



UNIVERSITY OF
CALGARY

Packet-Level Analysis of Zoom Performance Anomalies

Mehdi Karamollahi, Carey Williamson, and Martin Arlitt

ACM/SPEC ICPE 2023

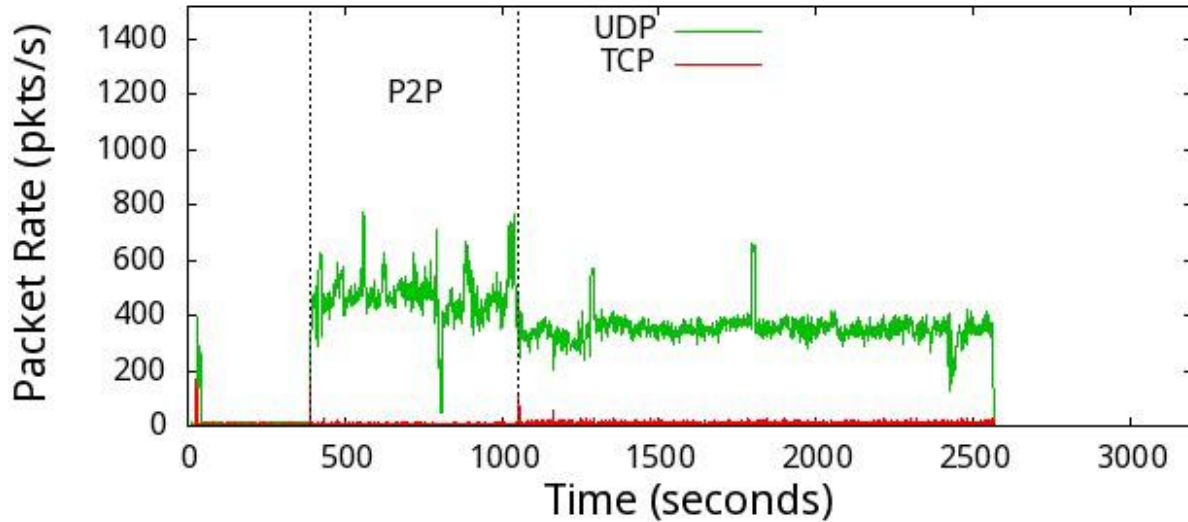
Coimbra, Portugal



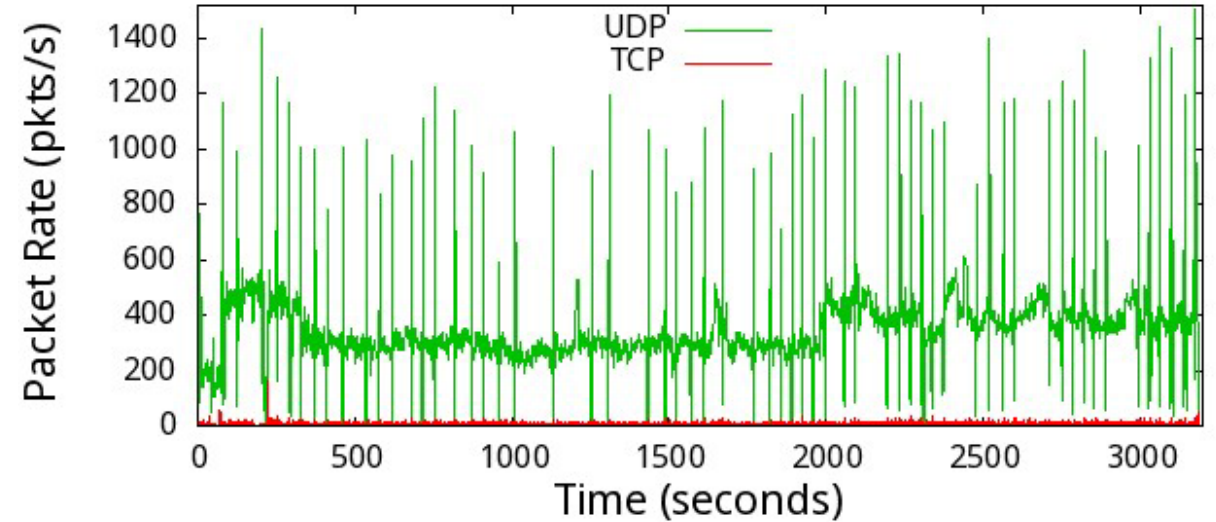
Motivation

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

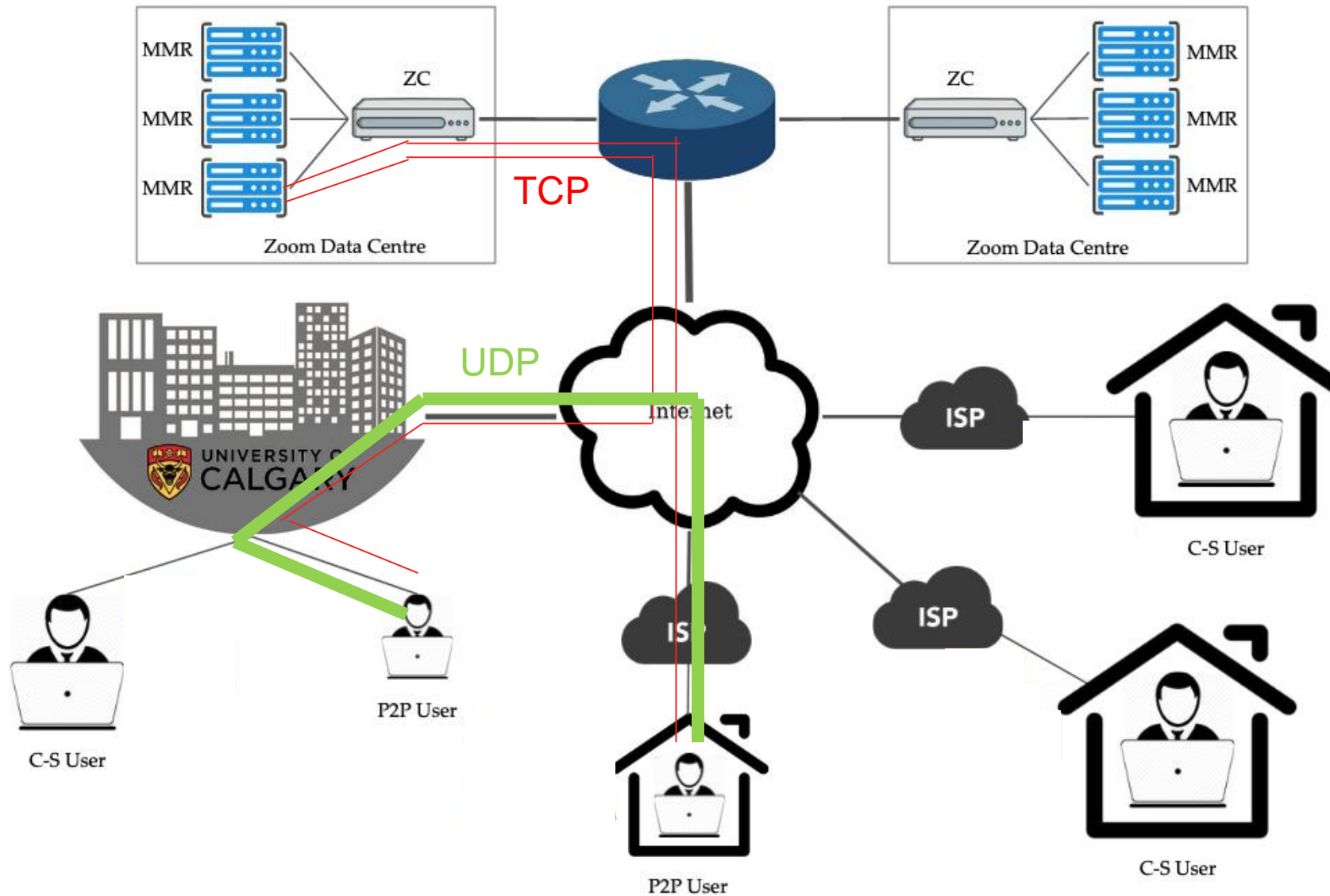
- To understand the structural properties of Zoom traffic
- To determine why these Zoom performance anomalies occurred
- To provide recommendations to improve Zoom performance on enterprise-level networks like our campus network

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)

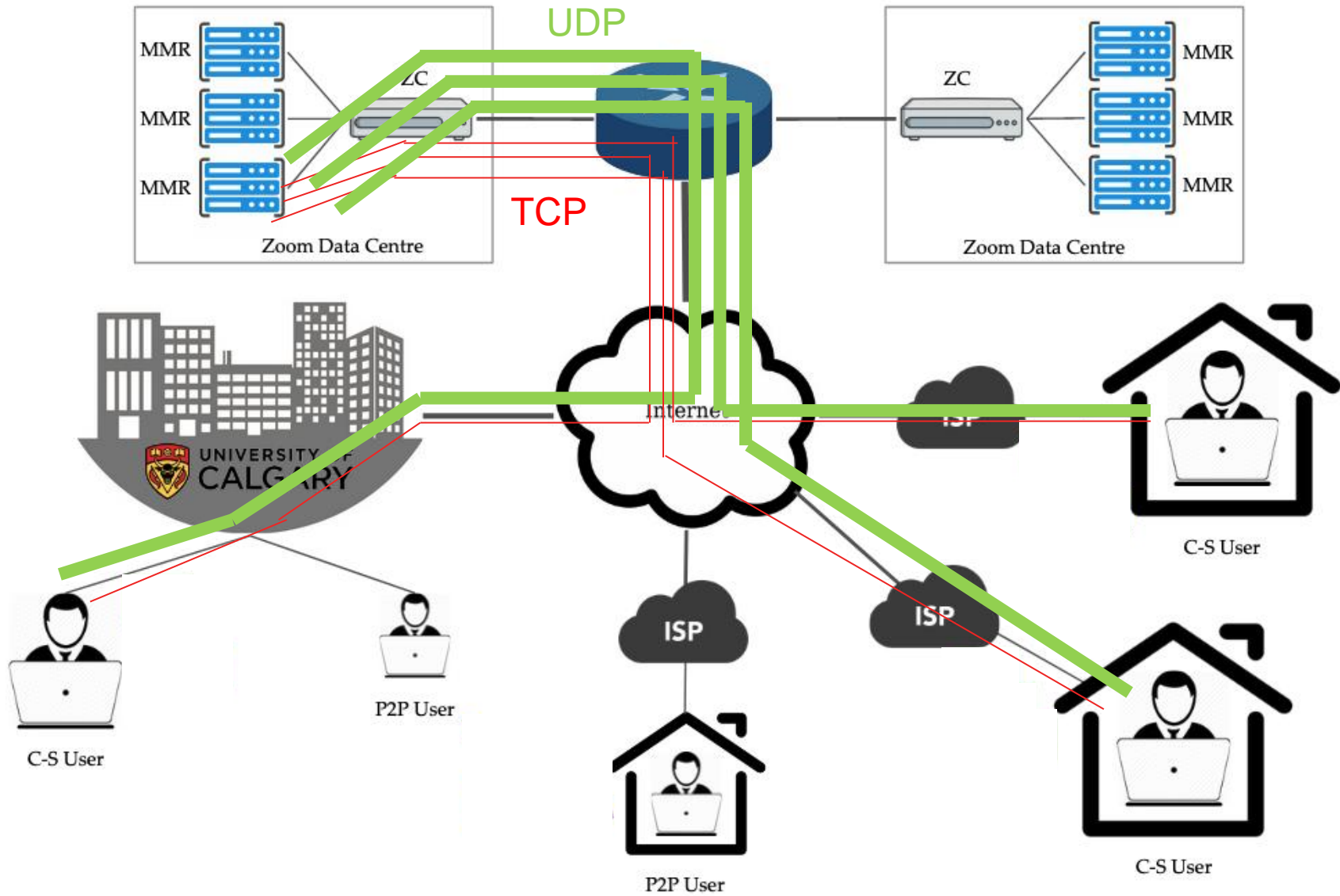
Zoom Overview: Peer-to-Peer (P2P) Mode



UNIVERSITY OF
CALGARY



Zoom Overview: Client-Server Mode

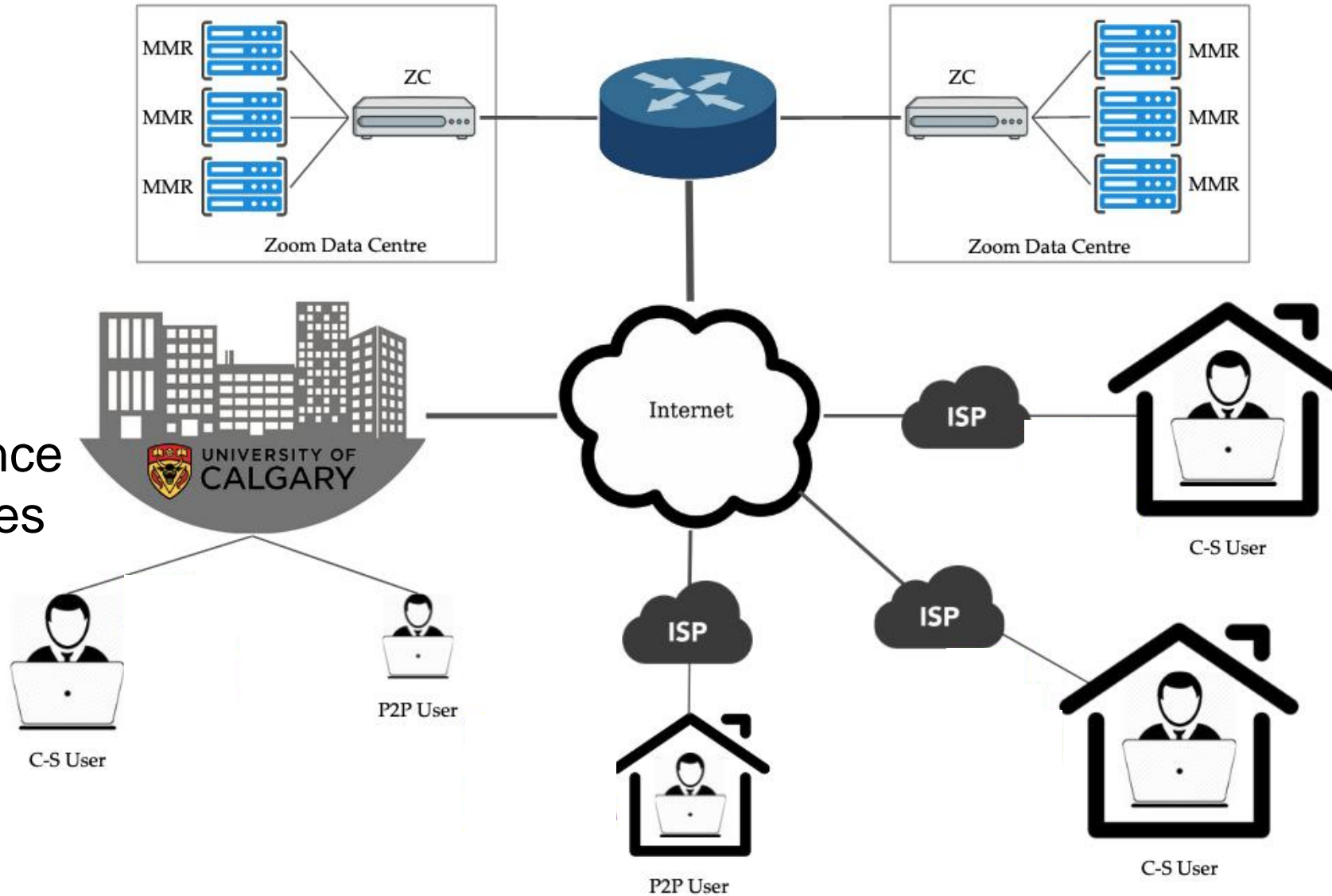


Answer: The Perfect Storm



UNIVERSITY OF
CALGARY

People
Protocols
Patterns
Policies
Performance
Peculiarities



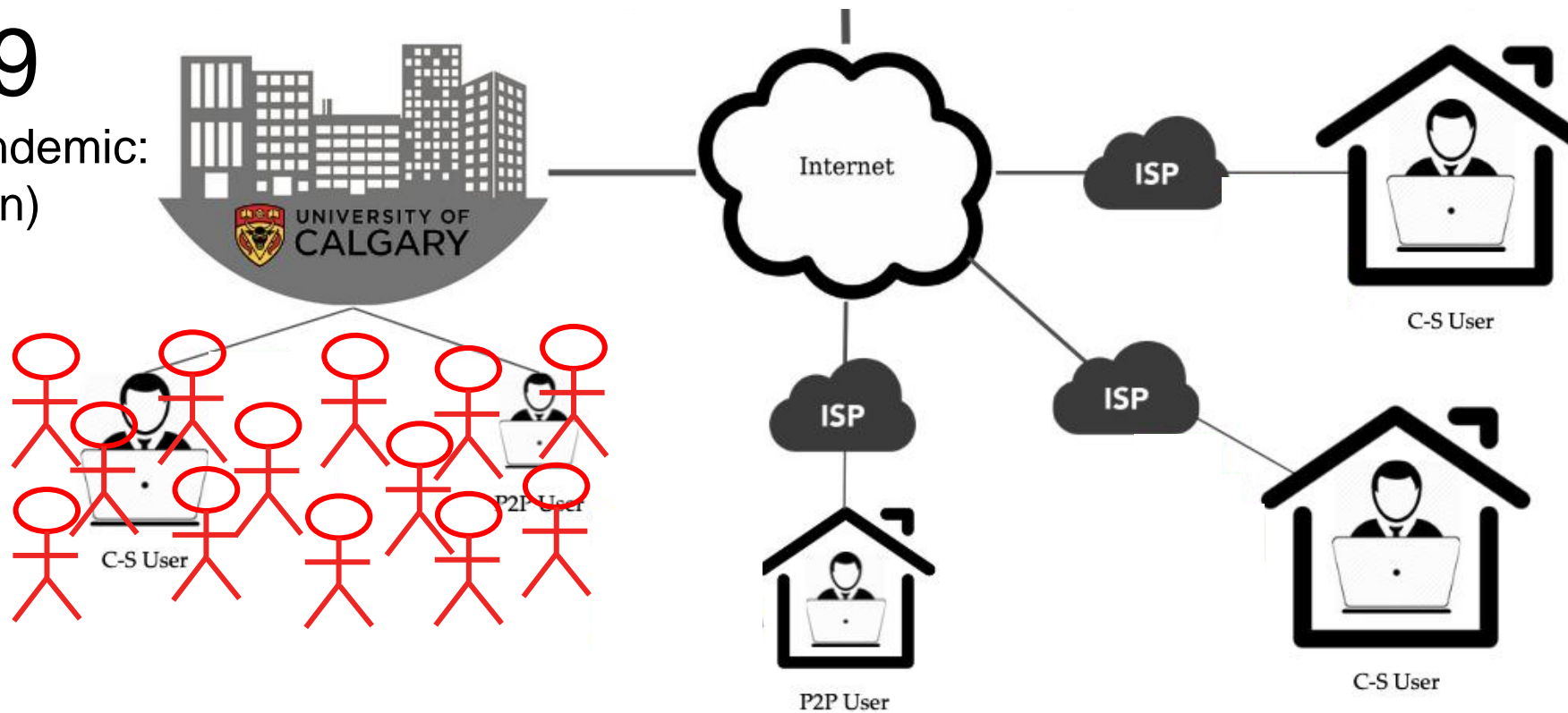
The Perfect Storm: People



UNIVERSITY OF
CALGARY

2019

(pre-pandemic:
in person)

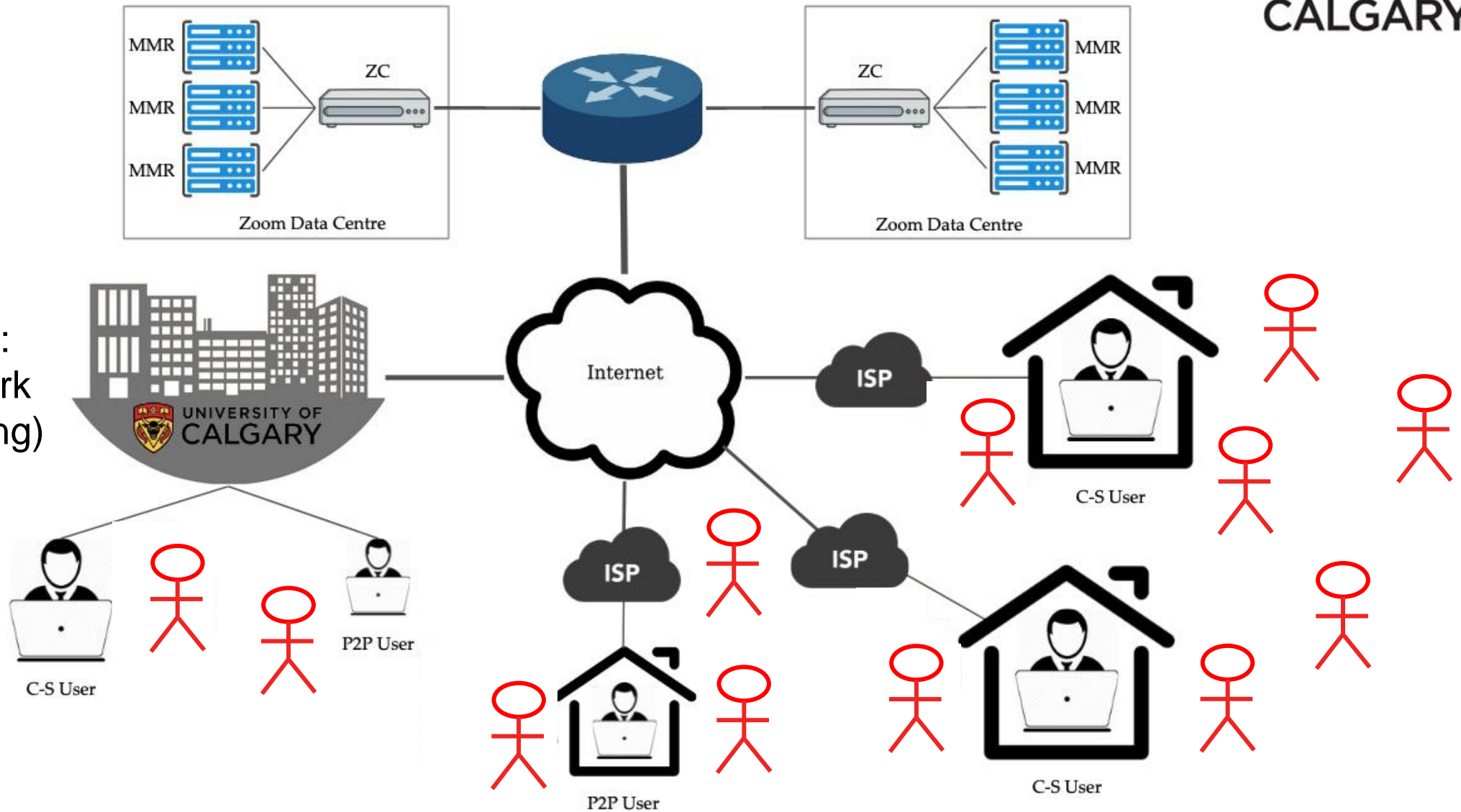


The Perfect Storm: People



UNIVERSITY OF CALGARY

2020
(pandemic:
remote work
and learning)

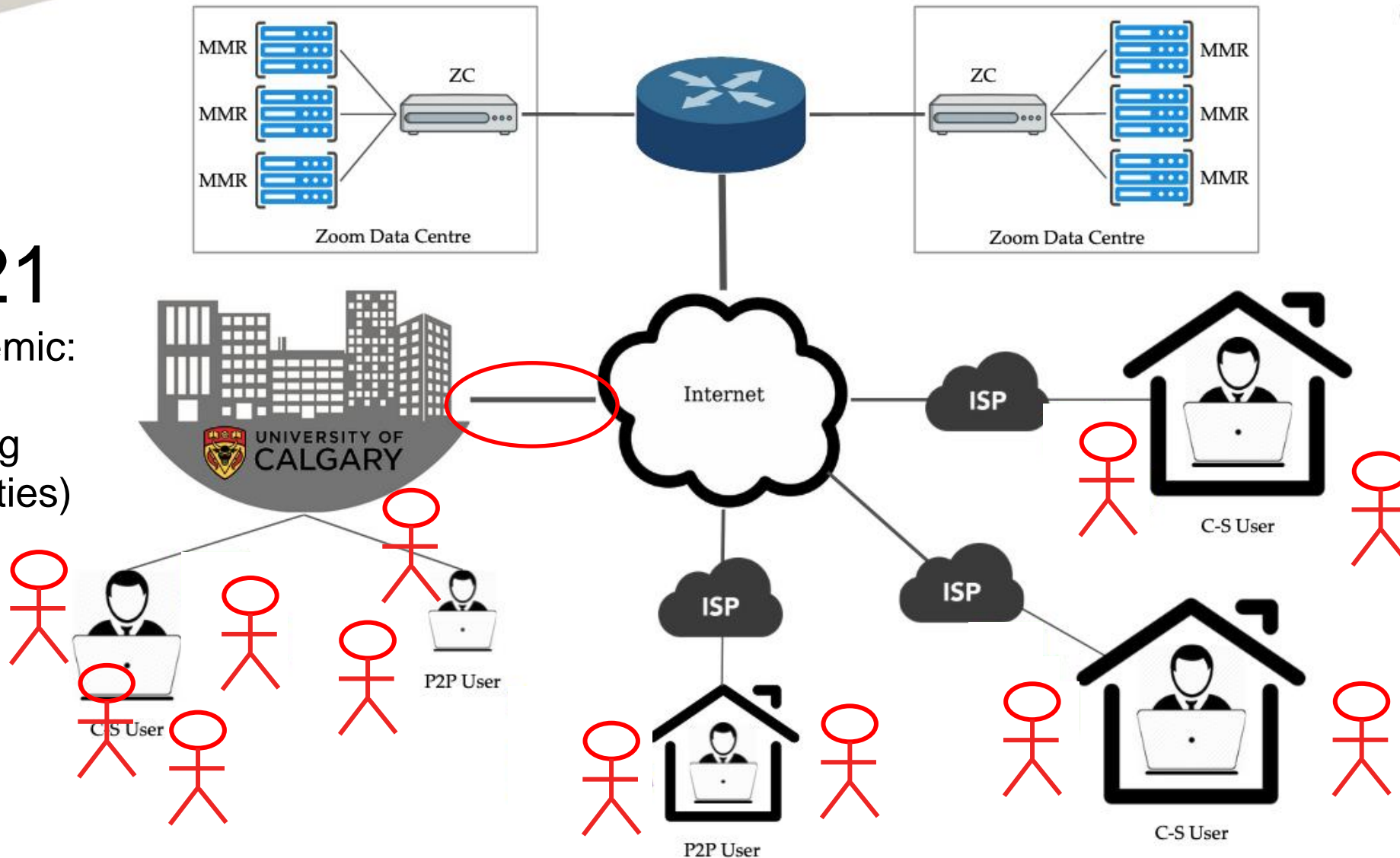


The Perfect Storm: People



UNIVERSITY OF CALGARY

2021
(pandemic:
hybrid
learning
modalities)



The Perfect Storm: Protocols

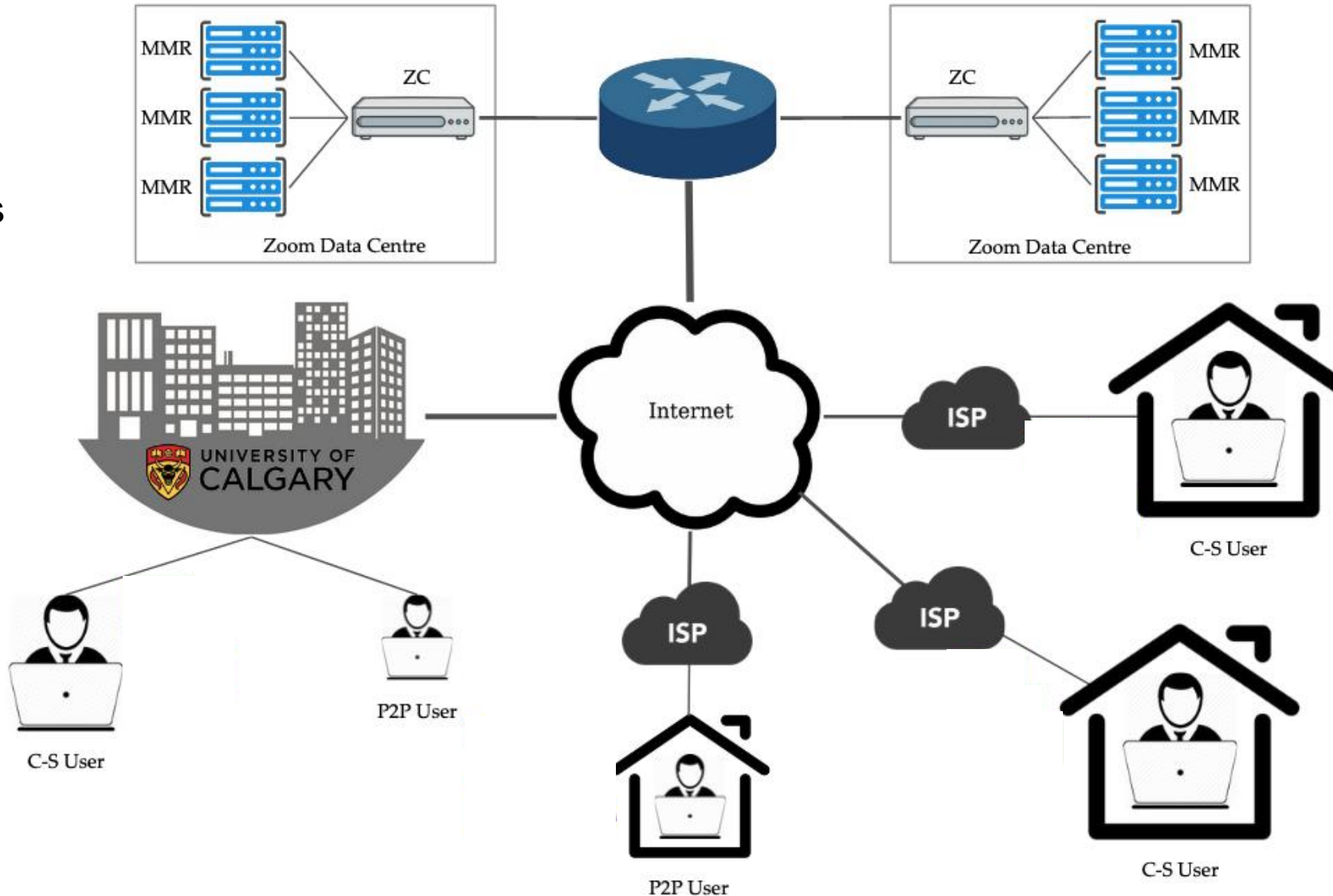


UNIVERSITY OF
CALGARY

Zoom uses
both TCP
and UDP

TCP uses
congestion
control

UDP
does not



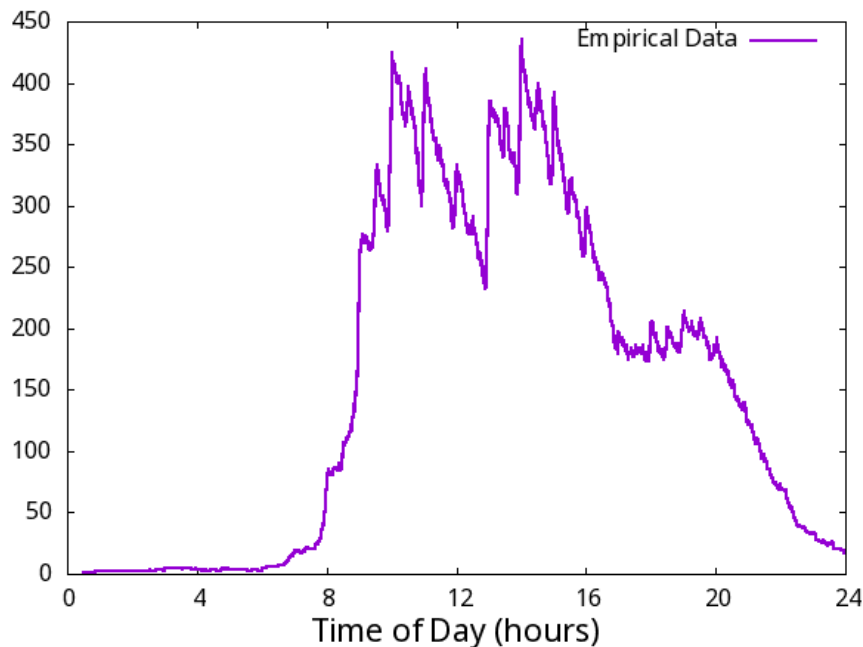


UNIVERSITY OF CALGARY

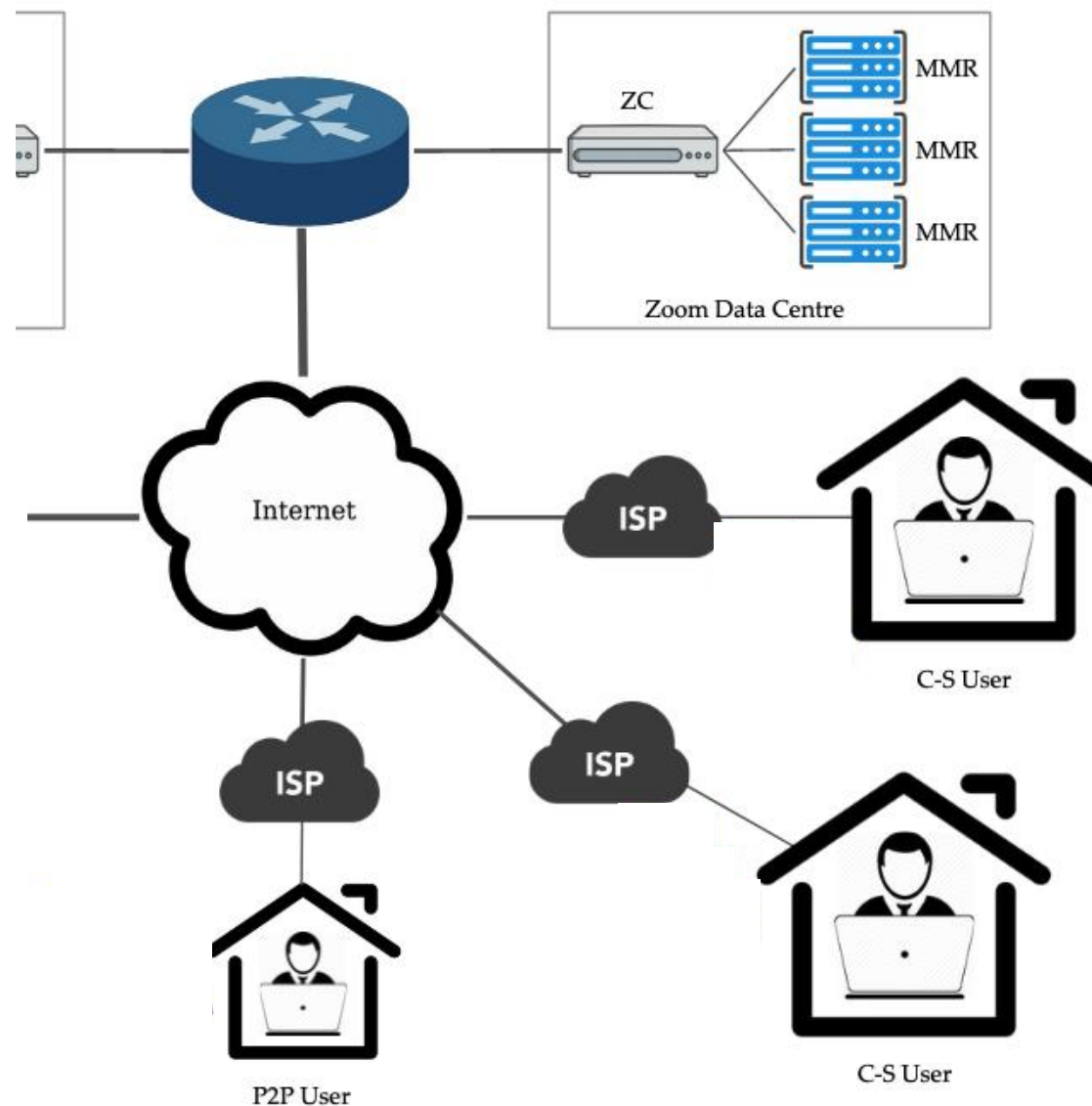
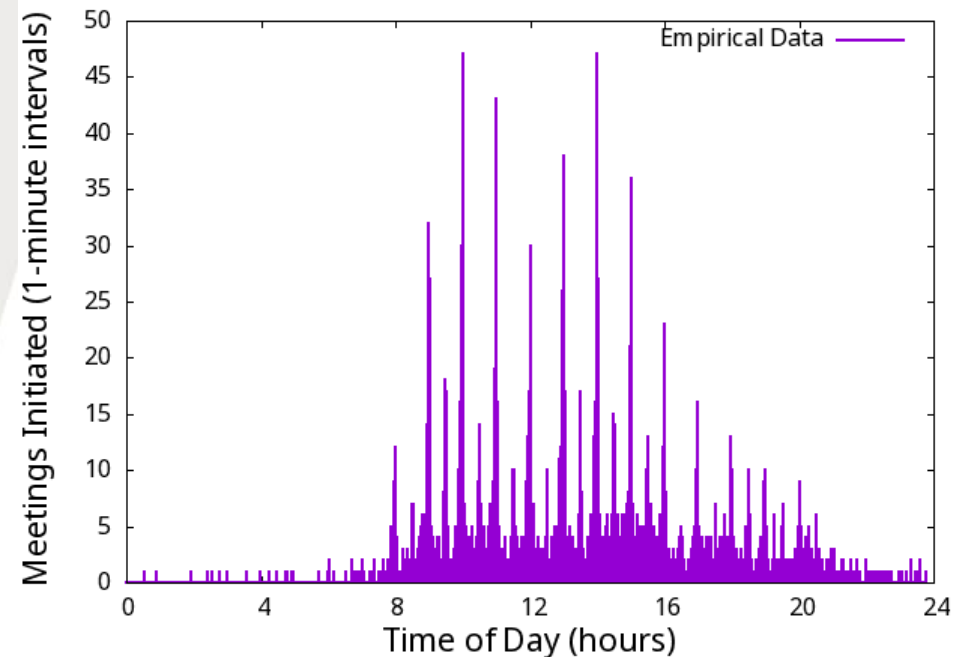
Perfect Storm: Patterns

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

Concurrently Active Zoom Meetings (Wed Sept 22, 2021)



Arrival Counts for Zoom Meetings (Wed Sept 22, 2021)

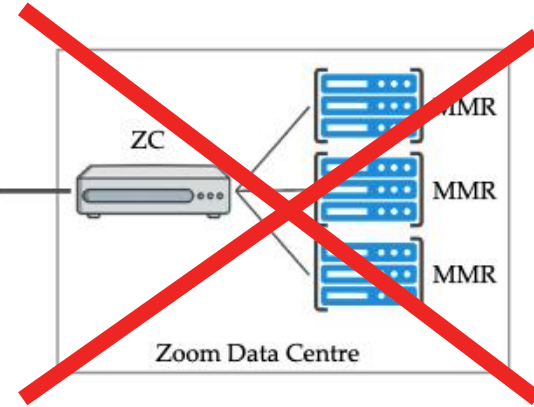
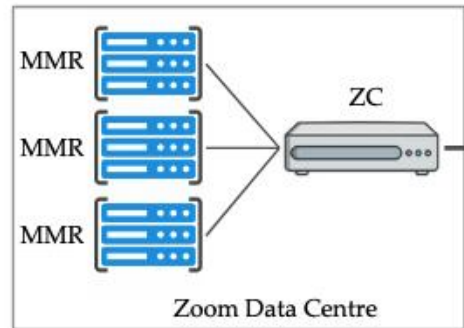


The Perfect Storm: Policies



UNIVERSITY OF
CALGARY

Licensed
version
of Zoom
(> 1Mbps)



Use Zoom
servers in
Canada
(limited
supply)



C-S User

Use the
commercial
Internet link
(6 Gbps)



C-S User



P2P User



P2P User



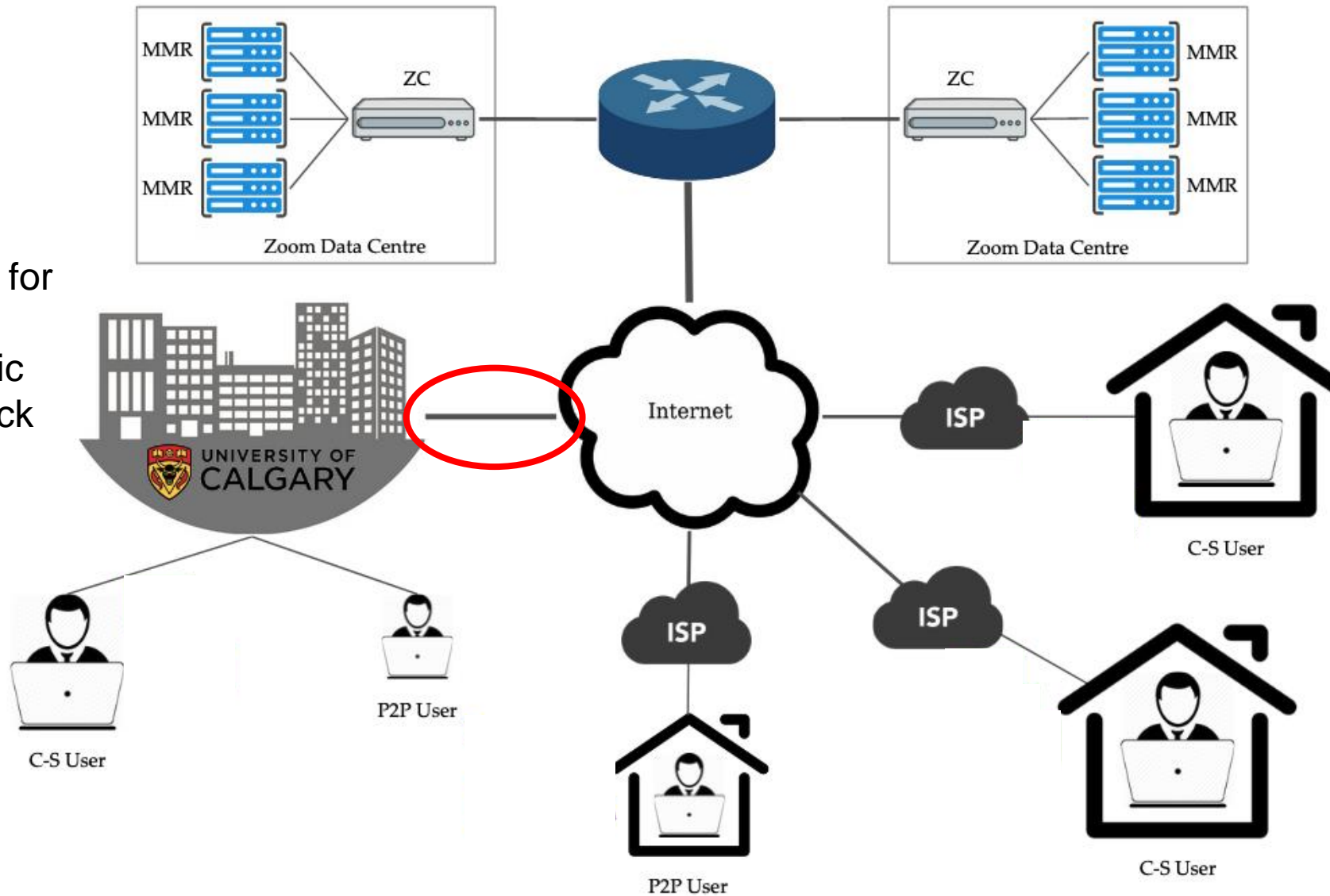
C-S User

The Perfect Storm: Performance



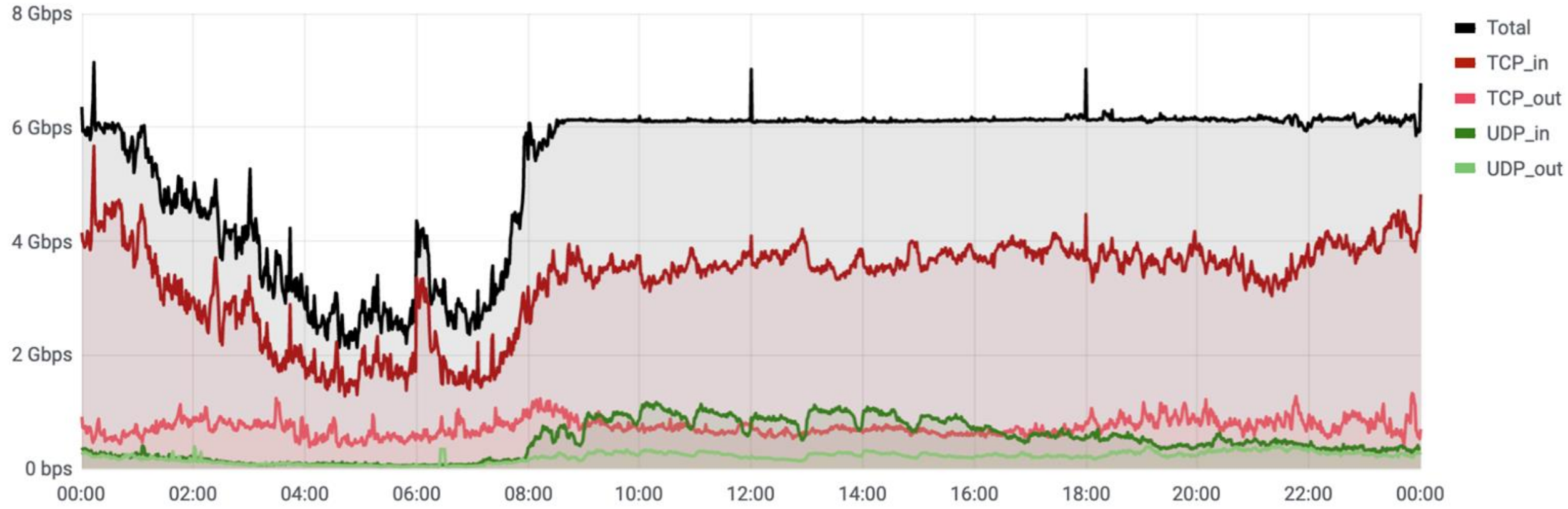
UNIVERSITY OF
CALGARY

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





Root Cause of Problems: Congested Bottleneck Link

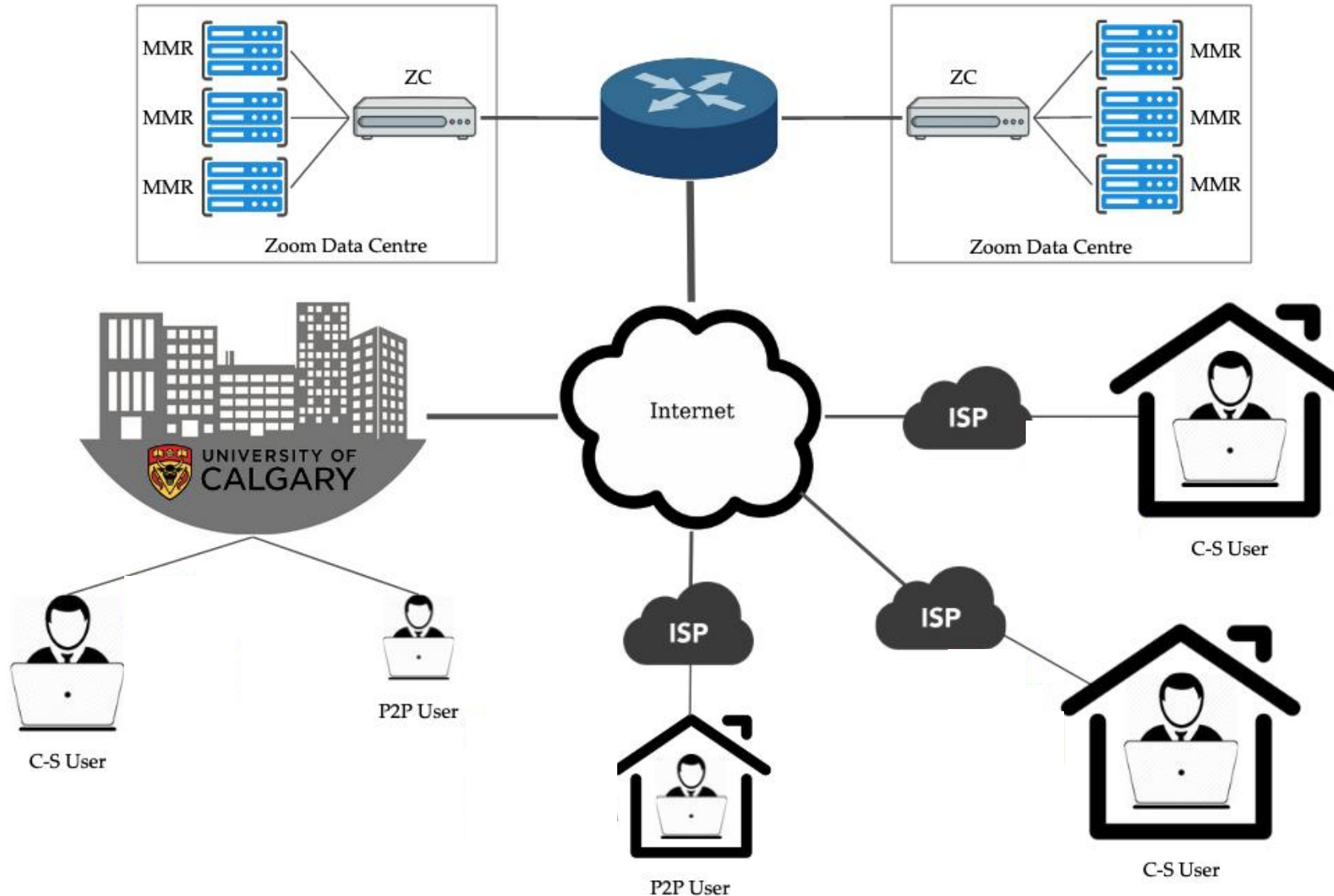


Usage of campus external link for commercial Internet traffic (October 6, 2021)

The Perfect Storm: Peculiarities



UNIVERSITY OF
CALGARY



Zoom does not share bandwidth fairly with other applications

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



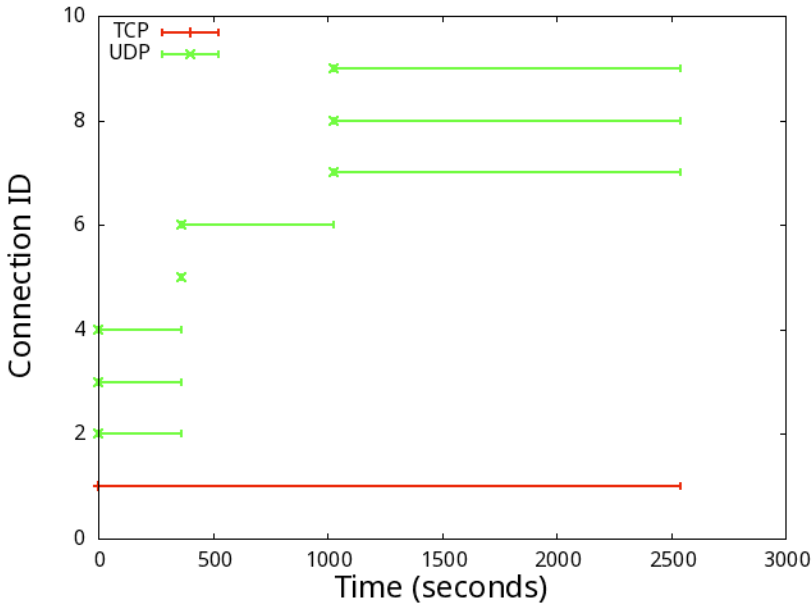
Zoom Wireshark Traces

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

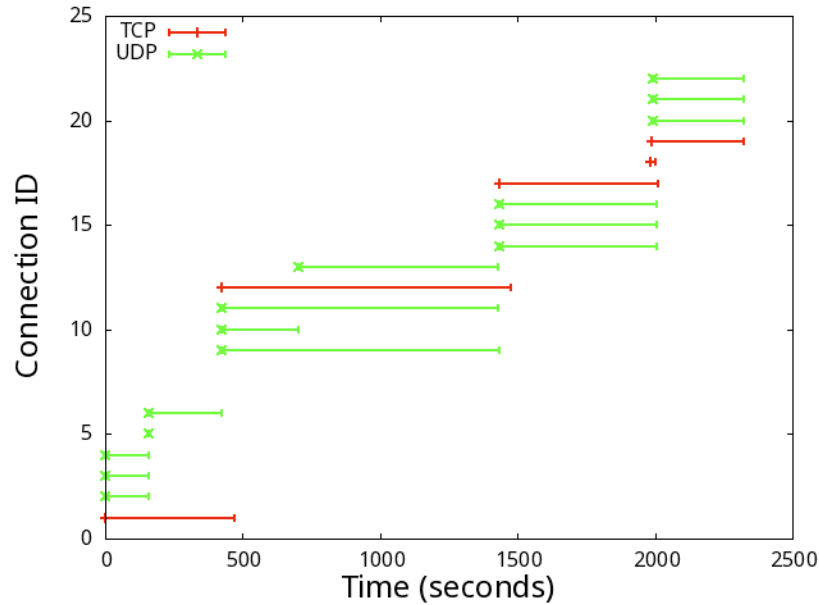


Connection-Level Analysis of Zoom Test Sessions

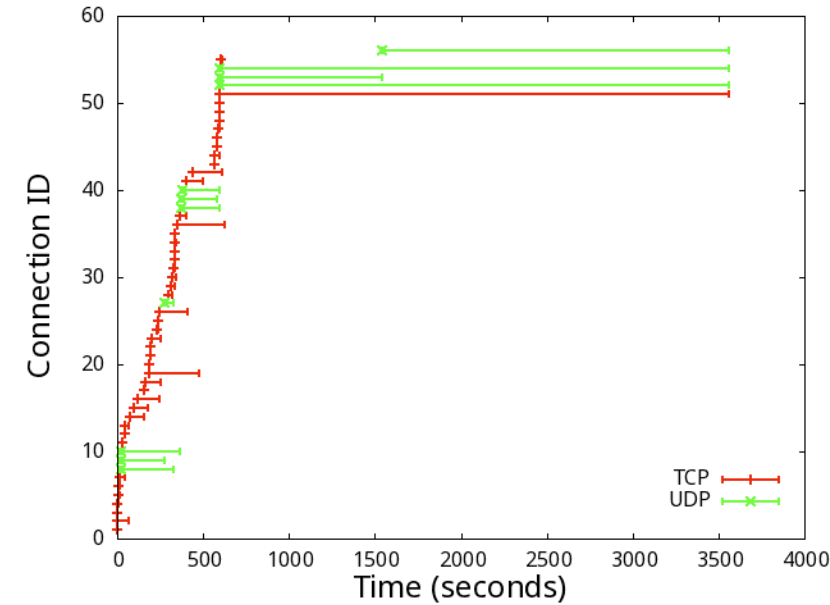
Trace A (on campus, Aug 31, 2021)



Trace D1 (on campus, Oct 27, 2021)



Trace B (on campus, Oct 6, 2021)



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

Packet-Level Analysis: Empirical Observations

- 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.

No.	Time	Source	Destination	SrcPort	DstPort	Protocol	Length	Info
608274	1822.568841	10.13.145.29	149.137.20.227	57194	8801	UDP	1239	57194 → 8801 Len=1197
608275	1822.578921	10.13.145.29	149.137.20.227	57192	8801	UDP	207	57192 → 8801 Len=165
608276	1822.578990	10.13.145.29	149.137.20.227	57194	8801	UDP	1271	57194 → 8801 Len=1229
608277	1822.579173	149.137.20.227	10.13.145.29	8801	57194	UDP	1239	8801 ← 57194 Len=1197
608278	1822.579562	149.137.20.227	10.13.145.29	8801	57192	UDP	207	8801 ← 57192 Len=165
608279	1822.579742	10.13.145.29	149.137.20.227	57194	8801	UDP	1271	57194 → 8801 Len=1229
608280	1822.599608	10.13.145.29	149.137.20.227	57194	8801	UDP	1271	57194 → 8801 Len=1229
608281	1822.620512	10.13.145.29	149.137.20.227	57194	8801	UDP	1271	57194 → 8801 Len=1229
608282	1822.620574	10.13.145.29	149.137.20.227	57194	8801	UDP	1260	57194 → 8801 Len=1260
608283	1822.620605	10.13.145.29	149.137.20.227	57194	8801	UDP	1260	57194 → 8801 Len=1260
608284	1822.620618	10.13.145.29	149.137.20.227	57194	8801	UDP	1260	57194 → 8801 Len=1260
608285	1822.620632	10.13.145.29	149.137.20.227	57194	8801	UDP	1260	57194 → 8801 Len=1260
608286	1822.629651	149.137.20.227	10.13.145.29	8801	57194	UDP	1260	8801 ← 57194 Len=1260
608287	1822.629851	149.137.20.227	10.13.145.29	8801	57194	UDP	1260	8801 ← 57194 Len=1260
608288	1822.629919	10.13.145.29	149.137.20.227	57194	8801	UDP	1260	57194 → 8801 Len=1260
608289	1822.630319	149.137.20.227	10.13.145.29	8801	57194	UDP	1260	8801 ← 57194 Len=1260
608290	1822.630319	149.137.20.227	10.13.145.29	8801	57194	UDP	1260	8801 ← 57194 Len=1260
608291	1822.639987	10.13.145.29	149.137.20.227	57194	8801	UDP	1260	57194 → 8801 Len=1260
608292	1822.640124	149.137.20.227	10.13.145.29	8801	57194	UDP	1260	8801 ← 57194 Len=1260
608293	1822.640547	149.137.20.227	10.13.145.29	8801	57194	UDP	1260	8801 ← 57194 Len=1260
608294	1822.640645	10.13.145.29	149.137.20.227	57194	8801	UDP	1260	57194 → 8801 Len=1260
608295	1822.640701	10.13.145.29	149.137.20.227	57194	8801	UDP	1260	57194 → 8801 Len=1260
608296	1822.640967	149.137.20.227	10.13.145.29	8801	57194	UDP	1260	8801 ← 57194 Len=1260
608297	1822.640967	149.137.20.227	10.13.145.29	8801	57194	UDP	1260	8801 ← 57194 Len=1260
608298	1822.651401	10.13.145.29	149.137.20.227	57194	8801	UDP	1260	57194 → 8801 Len=1260
608299	1822.651510	10.13.145.29	149.137.20.227	57194	8801	UDP	1260	57194 → 8801 Len=1260
608300	1822.661458	10.13.145.29	149.137.20.227	57194	8801	UDP	1260	57194 → 8801 Len=1260
608301	1822.661520	10.13.145.29	149.137.20.227	57194	8801	UDP	1260	57194 → 8801 Len=1260
608302	1822.661538	10.13.145.29	149.137.20.227	57194	8801	UDP	1260	57194 → 8801 Len=1260
608303	1822.682117	10.13.145.29	149.137.20.227	57194	8801	UDP	1260	57194 → 8801 Len=1260
608304	1822.682180	10.13.145.29	149.137.20.227	57194	8801	UDP	1260	57194 → 8801 Len=1260
608305	1822.682196	10.13.145.29	149.137.20.227	57194	8801	UDP	1260	57194 → 8801 Len=1260
608306	1822.682209	10.13.145.29	149.137.20.227	57194	8801	UDP	1260	57194 → 8801 Len=1260
608307	1822.682227	10.13.145.29	149.137.20.227	57194	8801	UDP	1260	57194 → 8801 Len=1260
608308	1822.692315	10.13.145.29	149.137.20.227	57194	8801	UDP	1260	57194 → 8801 Len=1260

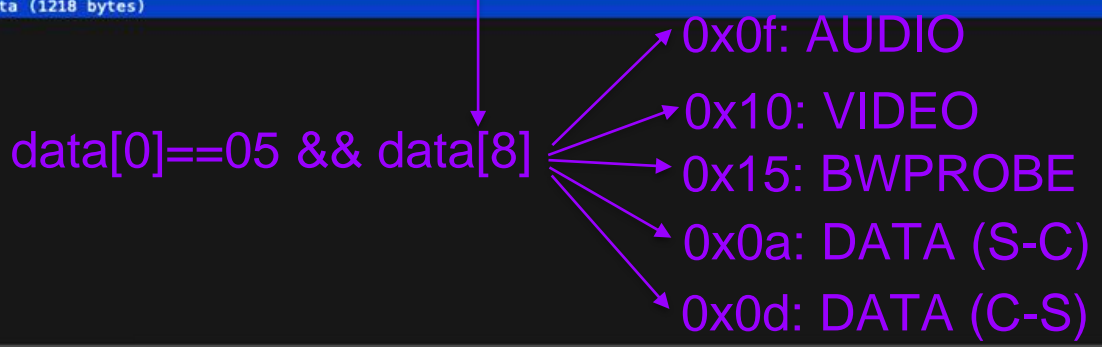
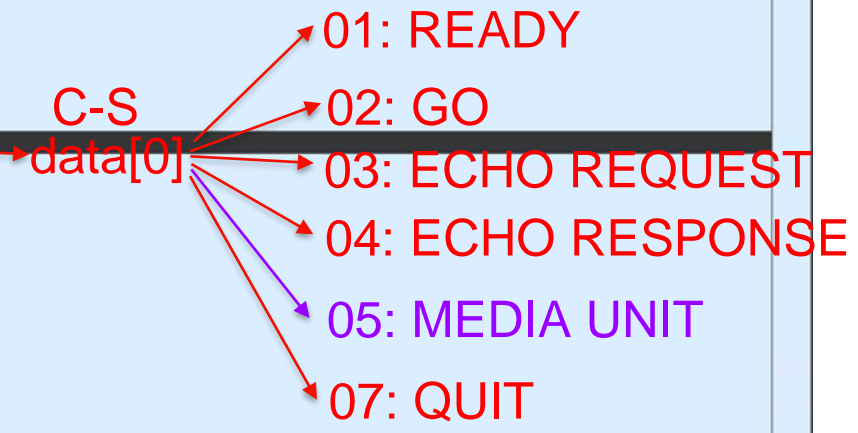

```

00 08 e3 ff fc 30 d4 1b 81 0e 5b e9 08 00 45 00 .....0...[...E...
04 de 80 ab 00 00 80 11 6f cd 0a 0d 91 1d 95 89 .....o.....
14 e3 df 6a 22 61 04 ca 59 2c 05 d0 28 00 3b a4 ...j"a...Y,.(;...
6c 00 10 01 00 fb 90 0c 18 0c 01 c0 7a 0b f9 a9 [...].....z...
55 02 00 00 00 00 02 9d ec 03 90 62 25 f1 4c 4b U.....b%LK
e4 f4 01 00 04 01 be de 00 04 12 5f f7 77 35 a2 ....._w5...
00 9d fc 9d fb 50 00 70 00 00 1c 00 8f 9a bc 47 .....P.p.....G
0f 2a 1d c6 f6 99 db 8a c2 a8 cb c7 bf 4b 89 f7 .....*.....K...
49 9b ac 59 9a 0a ef 3f d0 67 48 36 1f 37 b8 22 I..Y...? .gH6.7."
82 96 1e ab a3 e8 67 8e cf 75 5b f9 8e ed 7b 3e .....g. u[...{>
38 a1 95 35 72 55 c6 23 81 65 86 8e 6f 1f b4 ef 8..5rU.# .e.o...
1f 36 92 a2 74 94 82 bc 5f 1f ab 3a f0 98 19 5d .6..t..._:...]
51 ce a0 f3 8d 0a 50 7e 0b 76 a0 a8 16 76 af 00 Q.....P~.v...v..
cc ad 50 69 0a 2c b2 a6 c3 67 1b d2 92 e9 54 00 ..Pi,..g...T.
eb bd f3 5a a3 3e 99 b6 4a 8c 1f 84 ef c3 77 cf ...Z>..J...w.
ba e0 a5 c3 1e 9a f2 1f 9e 75 d3 bb 82 3f d5 42 .....u...?B
77 f6 9f b6 42 8b 37 03 55 a8 00 e1 7e 21 12 16 w...B.7. U...~!..
ed d3 3d df 98 6a ee cc a2 87 8c 34 d3 e1 b1 f7 ..=..j...4...
c2 8c 46 3a 1a d0 3c 93 15 36 ab 87 66 1c 02 1a ..F:..<.6..f...
8c b8 7b 59 7d a3 9b 1f b6 5b 6a bf ec 42 4a f9 ..{Y}...[j..BJ.
20 a3 18 3b f2 b9 d3 df b9 78 f7 cc 30 ea b2 07 ..;....x..0...
22 47 8d 7e 20 4e d7 63 eb 9b 35 dd dd 9e b5 aa "G~N.c..5....
c3 6a fd b4 1c 8b 1a 89 ab 6f 6e 80 8c a7 4d 15 .j.....on...M.
  
```



```

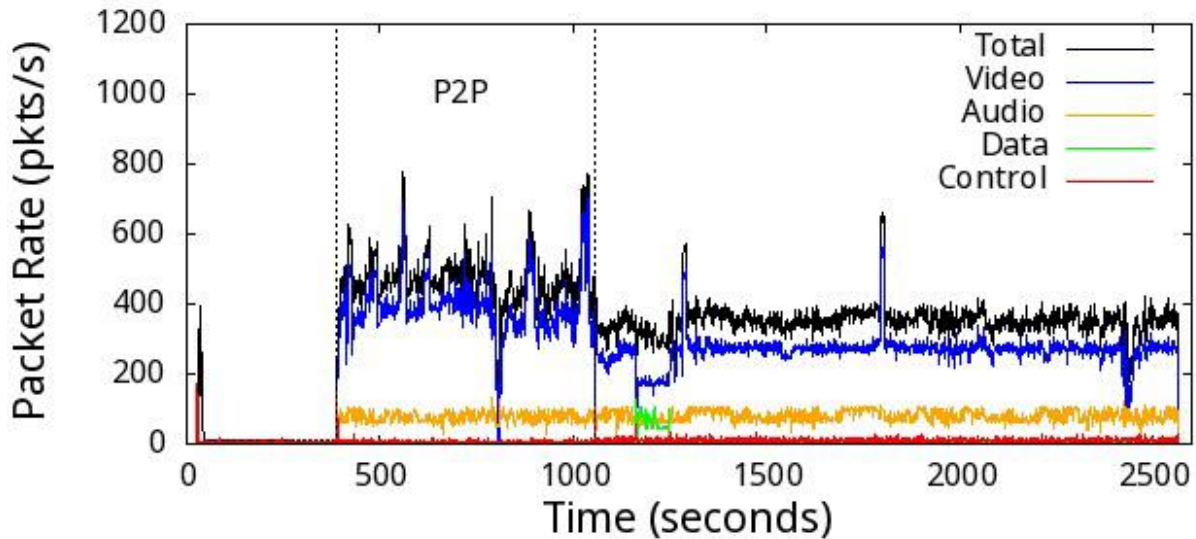
> Frame 608282: 1260 bytes on wire (10080 bits) captured on interface eth0 (08:00:0c:00:00:00)
> Ethernet II, Src: Chongqin_0e:5b:e9 (08:00:0c:00:00:00), Dst: Cisco_Ethernet_00:00:0c:00:00:00
> Internet Protocol Version 4, Src: 10.13.145.29, Dst: 149.137.20.227
> User Datagram Protocol, Src Port: 57194, Dst Port: 8801
> Data (1218 bytes)
  
```



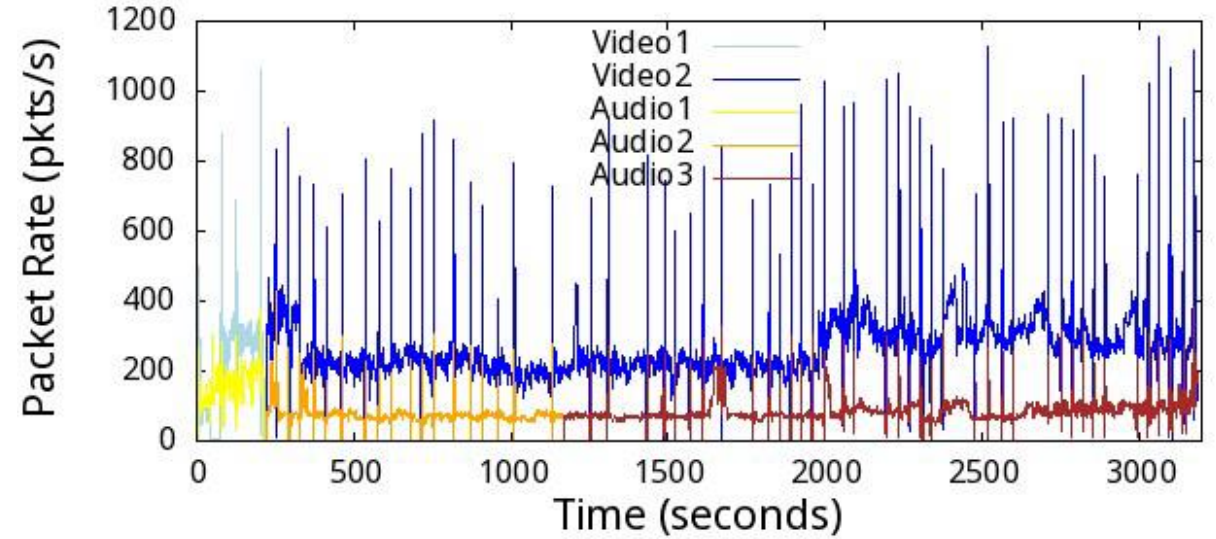


Media Stream Analysis

Trace A (August 31, 2021)



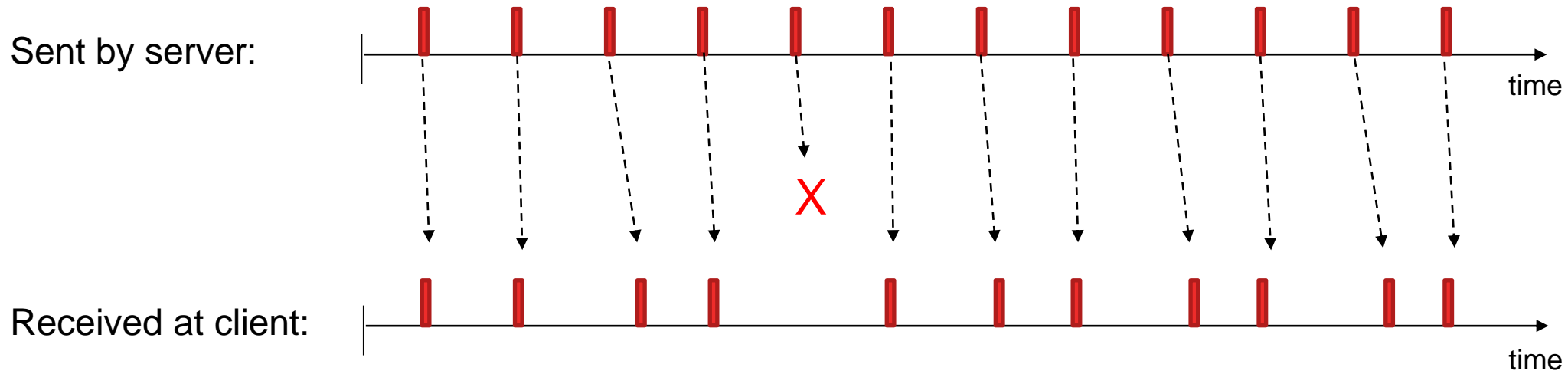
Trace B (October 6, 2021)



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



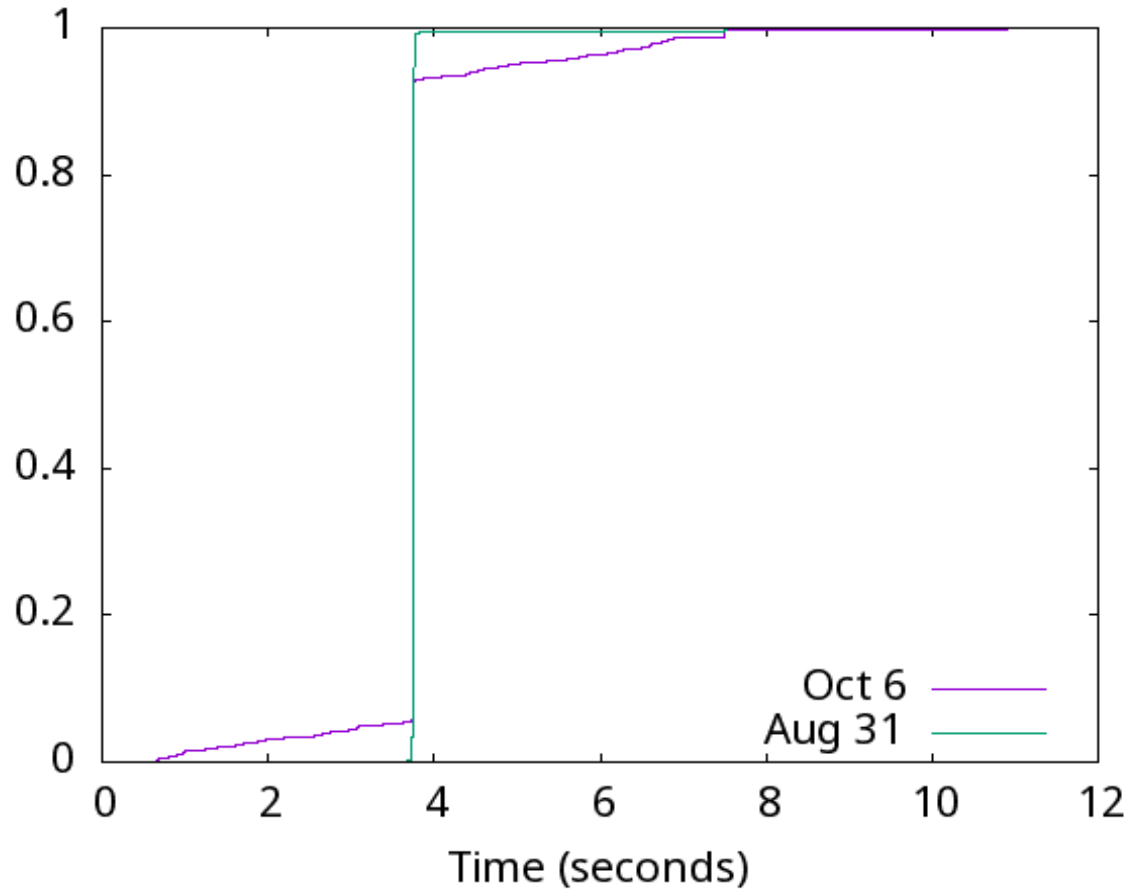
Delay and Jitter Analysis from Timing Probes (3.75 sec)



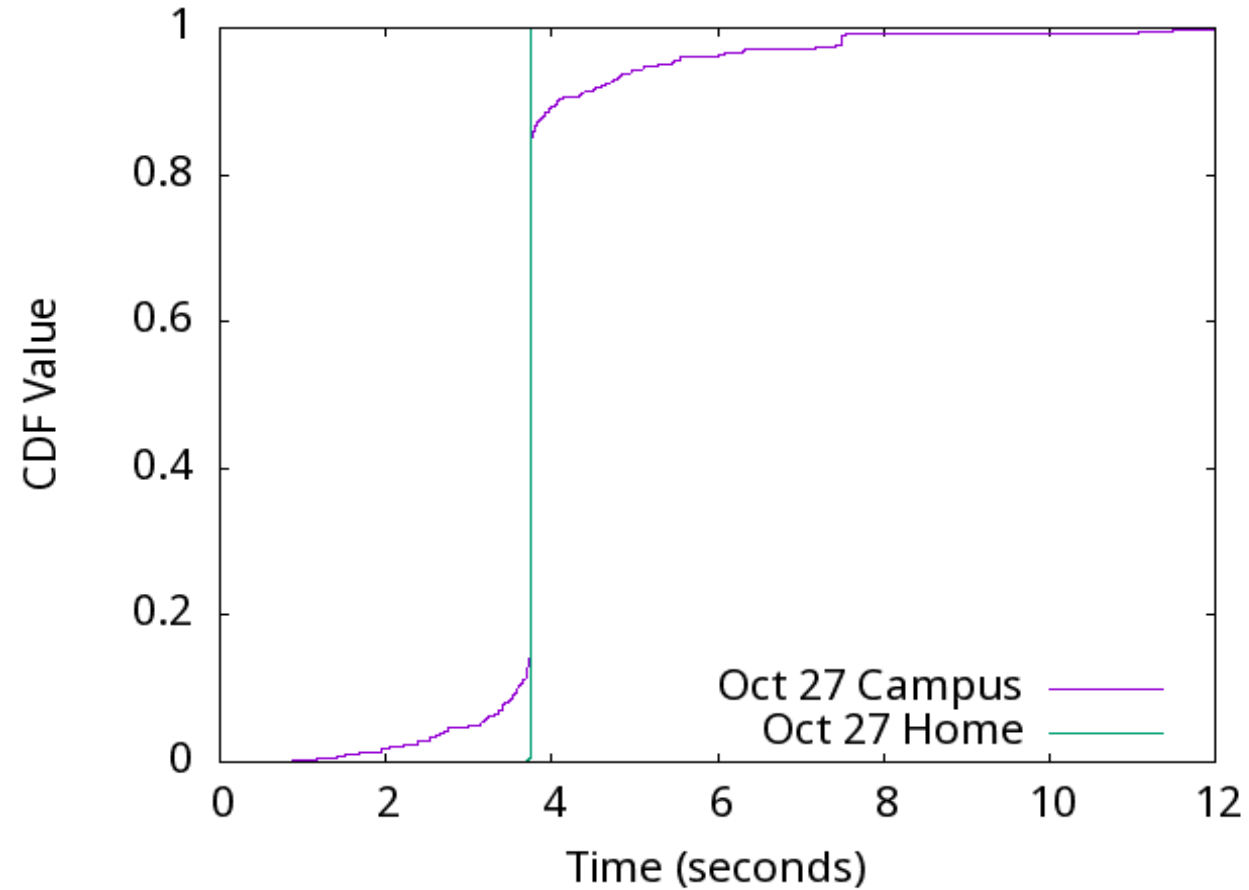


Delay and Jitter Analysis from Timing Probes (3.75 sec)

Traces A and B



Traces D1 and D2

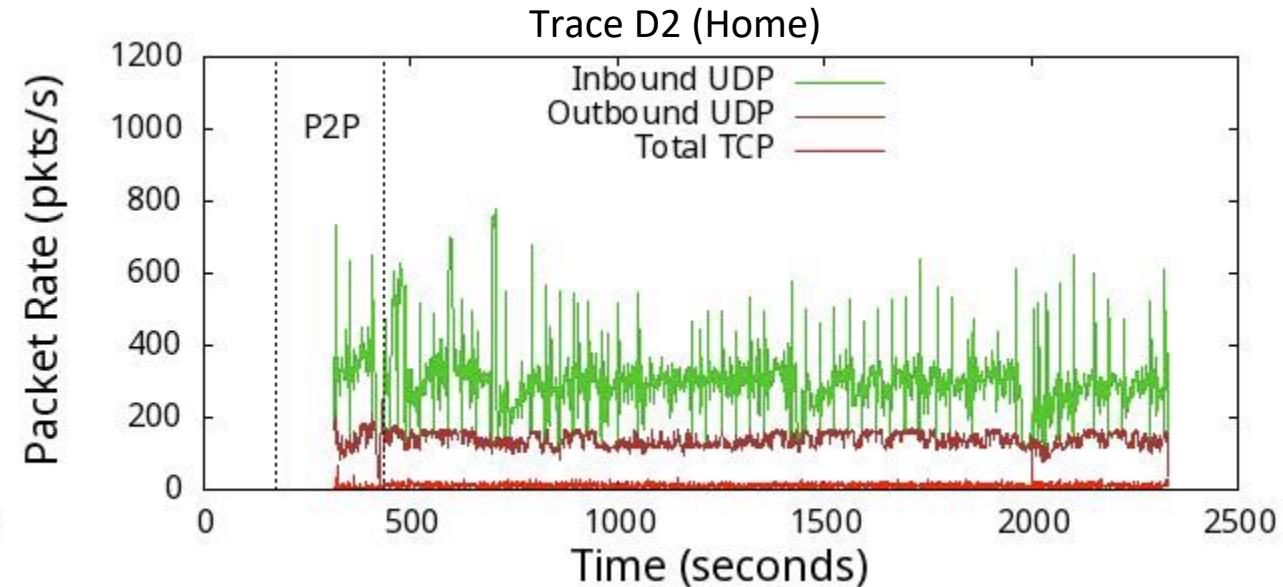
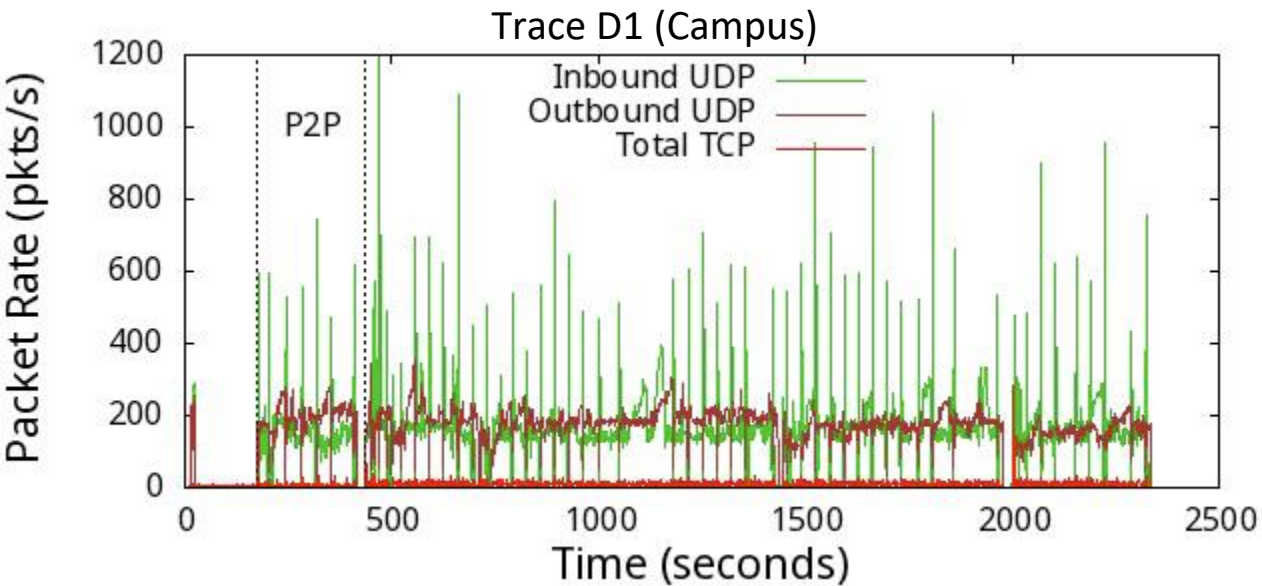


Key Insight: The bottleneck is located on the campus network.



Directionality Effects

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



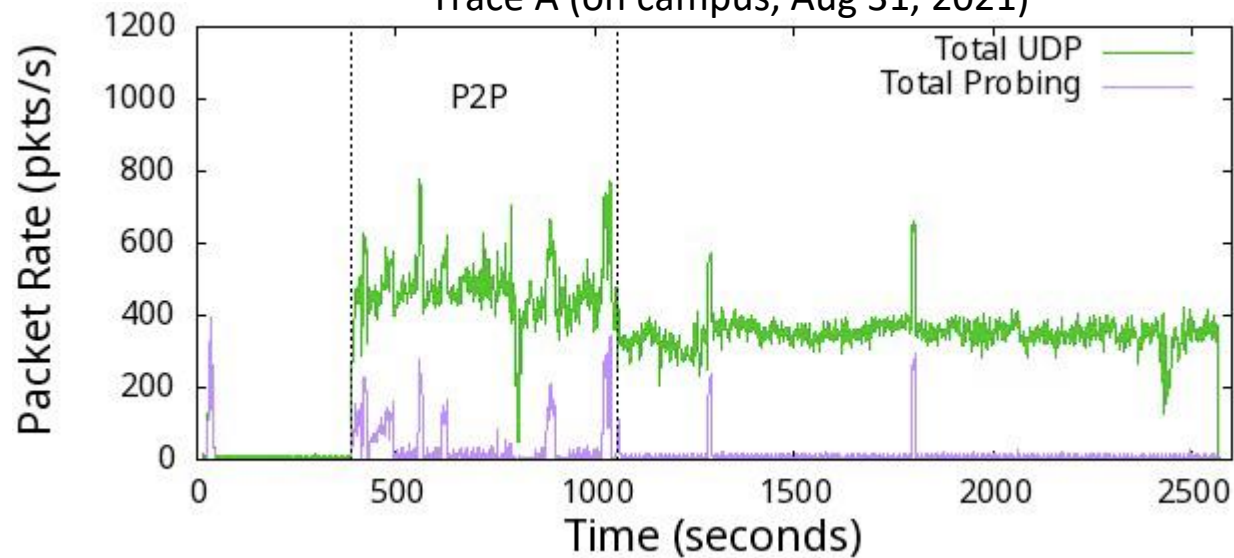
Key Insight: The bottleneck affects both inbound and outbound traffic.



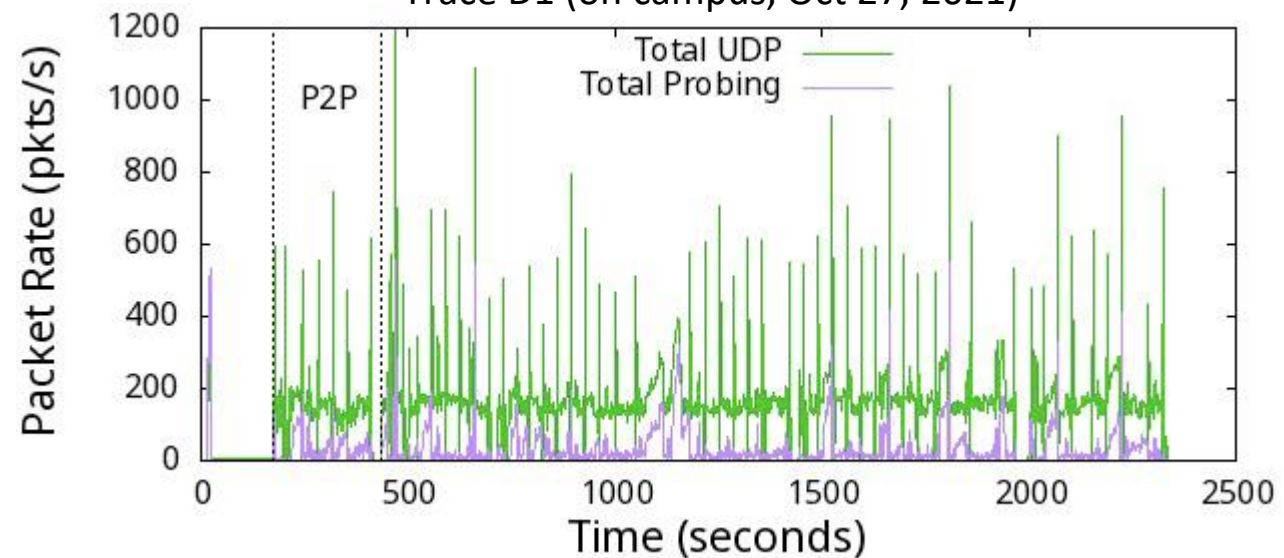
Bandwidth Probing (1 of 2)

Analysis of video bandwidth probing traffic in Zoom test sessions:

Trace A (on campus, Aug 31, 2021)



Trace D1 (on campus, Oct 27, 2021)



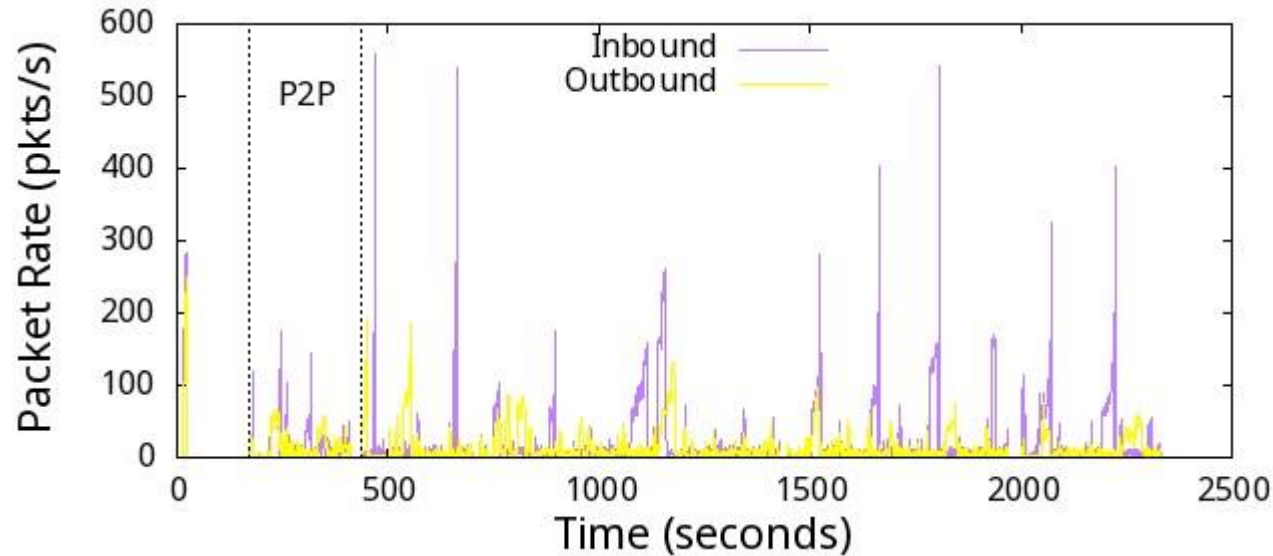
Key Insight: Bandwidth probing happens more often on a congested network.



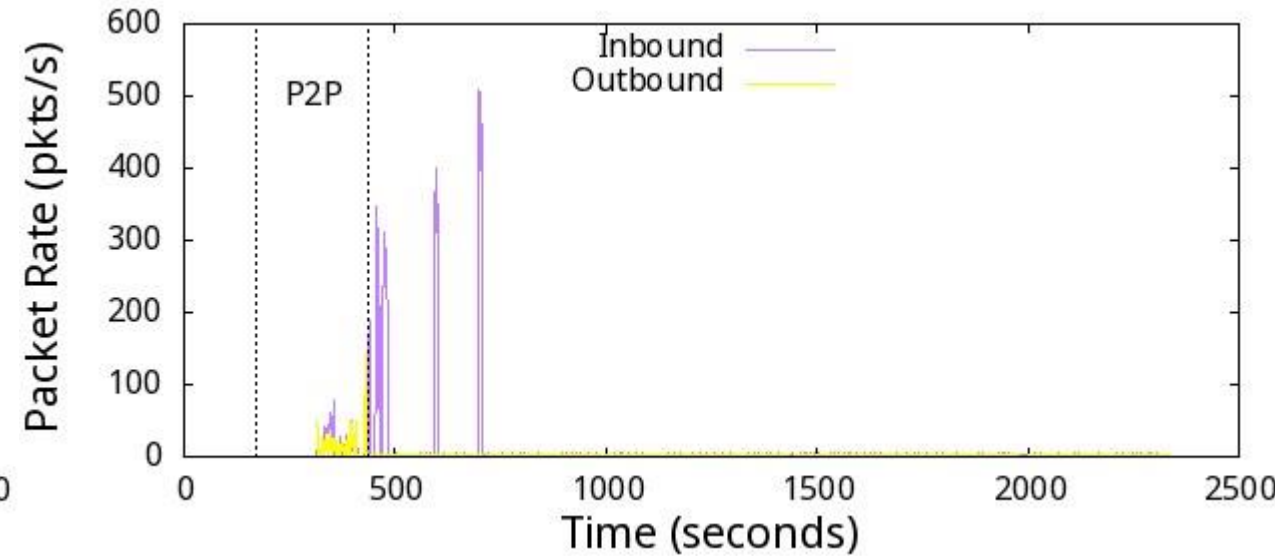
Bandwidth Probing (2 of 2)

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

Trace D1 (on campus, Oct 27, 2021)



Trace D2 (at home, Oct 27, 2021)



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

Recommendations

- 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

- 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).



UNIVERSITY OF
CALGARY

Thank you for listening!

Questions?

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