect Storm: Policies

Licensed version of Zoom (> 1Mbps)

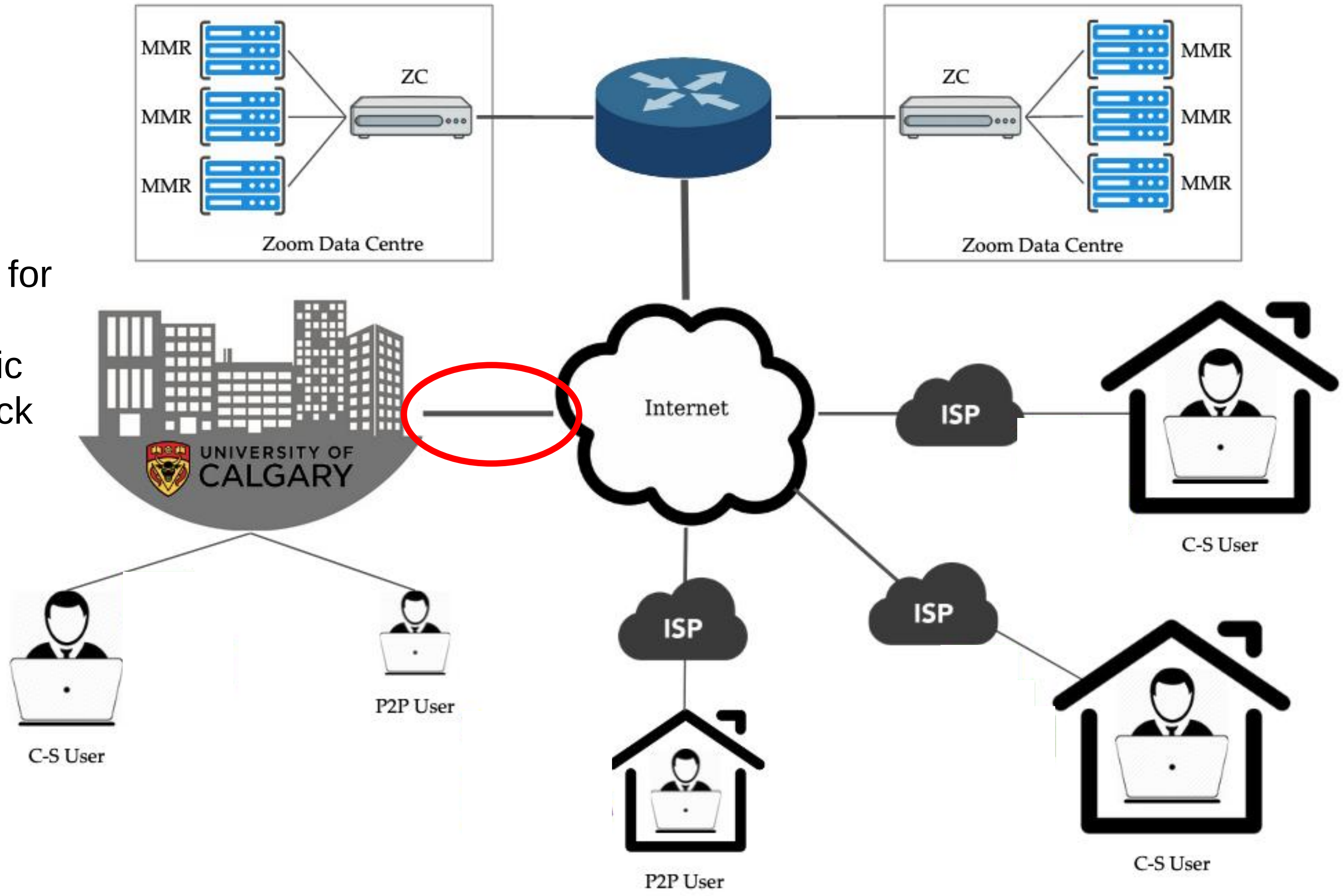
Use Zoom servers in Canada (limited supply)

Use the commercial Internet link (6 Gbps)



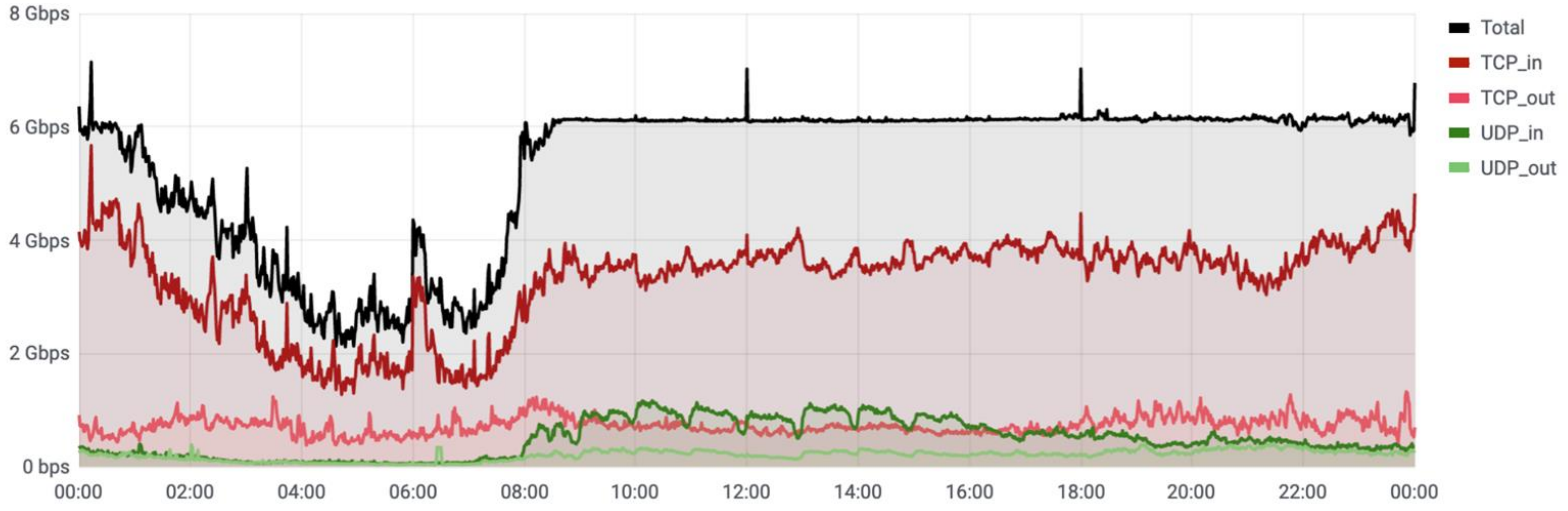
The Perfect Storm: Performance

External link for commercial Internet traffic is a bottleneck (6 Gbps)



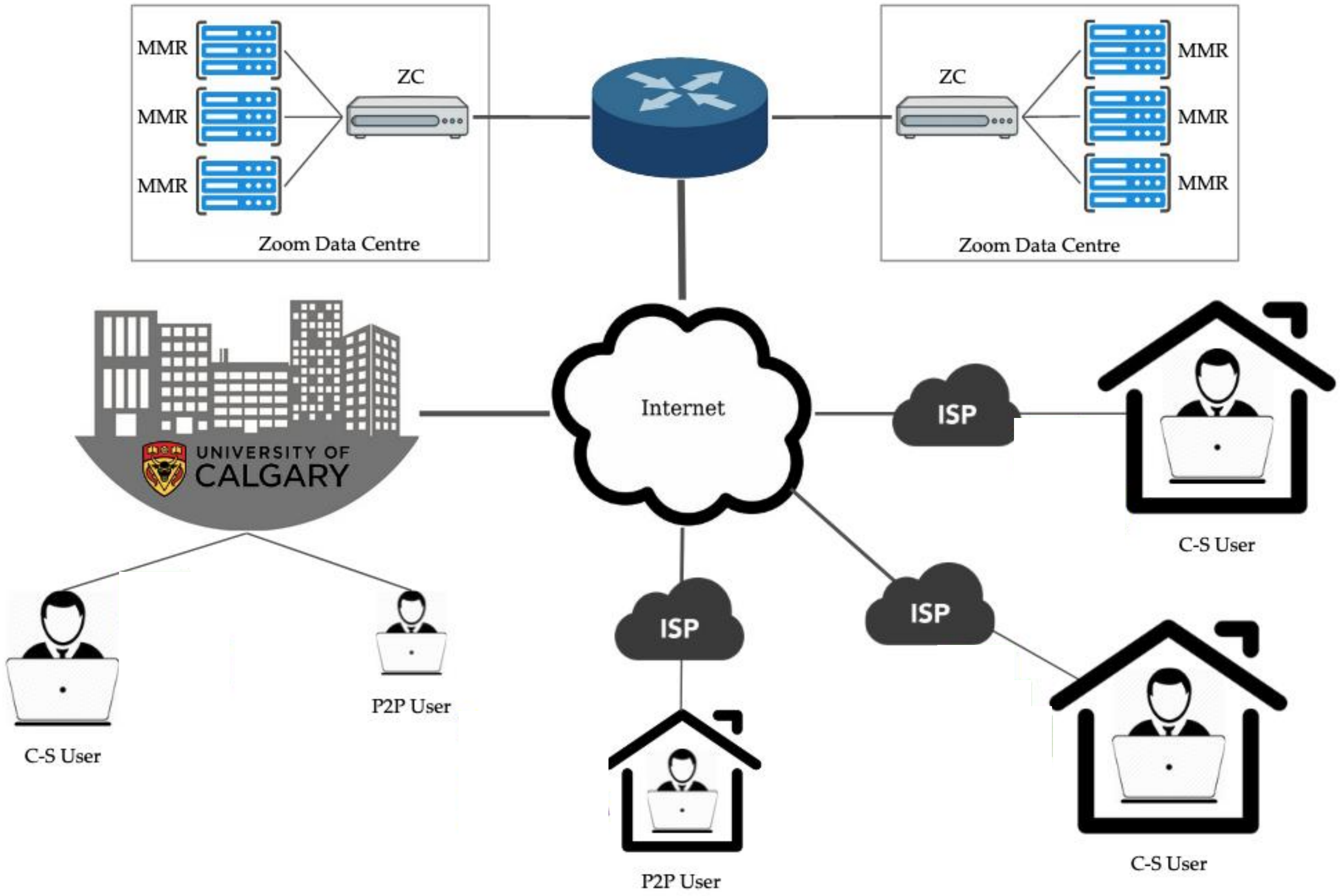
Root Cause of Problems: Congested Bottleneck Link

UNIVERSITY OF CALGARY



Usage of campus external link for commercial Internet traffic (October 6, 2021)

The Perfect Storm: Peculiarities



Zoom does <u>not</u> share bandwidth fairly with other applications

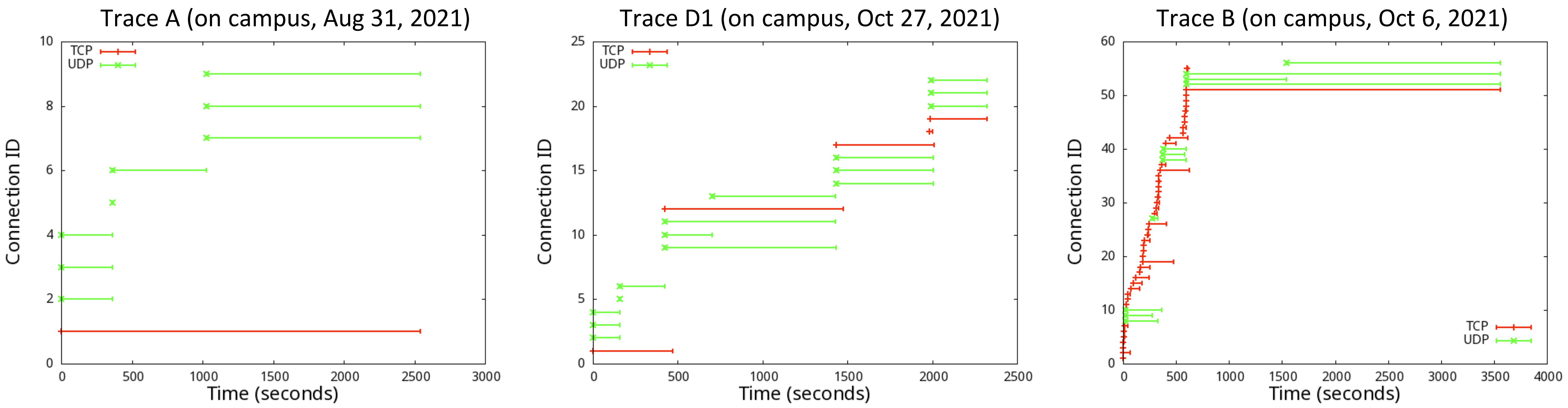
Zoom is quite aggressive with its bandwidth probing algorithm (see details later)

Zoom Wireshark Traces

Wireshark Trace Metadata						
Trace	Date	Time	Location	Mode	Duration	Packets
A	Tue Aug 31 2021	12:08pm	Campus	P2P	11 min	315,666
			Campus	C-S	32 min	559,827
B	Wed Oct 6	2:08pm	Campus	C-S	53 min	1,114,451
C1	Wed Oct 13 2021	12:58pm	Campus	P2P	36 min	884,467
C2		1:00pm	Home	P2P	34 min	844,538
D1	Wed Oct 27 2021	12:57pm	Campus	P2P	4 min	94,400
			Campus	C-S	35 min	653,494
D2		1:02pm	Home	P2P	2 min	37,612
			Home	C-S	32 min	593,973

Connection-Level Analysis of Zoom Test Sessions

UNIVERSITY OF CALGARY

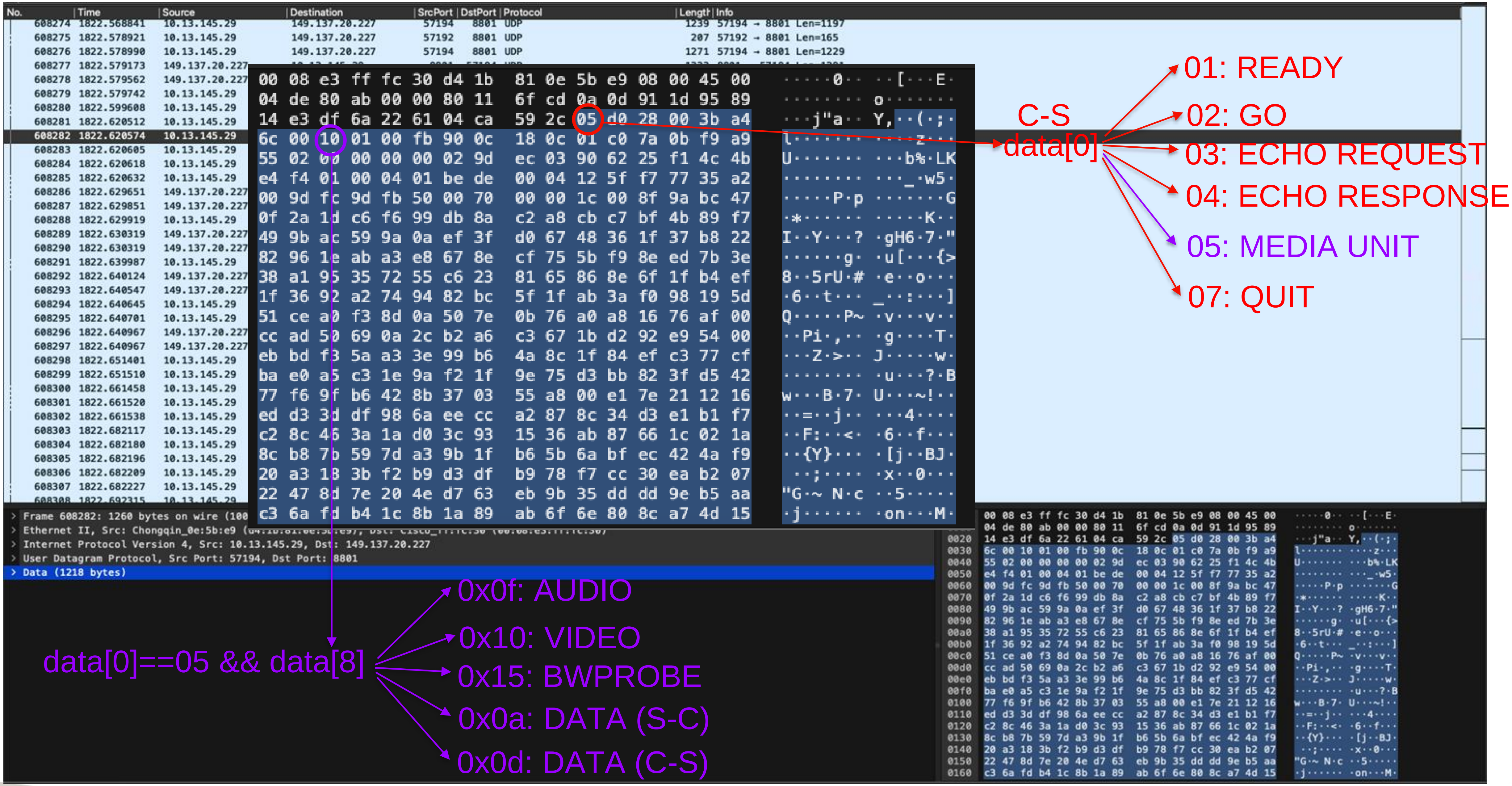


Key Insight: Zoom “breaks” in many different ways, but is highly resilient.

Packet-Level Analysis: Empirical Observations

UNIVERSITY OF CALGARY

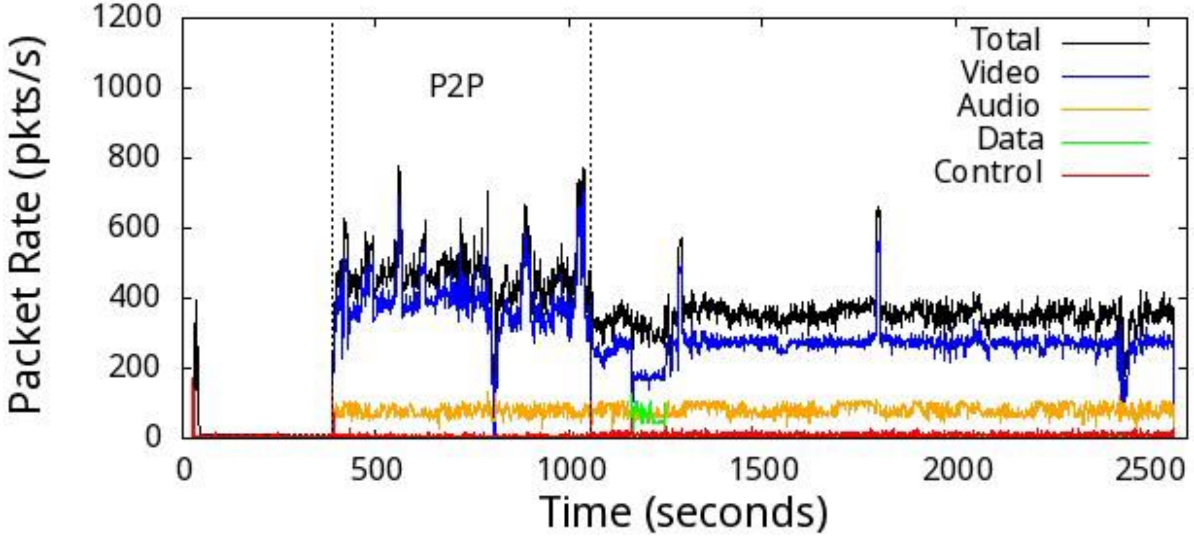
- There are unencrypted protocol headers carried in Zoom’s UDP packets.
- The first byte of the payload (`data[0]`) indicates an opcode.
- In C-S mode, over 90% of UDP packets carry opcode 0x05 (media unit).
  - At client side: 3 separate UDP ports (video, audio, screen-sharing)
  - At server side: a single UDP port (8801) for all media traffic
- In C-S mode, there are periodic timing probes for each client port.
- Within each media type, there are 16-bit sequence numbers.
- In P2P mode, the opcode functionality appears in a different position.



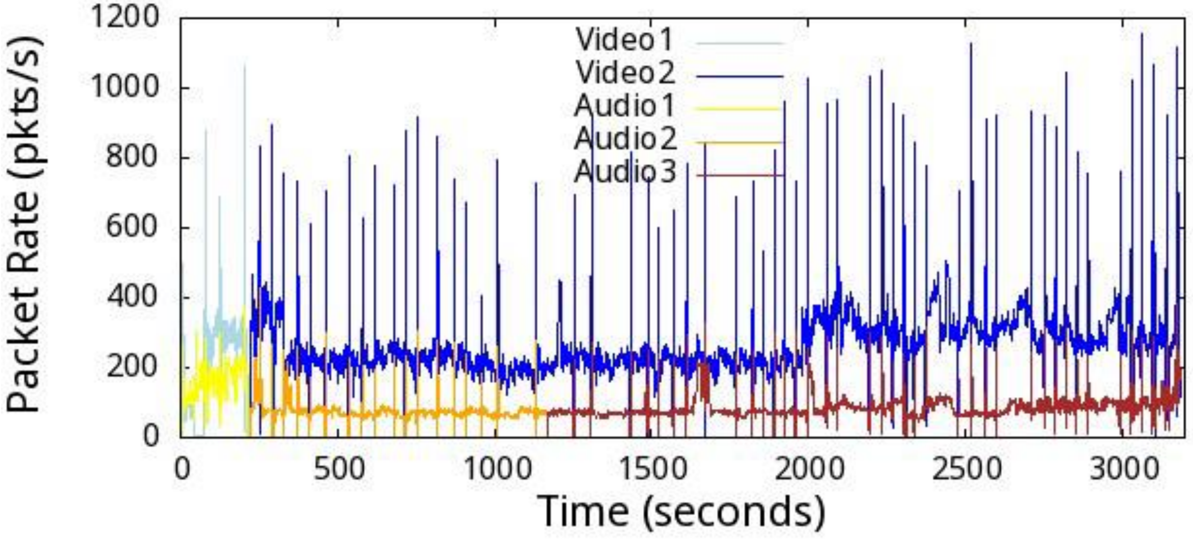
C-S
data[0]
01: READY
02: GO
03: ECHO REQUEST
04: ECHO RESPONSE
05: MEDIA UNIT
07: QUIT
data[0]==05 && data[8]
0x0f: AUDIO
0x10: VIDEO
0x15: BWPROBE
0x0a: DATA (S-C)
0x0d: DATA (C-S)
Frame 608282: 1260 bytes on wire
Internet Protocol Version 4, Src: 10.13.145.29, Dst: 149.137.20.227
User Datagram Protocol, Src Port: 57194, Dst Port: 8801
Data (1218 bytes)

Media Stream Analysis

Trace A (August 31, 2021)

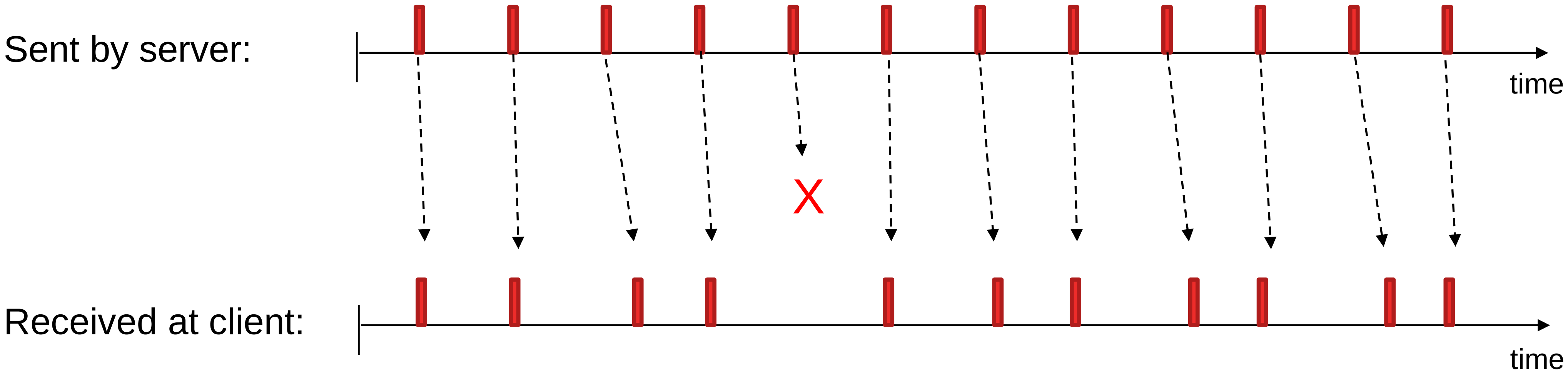


Trace B (October 6, 2021)



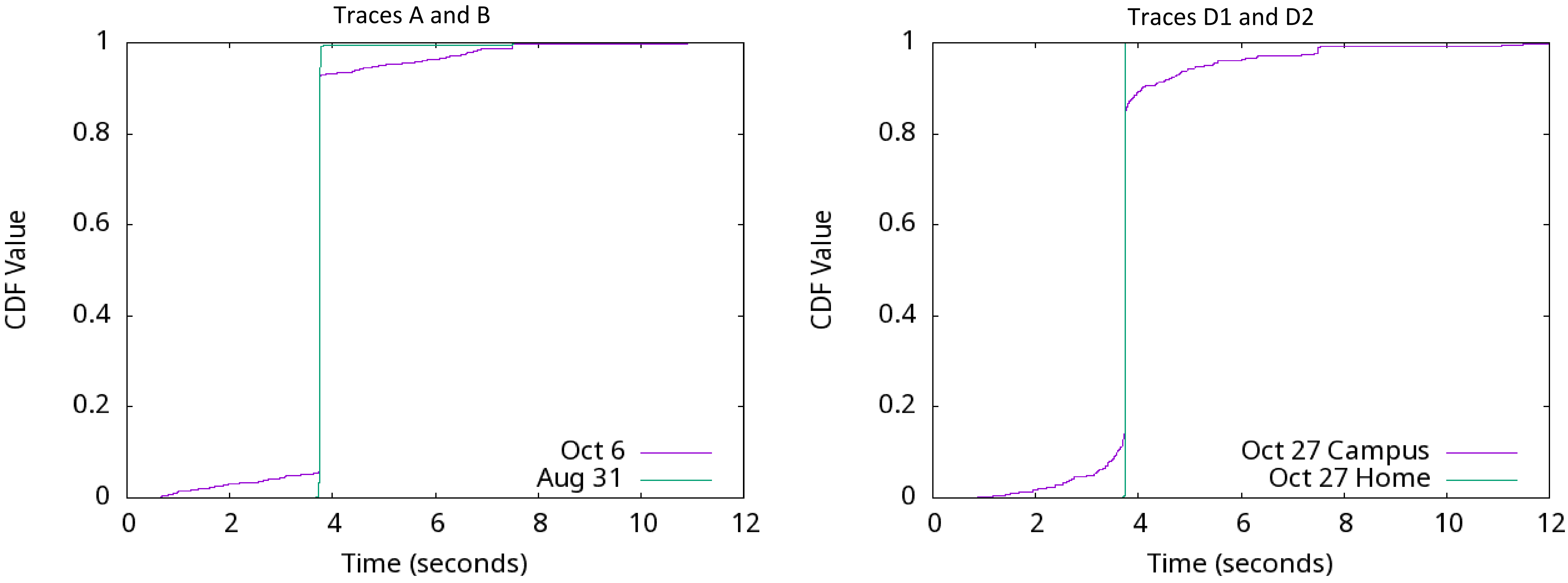
Key Insight: We can analyze each Zoom media stream separately.

Delay and Jitter Analysis from Timing Probes (3.75 sec)



Delay and Jitter Analysis from Timing Probes (3.75 sec)

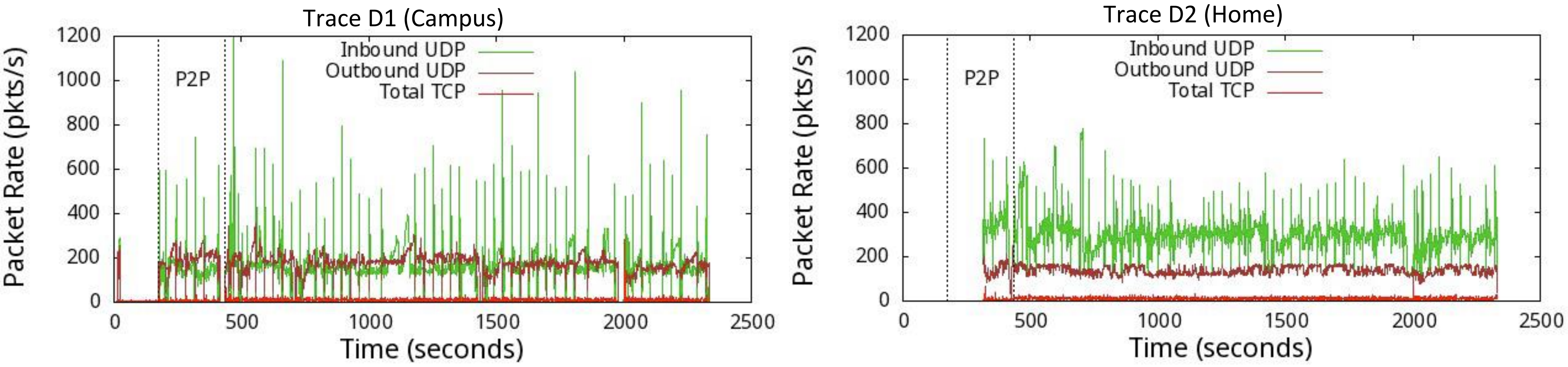
UNIVERSITY OF CALGARY



Key Insight: The bottleneck is located on the campus network.

Directionality Effects

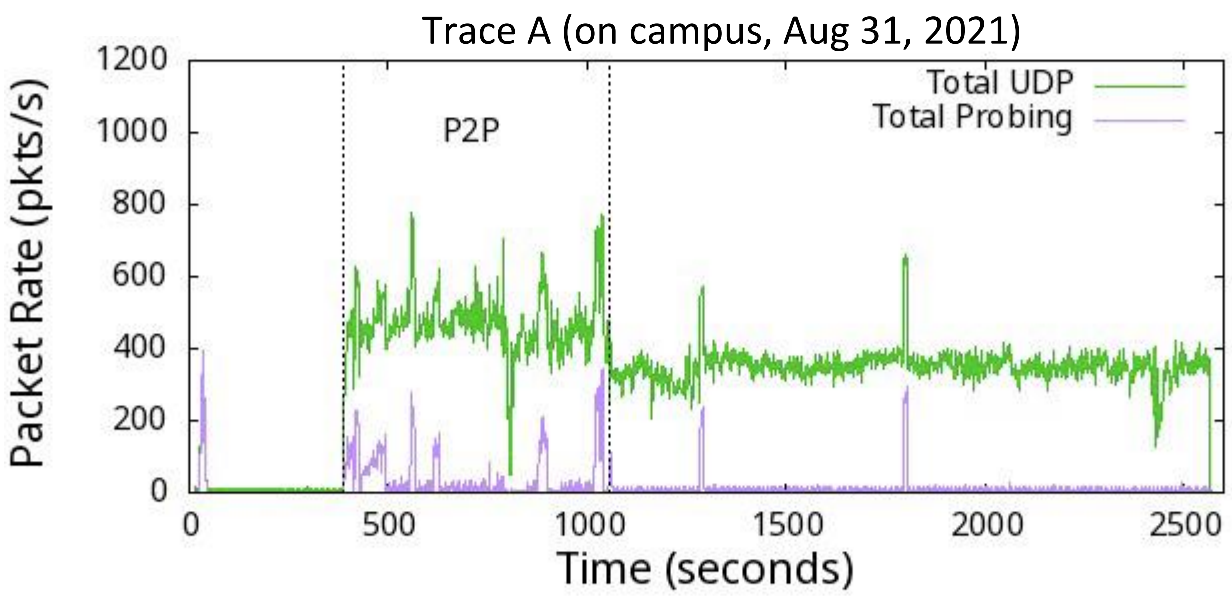
Directional analysis of UDP traffic in a Zoom test session (Oct 27, 2021):

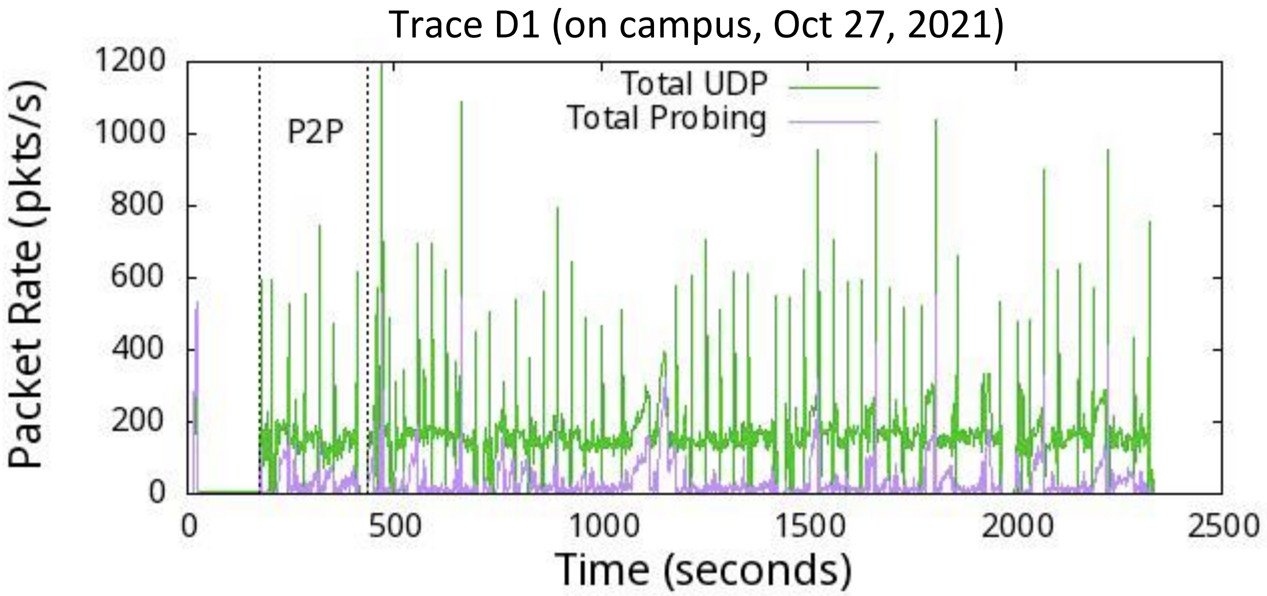


Key Insight: The bottleneck affects both inbound and outbound traffic.

Bandwidth Probing (1 of 2)

Analysis of video bandwidth probing traffic in Zoom test sessions:

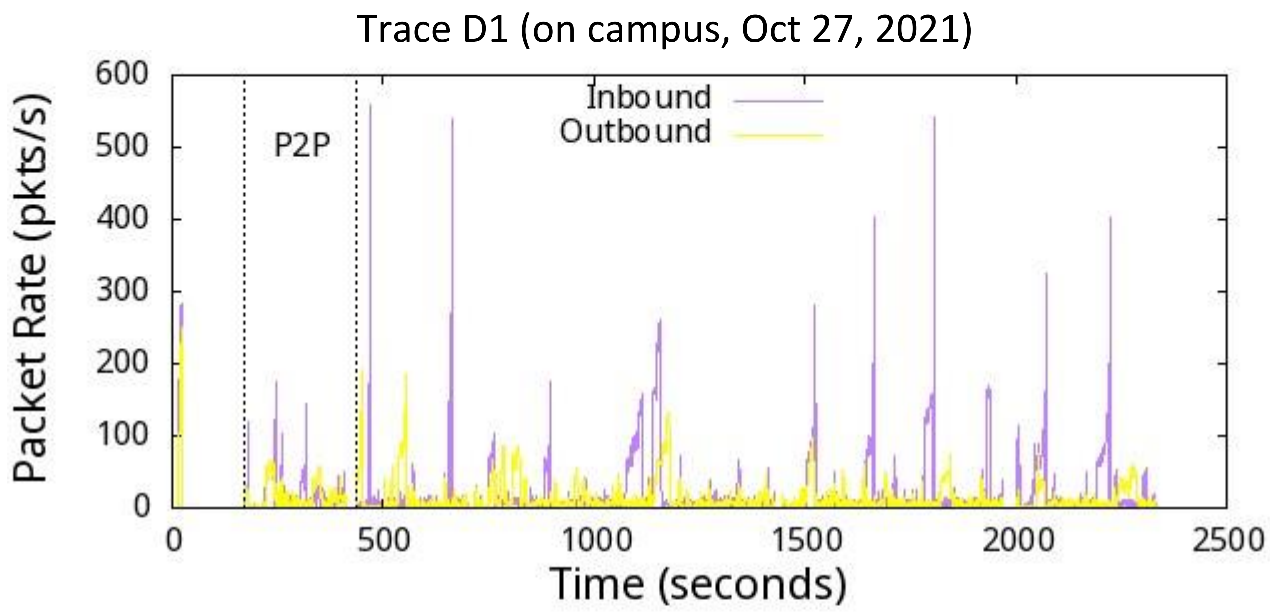


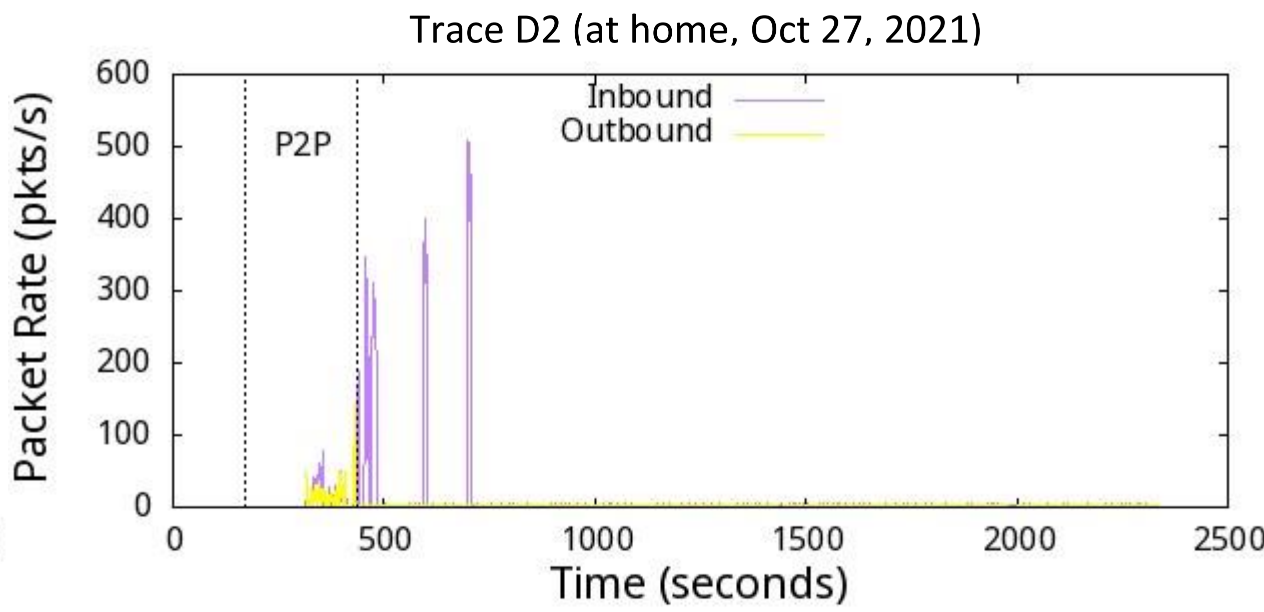


Key Insight: Bandwidth probing happens more often on a congested network.

Bandwidth Probing (2 of 2)

Directional analysis of video bandwidth probing traffic in Zoom test sessions:





Key Insight: Bandwidth probing is done on a per-user basis (even if co-located!).

Recommendations

UNIVERSITY OF CALGARY

- For University of Calgary network:
  - Could route Zoom traffic over the research/education link.
  - Could increase the bandwidth limit on the commercial link.
- For Zoom:
  - Better load-balancing across a larger pool of Zoom servers.
  - Less aggressive bandwidth probing (e.g., per network prefix vs per user).
  - Use advanced network protocols such as IP multicast, PIM, SRM, or QUIC when supporting a large number of co-located users.

Conclusions

UNIVERSITY OF CALGARY

- Zoom UDP packets carry unencrypted application-layer headers.
  - Packet loss can be estimated from media sequence numbers.
  - Delay and jitter can be estimated from the timing probes.
- Zoom is highly resilient to different network conditions.
  - Connection-level restart (TCP or UDP or both).
  - Dynamic bandwidth probing to adjust media bit rates.
- A congested external link is the root cause of Zoom-related problems.
- Multi-layer protocol interactions exacerbate Zoom performance issues (e.g., bandwidth probing, connection restarts, TLS handshakes).

Thank you for listening!

Questions?

You may also send your questions to carey@cpsc.ucalgary.ca

UNIVERSITY OF CALGARY