Impact of Provider Failures on the Traffic at a University Campus

Rodrigo Duarte Alex B. Vieira
Universidade Federal de Juiz de Fora
Email: {rodrigo.duarte,alex.borges}@ufjf.edu.br

Ítalo Cunha Jussara M. Almeida
Universidade Federal de Minas Gerais
Email: {cunha,jussara}@dcc.ufmg.br

***Abstract*—In this paper we characterize the impact of failures in Brazil's national research network (RNP) on traffic at a large client university. We analyze *reachability disruptions*, caused by failures of RNP's interdomain links, that block all international traffic. We also analyze *performance disruptions*, caused by simultaneous failure of multiple RNP intradomain links, which result in congestion and performance degradation. We study the impact of disruptions on traffic, application mix, and user behavior. Our results show that users adapt their behavior when some applications become unavailable and when network performance degrades. For example, users tend to migrate to Youtube when Facebook becomes unavailable during reachability disruptions; similarly, users migrate to Facebook when congestion during performance disruptions severely degrade Youtube experience. We also correlate the impact of disruptions to network topology and show that performance during a performance disruption depends on the location and importance of failed links.**

***Keywords*—Network failures, performance degradation, passive measurements, user behavior**

I. Introduction

Interactive networked applications like social networks, collaborative authoring, and online banking reach an increasing fraction of users. Services that used to run locally, like media consumption, or asynchronously, like e-mail, now often require continuous low-latency high-bandwidth connectivity to the Internet. Such greater dependence on network connectivity increases the impact of Internet failures on users.

Most network failures in the Internet go unnoticed due to automatic traffic rerouting [1], [2]. Some failures, however, require human intervention and may take hours to resolve [2]–[4]. Although there is a significant body of work on characterizing anomalies and failures in the Internet (e.g., [1], [2], [5]–[9]), our understanding of the impact of these failures on traffic and user behavior remains limited.

We investigate the impact of seven failures in Brazil's national research network (*Rede Nacional de Ensino e Pesquisa*, RNP) on the traffic and user behavior at a client university. We analyze *reachability disruptions* caused by failures of RNP's interdomain links, which blocked all international traffic (§III). We also analyze *performance disruptions* caused by failures of multiple RNP intradomain links, which resulted in congestion at low-capacity links but no reachability problems (§IV). Our analyses use packet traces collected throughout 2013 at the border router in Universidade Federal de Juiz de Fora, Brazil. This is a large university, with over 19,000 students, 2,900 thousand faculty and staff, around 6,000 end-hosts, and average external bandwidth utilization of 46 Mbps (§II).

ISBN 978-3-901882-68-5 © 2015 IFIP

Our results show that reachability disruptions have no significant impact on the performance of domestic traffic due to overall reduction of intradomain link utilization. However, traffic volume decreases during reachability disruptions, even for destinations that remain reachable, suggesting that users give up on network applications due to the limited connectivity. Another observed pattern is that users tend to migrate from unreachable sites hosted abroad to reachable domestic sites. This is particularly true for entertainment and social networking websites. We also show that asynchronous background applications, e.g., Dropbox and SMTP, accumulate tasks during failures and cause traffic bursts after failure restoration.

We find that performance disruptions may have low or high impact on traffic and user behavior, depending on where the failed links are located and on the routes chosen after failure onset. Only intradomain failures that break both default and backup routes to RNP's main traffic exchange point cause serious performance disruptions, resulting in congestion, packet losses, and increased round-trip times. Under serious performance disruptions, users tend to give up on using high-bandwidth services such as media streaming (e.g., Youtube) but continue using lower-bandwidth services like Facebook. Finally, we show that alternate routes used during performance disruptions may improve performance to destinations reachable before traversing congested links.

As far as we know, no previous study investigated how partial failures impact user behavior and traffic patterns on a local network. Thus, though limited to a single university network, our work contributes to provide better understanding of the impact of network failures on user behavior, offering valuable insights to network operators and system developers.

II. Traffic Dataset and Failure Description

We analyze the impact of failures in Brazil's national research network (RNP) on traffic at Universidade Federal de Juiz de Fora (UFJF). UFJF is a large university with approximately 19,000 students, 1,500 staff, and 1,400 professors. UFJF's network interconnects 22 institutes with approximately 6,000 computers interconnected by wired networks on research laboratories, administration offices, and classrooms; plus personal devices connected to campus-wide WiFi networks.

Fig. 1 shows an overview of the data collection infrastructure. We installed a switch between the university's border router and the university's firewall to mirror all traffic to a data collector. The border router and the firewall are responsible for routing and filtering, respectively, all ingress and egress traffic. The firewall also performs NAT for about 86% of

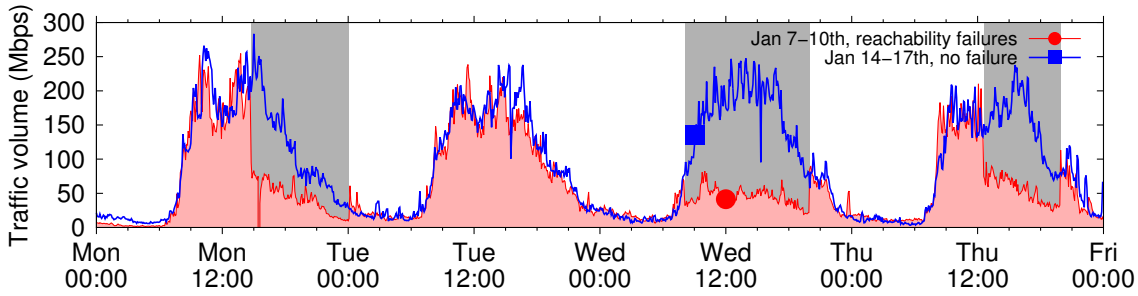


Figure 2: Overview of traffic at UFJF during normal network operation (blue line with the square) and during reachability disruptions (red line with the circle, shaded areas).

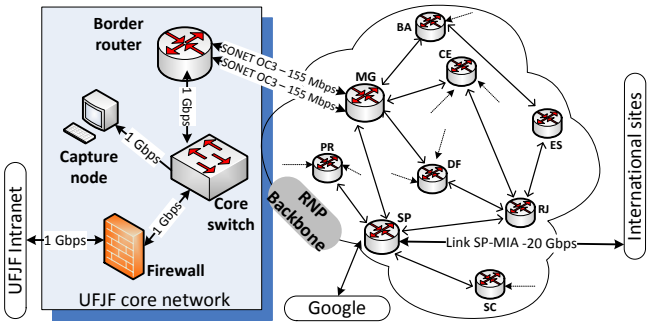


Figure 1: Overview of the Data Collection Deployment.

institutional computers and all personal devices in the network. As total traffic amounts to approximately 15 TB per month (46 Mbps on average), the collector summarizes traffic using TSTAT [10]. TSTAT is a free software tool that collects more than 110 flow metrics, including source and destination, start and end times, number of packets, transmitted bytes, and average latency. TSTAT also identifies flows belonging to some select applications. The mirrored packets are discarded after summarization to reduce storage requirements and safeguard user privacy. Our data does not include UFJF's internal traffic; although the analysis of intradomain traffic would be interesting, collecting it would require a significantly larger data collection infrastructure.

RNP's infrastructure is managed in cooperation with various regional Internet exchange points operated by universities. Enterprise and commercial networks can peer with RNP, settlement-free, at any regional exchange point. All traffic from UFJF is sent to RNP's exchange point at Minas Gerais (shown as 'MG' in Fig. 1) by two point-to-point OC-3 links. At the Minas Gerais exchange point the traffic gets into RNP, which forwards the traffic to its destination. RNP interconnects most public universities in Brazil, as well as some governmental institutions like research institutes and regulatory agencies. At the time when the failures we analyze happened, RNP had only one 20 Gbps international link between São Paulo (shown as 'SP') and Miami (US).

We here analyze failures confirmed by RNP operators [11]. Although the results reported in the next sections are computed for the particular failures analyzed, the observed patterns may generalize to other networks, in particular university networks.

Table I: Reachability disruptions reported by RNP in 2013.

Start time	End time	Duration
Jan. 7, 2:45PM	Jan. 8, 0:05AM	11h20
Jan. 9, 8:05AM	Jan. 9, 8:00PM	11h55
Jan. 10, 12:35PM	Jan. 10, 7:55PM	7h20

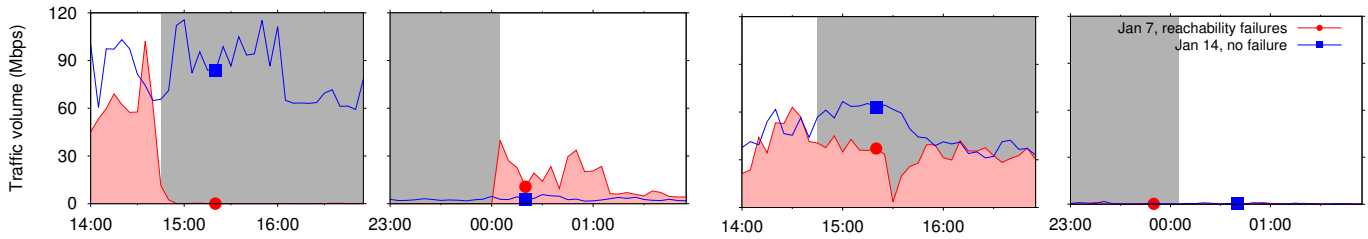
In this paper we analyze failures that happened between January 2013 and December 2013. During this period, our traffic monitor has summarized more than 252 TB of traffic into 453 GB of compressed TSTAT logs. We make our dataset publicly available [11].

III. Impact of Reachability Disruptions

According to RNP reports, there were failures at the fiber optics infrastructure of RNP's international link between São Paulo and Miami on January 7th, 9th, and 10th, 2013. These failures rendered destinations abroad unreachable. Only networks connected to one of RNP's exchange points, and their clients, continued reachable (e.g., sites hosted within the country). We refer to these failures as *reachability disruptions* in the next sections. Sec. III-A analyzes the impact of reachability disruptions on UFJF's traffic. These results will serve as basis for understanding more detailed results on user and application behavior in Secs. III-B and III-C, respectively.

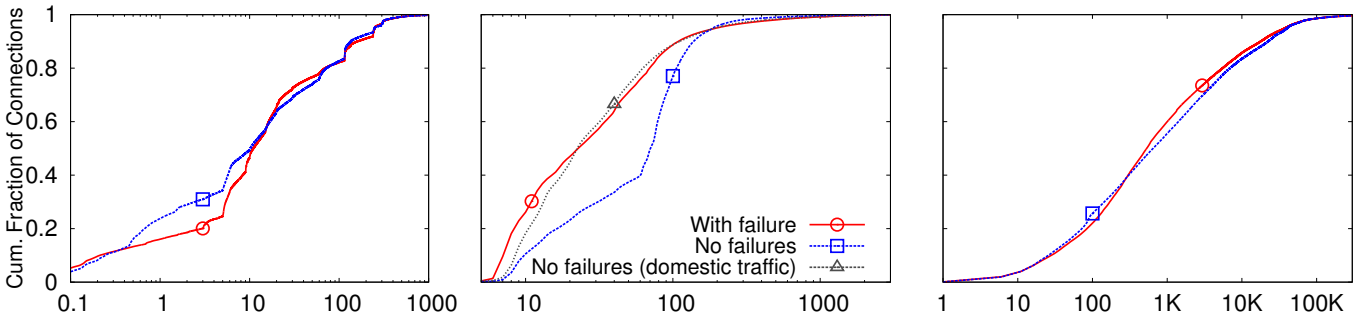
A. Impact on Traffic

Fig. 2 shows an overview of UFJF's traffic volume computed over 5-minute intervals during two distinct 4-day time periods. We distribute the bytes in each flow uniformly over its duration. The blue line with a square show total traffic between January 14th and 17th, 2013, when no failures were reported. The red lines with a circle show total traffic between January 7th and 10th, 2013, when RNP reported three reachability disruptions. Both periods cover week days from Monday to Thursday. Reachability disruptions occurred on time periods shown in Tab. I (all times BRST). Periods with reachability disruptions are shaded gray in Fig. 2. Note that, when computing the traffic, we do not include connections that do not complete the TCP three-way handshake (labeled 'incomplete' by TSTAT). The increase in traffic after 7AM is steeper than the decrease after 6PM due to night courses having fewer students than diurnal courses. The number of stablished TCP connections (not shown) is qualitatively similar. We also note that the week starting on January 7th was a mid-term week as



(a) International, onset (b) restoration (c) Google, onset (d) restoration

Figure 3: Close up of Fig. 2 showing traffic around onset and restoration of the reachability disruption of January 7th. We show traffic to international destinations (a, b) and to Google services (c, d).



(a) Duration (s) (b) End-to-end latency (ms) (c) Throughput (Kbps)

Figure 4: Performance comparison of TCP connections during the reachability disruption on January 7th and during the same period in the following week.

a result of a nationwide professor strike in 2012 shifting the university's calendar.

We split traffic into three sets: domestic traffic, with destination in Brazil; international traffic, with destination out of Brazil; and traffic to Google services. We separate traffic toward Google services because they continue reachable during reachability disruptions through RNP's São Paulo exchange point. Moreover, a significant fraction of the university's traffic is directed to Youtube, provided by Google (Sec. III-B). We split traffic into domestic and international using MaxMind's free IP geolocation database. Even though inaccuracies of IP geolocation databases are well known, MaxMind's database's accuracy is enough for our coarse-grained localization [12]. To identify traffic towards Google, we resolve IP addresses of Google services (e.g., youtube.com, gmail.com, google.com) at UFJF. We then obtain the set of BGP prefixes containing Google IP addresses from São Paulo exchange point's route server. We label traffic to destinations in these prefixes as toward Google.

Fig. 3 shows a close up of Fig. 2 for international and Google traffic during three-hour periods that cover the onset and restoration of the reachability disruption on January 7th. For comparison purposes, the figure also shows similar measurements for January 14th, which is the same day of the following week but with no reported failure. Traffic to domestic destinations (not shown) behaves similarly to Google traffic. Fig. 3(a) shows that international traffic immediately falls to zero and Fig. 3(c) shows that Google (and domestic) traffic decrease slightly after the onset of the reachability disruption. The valley in Fig. 3(c) around 3:30PM was caused by a local failure at UFJF (a reboot of UFJF's border router). Fig. 3(b) shows a burst of international traffic generated by asynchronous applications right after the failure is restored, as we will discuss in Sec. III-C. The impact on the number of established TCP sessions is qualitatively similar (not shown).

Fig. 4 shows the cumulative distribution function of the duration, end-to-end latency, and throughput of TCP connections during the reachability disruption on January 7th (solid lines with circles) and during the same period in the following week (dashed lines with squares, without failures). Results for the other reachability disruptions are quantitatively similar.

Fig. 4(a) shows a 54% reduction of the fraction of connections with duration between 0.5 and 3 seconds and a 16% increase of the fraction of connections with duration larger than 3 seconds, during the period with reachability disruption. Fig. 4(b) shows that end-to-end latency during reachability disruptions is quantitatively similar to the end-to-end latency of domestic flows during normal network operation (compare the lines with cicle and triangle). This indicates that reachability disruptions do not impact end-to-end latency for domestic connections. As expected, international connections have longer end-to-end latencies (line with square). Fig. 4(c) shows that TCP connection throughput does not decrease due to reachability disruptions. Fig. 4(c) also shows that the change in application mix during the disruption (Sec. III-B) does not impact the overall distribution of connection throughput (unlike connection duration in Fig. 4(a)). We also analyzed packet losses of active TCP connections from TCP retransmissions

Table II: Comparison of application traffic during the reachability disruption on January 7th and the same period on the following week (no failure).

Traffic Class	Application	Percentage of Connections		Thousands of Connections		Percentage of Volume		Volume (GB)		Vol/Conn (KB)	
		Jan 7	Jan 14	Jan 7	Jan 14	Jan 7	Jan 14	Jan 7	Jan 14	Jan 7	Jan 14
HTTP	Youtube	3.05	1.09	60.48	63.16	38.42	17.73	55.38	63.62	959.84	1055.54
	Advs	2.32	2.18	46.01	126.32	0.35	0.41	0.50	1.48	11.40	12.29
	Social	—	0.78	—	45.20	—	0.16	—	0.59	—	13.69
	Facebook	—	8.89	—	515.10	—	4.71	—	16.91	—	34.42
	Domestic GET	48.08	23.88	953.42	1383.70	30.76	24.10	44.34	86.47	48.77	65.53
	Domestic POST	1.29	0.74	25.58	42.88	0.35	0.11	0.50	0.39	20.48	9.53
	Peering GET	15.46	3.84	306.57	222.50	10.19	4.31	14.69	15.49	50.24	73.00
	Peering POST	0.90	0.14	17.85	8.11	0.10	0.24	0.15	0.79	8.84	102.27
	Intl GET/POST	—	17.77	—	1029.66	—	25.87	—	92.86	—	94.56
	Other	0.27	1.18	5.35	68.37	0.36	3.54	0.53	12.7	109.92	194.69
SSL/TLS		11.12	18.27	220.51	1058.70	10.62	14.42	15.31	51.75	72.81	51.26
E-Mail		1.36	0.82	26.97	47.51	0.67	0.78	0.96	2.81	37.28	62.03
P2P		0.46	1.20	9.12	69.53	3.34	1.65	4.82	5.91	554.40	89.17
Other		15.69	19.22	311.13	1113.68	4.83	1.97	6.96	7.08	23.46	6.67

and did not observe any significant changes during reachability disruptions (the fraction of bytes retransmitted is below 1.5%, not shown). These results confirm that, even though we do observe some decrease in the total volume of domestic traffic during reachability disruptions, such failures did not cause any noticeable impact on traffic performance. This is expected due to the reduction in overall traffic volume and network utilization.

B. Impact on Application Mix

Tab. II compares traffic of different application classes during the reachability disruption on January 7th and on the same period in the following week. Results for the other two reachability disruptions are qualitatively similar. We aggregate some social applications like Twitter, MSN, and Flickr into "social", several advertisement providers into "Ads", and applications like BitTorrent and eDonkey into "P2P". Some specific applications, such as Facebook and Youtube, which account for a significant fraction of traffic, are considered individually. We aggregate unclassified traffic and other low-traffic applications in "Other". Traffic was classified into applications by TSTAT; we extend TSTAT to classify encrypted Facebook traffic by identifying BGP prefixes used by Facebook servers (same methodology used for Google services in Sec. III-A).

On one hand, Facebook traffic reduces to zero during the failure as it is hosted out of Brazil. On the other hand, Youtube, which peers at the São Paulo exchange point, experiences one of the smallest relative decreases in traffic volume among applications that are locally hosted. Similarly, we have observed that some domestic news and entertainment sites may receive *more* traffic during the failure than during normal network operation (e.g., Globo.com portal, not shown). One of the domestic sites with highest traffic *decrease* is Yahoo! Brasil, as most of its content is hosted abroad and cannot be fetched from Yahoo!'s international website. This indicates that users are flexible and migrate to services that remain reachable during reachability disruptions.

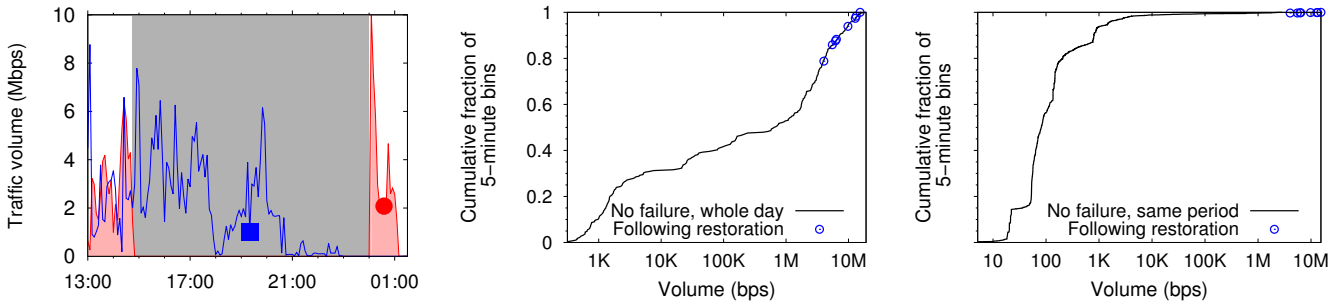
We note that the fraction of traffic to file hosting services and P2P applications is small, regardless of the occurrence of failures, due to firewall rules at UFJF that block these applications. Thus, we did not observe clear tendencies and cannot tell whether changes in P2P traffic are due to the reachability disruptions.

We have also observed that the fraction of connections and traffic for most application classes return to their normal levels 30 minutes after the resolution of reachability disruptions (not shown). For example, 30 minutes is sufficient for the fraction of Facebook connections to return to the same level observed during periods with no failure.

C. Impact on Application Behavior

Fig. 5(a) shows traffic volume, aggregated in 5-minute intervals for Dropbox connections. As Dropbox is hosted on Amazon Web Services, all traffic is interrupted during reachability disruptions (shaded period). A similar pattern is observed for SMTP traffic (omitted), which decreases significantly during the failure as part of the traffic, directed to international domains, is interrupted. Disruption resolution (at 0:05AM in Fig. 5(a)) triggers the execution of tasks accumulated by both applications during the disruption and a burst of traffic (i.e., synchronization of new and modified files on Dropbox or queued-up e-mails in SMTP servers). The burst significantly increases the traffic sent by each application and has a relatively short duration, between 30 minutes and 1 hour. We expect other asynchronous applications to show similar behavior.

Fig. 5(b) compares Dropbox traffic bursts to overall Dropbox traffic, showing the cumulative distribution function of Dropbox traffic volume aggregated over 5-minute intervals. The solid line shows Dropbox traffic over all 5-minute intervals during a day when no failure was reported (January 17th). The highlighted dots represent Dropbox traffic over the eight five-minute intervals following the restoration of the reachability disruption on January 10th. We focus on the reachability



(a) Dropbox traffic (b) Dropbox burst vs. overall traffic (c) Dropbox burst vs. typical traffic

Figure 5: Impact of failures on Dropbox traffic (similar to SMTP and possibly other asynchronous applications). Highlighted dots in subfigures (b) and (c) show Dropbox traffic volume over 5-minute intervals following resolution of the reachability disruption on January 10th.

Table III: Analyzed intradomain failures reported by RNP in 2013.

Start	Duration	Failed Links	Route to SP	Impact
Jul 9th, 8:48AM	5h00	SP-MG SP-SC	backup, MG-DF-RJ-SP, 10 Gbps	low
Aug 19th, 8:10AM	4h30	SP-RJ	default, MG-SP, 10 Gbps	low
Aug 28th, 3:10PM	3h30	MG-SP SP-RJ MG-DF **+4**	9 hops, 3 Gbps	high
Nov 21st, 9:00AM	7h30	MG-SP SP-RJ	7 hops, 3 Gbps	high

disruption on January 10th because it was the disruption with the earliest resolution time (7:55PM), when more users were still active in the campus and thus still using Dropbox, although results for other days and different disruption restoration times are qualitatively similar. We see that intervals following the disruption resolution have traffic volume larger than most 5-minute intervals over the whole day, and is comparable to Dropbox traffic volumes during peak utilization periods (top 20% of 5-minute bins).

Fig. 5(c) compares Dropbox traffic bursts to typical Dropbox traffic at the time when the reachability disruption was restored. Once again, the highlighted dots show Dropbox traffic over the eight 5-minute intervals following the restoration of the reachability disruption on January 10th. The solid line shows Dropbox traffic during 5-minute intervals during the time period on days when no failure was reported (January 16th, 17th, and 18th). Fig. 5(c) shows that Dropbox bursts are an order of magnitude higher than typical Dropbox traffic for the same time period. Currently, cloud storage and file hosting applications account for a small but non-negligible fraction of traffic on UFJF's network (Dropbox accounts for 4% of traffic at UFJF). Traffic bursts combined with a possible future increase of the traffic volumes of these applications may compromise network performance after failure restorations, degrading the experience provided by interactive applications like VoIP.

IV. Impact of Performance Disruptions

RNP reported failures on intradomain links caused by problems on the underlying optical infrastructure on four occasions during the second half of 2013. Intradomain failures resulted in routing changes, congestion, and performance degradation; but no reachability problems. We refer to these failures as *performance disruptions* and study their impact on UFJF's traffic (Sec. IV-A) and application mix (Sec. IV-B). We also correlate performance disruptions with RNP's topology (Sec. IV-C).

A. Impact on Traffic

The São Paulo exchange point is RNP's peering point for all Google and international traffic (which together average 76% of UFJF's total traffic), as well as the majority of domestic traffic. Thus, the route between UFJF and the São Paulo exchange point is critical for performance. Tab. III shows start times, durations and failed links for each disruption (see Fig. 1). Tab. III also describes the route to the São Paulo exchange point and the degree of impact of each failure (high or low). The default route from UFJF to the São Paulo exchange point is MG-SP and the backup route is MG-DF-RJ-SP, as indicated in Tab. III. RNP exchange points and some routes can be seen on Fig. 1.

The first two performance disruptions do not break both UFJF's default and backup routes toward São Paulo, and thus have low impact on UFJF's traffic. We focus our analysis on the performance disruptions on August 28th and November 21st, as they impacted more links and broke both default and backup routes toward São Paulo. These last two disruptions caused traffic to traverse longer routes (at least seven hops), congestion at low-capacity links, and significant performance degradation.

The red line with a circle on Fig. 6 shows total traffic volume on August 28th, when RNP reported failures on seven intradomain links. For comparison purposes, the blue line with a square on the same figure shows total traffic volume on the same period in the previous week, when no failure was reported. The seven links do not fail simultaneously. Total traffic volume decreases slightly after failure of the default route at 3:10PM (shaded area), then sharply at 3:45PM (black vertical line) when the backup route fails and congestion starts. Traffic stabilizes around 22% of the normal volume

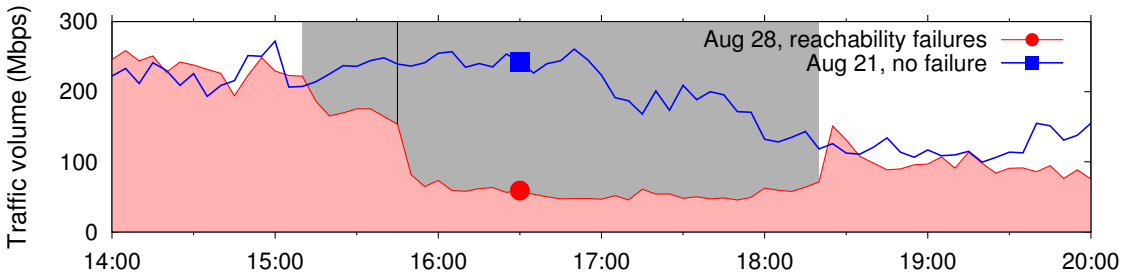
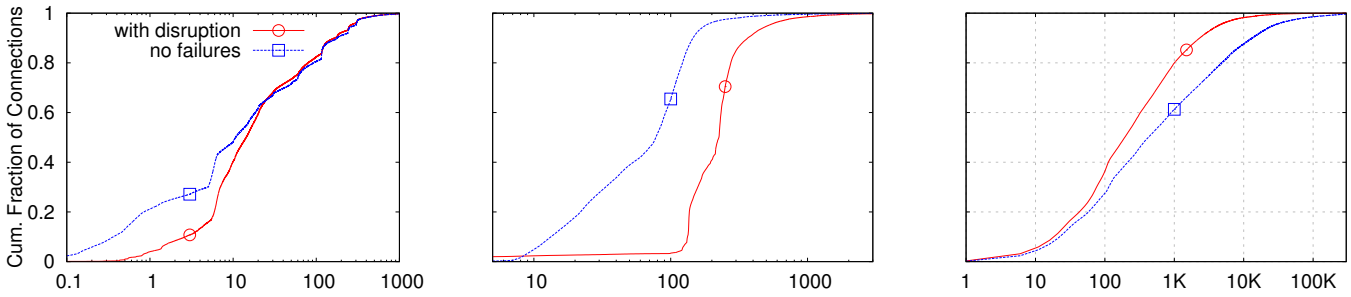


Figure 6: UFJF's traffic overview during RNP performance disruptions.



(a) Duration (s) (b) End-to-end latency (ms) (c) Throughput (Kbps)

Figure 7: Performance comparison of TCP connections during the performance disruption on August 28th and the same period with no failure.

five minutes after failure of the backup route. Similar to *reachability disruptions*, we have observed that 30 minutes is sufficient for traffic to normalize after the restoration of performance disruptions. In the rest of this section we report results computed over the period after failure of the backup route (black vertical line).

The impact of performance disruptions is very similar for domestic, international and Google traffic (as defined in Sec. III-A). This is because all traffic shares the same (congested) route toward the São Paulo exchange point, where other Brazilian networks and Google peer with RNP, and where RNP's international link terminates.

Fig. 7 shows the cumulative distribution functions of duration, average end-to-end latency, and average throughput of TCP connections. We show metrics computed during the performance disruption on August 28th (after failure of the backup route) and during the same period in the previous week, when no failure was reported. Fig. 7(a) shows that connections get significantly longer. This increase in flow duration is a result of both higher end-to-end latency and lower throughput. Indeed, Fig. 7(b) shows significant increase in end-to-end latency due to the longer route toward the São Paulo exchange point (Sec. IV-C), which increases to approximately 146ms (from 28ms). Fig. 7(c) confirms that congestion impacts available bandwidth as less than 1% of TCP connections have average throughput higher than 10 Mbps during this performance disruption. During the disruption, the average TCP connection retransmission rate increases from 1.3% to 6.8% during the same period when there is no failure (not shown). These results show that the performance disruptions studied have significant negative impact on traffic performance and ultimately on user experience.

B. Impact on Application Mix

We also evaluated changes to application mix during performance disruptions. Similar to Tab. II, Tab. IV shows traffic statistics for different application classes during the performance disruption on August 28th. Results are qualitatively similar for the other high-impact performance disruption. We find that all applications continue working during performance disruptions, but at degraded performance. The most significant change observed was a reduction in traffic volume for bandwidth-intensive applications like Youtube. As shown in Tab. IV, Youtube traffic decreased to less than 3% of its normal volume during the performance disruption. Moreover, the average volume per connection decreased to 70KB, indicating that users probably give up watching a video after frequent buffering episodes. To further illustrate this point, Fig. 8 shows Youtube traffic over time during the disruption failure and during the same period in the previous week. We observe that the amount of Youtube traffic is close to zero throughout the disruption.

In contrast, the impact on the volume of Facebook traffic is not as significant. This finding agrees with what we observed for reachability disruptions: users adapt to network conditions and turn to applications that are not (as severely) impacted by disruptions. During performance disruptions, users focus on applications with lower latency and bandwidth requirements. Even though longer latencies are known to impact user experience [13], [14], our data indicates that its impact is minor compared to congestion. Tab. IV shows that the decrease in Facebook traffic is smaller than in HTTP GET traffic; which may indicate that, in general, Facebook is more resilient to performance disruptions than other websites.

Table IV: Comparison of application traffic during the performance disruption on August 28th and the same period on the previous week.

Traffic Class	Application	Percentage of Connections		Thousands of Connections		Percentage of Volume		Volume (GB)		Vol/Conn (KB)	
		Aug 28	21	Aug 28	21	Aug 28	21	Aug 28	21	Aug 28	21
HTTP	Youtube	0.87	1.13	16.27	22.69	2.44	19.89	1.09	35.56	70.25	1643.34
	Advs	1.59	2.85	29.73	57.23	0.77	0.40	0.34	0.72	11.99	13.19
	Social	0.36	0.37	6.73	7.43	0.19	0.11	0.08	0.20	12.46	28.23
	Facebook	3.22	3.71	60.13	74.49	3.87	2.47	1.73	4.41	30.17	62.08
	Domestic GET	15.06	18.17	281.63	364.85	28.54	23.19	12.75	41.46	47.47	119.16
	Domestic POST	0.71	0.68	13.28	13.65	0.45	0.14	0.20	0.26	15.80	19.97
	Peering GET	3.49	4.38	65.26	87.95	5.10	2.27	2.28	4.01	36.63	47.81
	Peering POST	0.43	0.47	8.04	9.44	0.06	0.19	0.06	0.34	7.82	37.78
	Intl GET/POST	15.59	18.92	291.54	379.91	21.00	22.19	9.52	39.73	34.24	109.66
	Other	0.26	0.60	4.86	12.05	0.67	4.31	0.11	7.69	23.72	669.23
SSL/TLS		29.38	29.62	549.50	594.77	30.06	19.13	13.42	34.20	25.61	60.29
E-Mail		0.08	0.52	1.50	10.44	1.78	0.94	0.80	1.69	560.74	169.72
P2P		0.31	0.63	5.80	12.65	0.26	1.72	0.12	3.08	21.71	255.31
Other		28.65	17.95	535.77	360.43	4.82	3.06	2.15	5.47	4.21	15.91

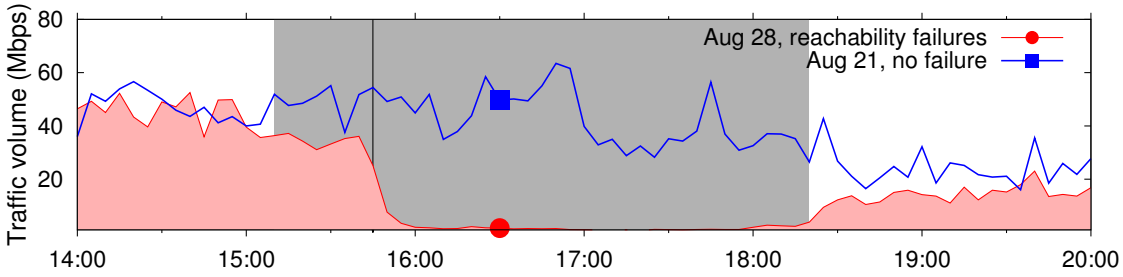


Figure 8: Comparison of Youtube traffic during the performance disruption on August 28th and the same period in the previous week.

Tab. IV also shows that the number of TCP connections does not decrease significantly during the performance disruption. In particular, the rate of new connections remains at 97% of the normal rate in the middle of the disruption's duration (5PM, not shown). This indicates that users and applications persist on using the network despite performance disruption. This result is different from that observed during reachability disruptions, where the number of connections decreased significantly even for websites that remained reachable. We note, however, that the number of TCP connections with no data increases by 56% (not shown), which explains the 10% increase of "Other" connections during performance disruptions in Tab. IV.

C. Relationship with Network Topology

Recall that Tab. III shows four cases of performance disruptions. Whereas the first two affected only a few links, the last two impacted a larger number of more important links. We now discuss the impact of these performance disruptions in light of the topology of RNP's backbone. In particular, we try to explain why performance disruptions have low or high impact by looking at RNP's network topology.

Fig. 1 shows an overview of RNP's network topology with sufficient detail for our analysis; the full topology is available at our dataset's website [11]. We identify the routes used by UFJF's traffic to reach the São Paulo exchange point during performance disruptions using iPlane [15] traceroutes collected from PlanetLab nodes at the Universidade Federal de Minas Gerais (UFMG). UFMG operates RNP's Minas Gerais (MG) exchange point, where UFJF peers, so UFMG's PlanetLab nodes use the same routes as UFJF's traffic. Given that we know the RNP exchange point where each federal university in Brazil peers, we compute the round-trip times from UFJF to each RNP exchange point by grouping TCP connections between UFJF and other federal universities.

The first two performance disruptions impact few links; they allow traffic to flow on the default or backup routes, which have 10 Gbps bandwidth and do not take long detours. There is no congestion during the first two disruptions and the average increase in round-trip times is 13 ms (not shown). We did not observe any significant changes in traffic patterns during these performance disruptions, which illustrates Internet's ability to mask failures.

The last two performance disruptions impact several links and break both default and backup routes. During these disruptions, traffic from Minas Gerais's exchange point (including UFJF's traffic) have to travel north, traverse several exchange points in Brazil's northeast region, before coming south again to São Paulo. RNP's links in the northeast are provisioned for lower traffic demands and have less capacity (3 Gbps and 1 Gbps links are common). Congestion happens when failures reroute a lot of traffic onto these low-capacity links, and round-trip times increase significantly due to the long detour.

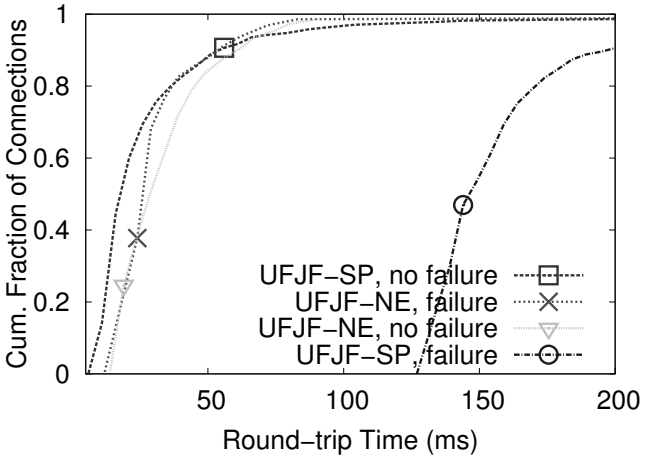


Figure 9: Comparison of round-trip time between UFJF RNP exchange points located in São Paulo and Brazil's northeast region for the reachability failure on August 28th.

Fig. 9 shows the round-trip time of TCP connections from UFJF to other universities during the performance disruption on August 28th and during the same period on the previous week. We show two curves for connections toward RNP's exchange points in the northeast and two curves for connections toward the São Paulo exchange point. We note only a small fraction (less than 0.5%) of UFJF's traffic is toward the northeast region when there is no disruption. The increase in round-trip times toward the São Paulo exchange point during high-impact disruptions is expected. However, rerouting during the performance disruption resulted in shorter routes (through lower-capacity links) toward northeastern exchange points during performance disruptions. This results in lower round-trip times to northeastern exchange points reached before traversing the congested links. This illustrates that failures may have mixed performance impact, even if for a small fraction of traffic. It also shows that default routes to the northeast region are not optimized for minimizing round-trip times.

In summary, our results show that reachability and performance disruptions have different impact on traffic as well as on application and user behavior. Our analyses also illustrate how knowledge of routes and network topology are useful for understanding the impact of failures.

V. Related Work

Detecting, understanding, and troubleshooting network disruptions is imperative to efficient and reliable communications. We now discuss previous work related to these topics. We note that this paper builds on our previous work (in Portuguese, see [11]) with a more thorough discussion about reachability disruptions and adding the study on performance disruptions.

Failure detection. The majority of network failures are detected by network equipment and automatically reported to operators by tools such as SNMP and syslog [1], [5], [16]. Unfortunately, some failures like those caused by software bugs and misconfiguration are not reported by network equipment, making their detection challenging. Moreover, only operators have access to network equipment and their reports. An alternative approach is to use active network measurements to detect and identify failures [2]–[4], [17]–[19]. Solutions in this category correlate complex network measurement techniques (e.g., Reverse Traceroute [20] and IP aliasing [21]) collected from diverse sources to detect when a failure happens and locate it. In this work we characterize failures reported by RNP operators (ground truth). We note that our results may provide insights that may be useful for improving existing failure and anomaly detection techniques and that our approach in Sec. IV-C was inspired by existing network tomography systems [2], [4], [19].

Failure characteristics. Researchers have characterized failures in CENIC [5] and Sprint [1]. In these networks, two common types of disruptions are scheduled maintenance and intermittent connectivity problems caused by malfunctioning hardware. These studies also show that no link is free of failures, but that some links are more likely of experiencing failures than others (e.g., due to different link-layer technologies). Recent work has characterized failures in datacenter networks [22], [23]. They show that, in datacenter networks, middleboxes dominate failure occurrences with short software-related faults and that middlebox and network redundancy is only partially successful in mitigating failures. Our study complements these prior studies by characterizing the impact of different failures on the network traffic as well as on user behavior. We are unaware of other prior studies using information from operational networks, possibly because operators seldom publish details on their networks and datacenters.

Most research on failure detection and identification using network measurements apply their techniques in the Internet and characterize the observations. These characterizations are not as detailed as the studies using information from network equipment mentioned above, but cover multiple networks and are more representative of the Internet. For example, Trinocular [17] found that, on average, 0.15% of Internet prefixes normally reachable are unreachable at any given time. Other studies found that most failures last for only a few minutes, but that a few long-lived failures account for most of the downtime [3], [4]. Unlike these prior studies, our focus is on the impact of failures on traffic and user behavior.

Failure impact. Several studies have characterized the impact of failures on Internet routing [8], [24]–[26], showing failures are usually followed (or even preceded) by BGP updates. Although routing events have been shown to correlate with network performance degradation [24], these studies do not consider the impact of failure on users. A recent paper shows that most issues on the Outages mailing list are reported by users [27], confirming that users are sensitive to failures and that understanding the impact of failures on user traffic is important. Unfortunately, we are aware of only a few studies about the impact of failures on users. A key challenge is that measurements of traffic impacted by a failure, and related information, are seldom available. This makes it impossible to evaluate the impact of most failures. For example, although researchers have characterized Egypt's shutdown of international links in 2012 [28], the lack of available traffic measurements collected inside Egypt makes it impossible to characterize the impact of the shutdown on user behavior and traffic. In this paper, we characterize the impact of two different types of disruptions on user traffic. In a sense, our work shares similarities (though different goal) to previous work that characterized the impact of round-trip times on user

patience [14] or the impact of datacenter failures on service availability and traffic [23].

VI. Discussion and Future Work

In this work, we have characterized the impact of seven failures in Brazil's national education and research network (RNP) on traffic at a large client university. The failures last for several hours and fall into two categories: Reachability disruptions that block all international traffic but do not impact domestic traffic, and performance disruptions that degrade network performance for all destination but do not cause unreachability. Our analysis combines multiple data sources including gigabytes of traffic flows, snapshots of RNP's topology, and traceroute measurements during the failures.

We have focused on the impact of failures on traffic and user behavior. Our characterization shows that users adapt their behavior according to network state. For example, users migrate from Facebook to Youtube during reachability disruptions, when Facebook becomes unavailable. Conversely, users migrate from Youtube to Facebook during performance disruptions, when congested links degrade Youtube experience. We have also found that asynchronous applications like Dropbox and e-mail generate traffic bursts upon failure restoration. Finally, we have found that the impact of performance disruptions depends on whether failed links break both the default and the backup routes between major PoPs; knowledge of routes used during the failures was essential for this analysis.

Our results shed new light and improve our understanding of the impact of network failures on traffic and user behavior. Although our results are specific to one network and the particular failures analyzed, the observed patterns may generalize to other networks, in particular university networks. We also believe our dataset is valuable for studying the impact of failures and may be useful for other analyses not covered in this study; we make our dataset publicly available [11].

We are working with other universities in Brazil to extend our data collection infrastructure and obtain more data for analysis of future failures. We also want to investigate how to apply our findings to network operation practices, e.g., how to provision backup routes to avoid congestion or where to setup new peering relationships to improve interdomain redundancy.

Acknowledgements

This research is partially funded by the Brazilian National Institute of Science and Technology for Web Research (Grant 573871/2008-6), and by the authors' individual grants from CNPq, CAPES, FAPEMIG, and RNP.

References

[1] A. Markopoulou, G. Iannaccone, S. Bhattacharyya, C. N. Chuah, Y. Ganjali, and C. Diot, "Characterization of Failures in an Operational IP Backbone Network," *IEEE/ACM Trans. Netw.*, vol. 16, no. 4, pp. 749–762, 2008.

[2] R. Kompella, J. Yates, A. Greenberg, and A. Snoeren, "Detection and Localization of Network Blackholes," in *Proc. IEEE INFOCOM*, 2007.

[3] E. Katz-Bassett, H. Madhyastha, J. P. John, A. Krishnamurthy, D. Wetherall, and T. Anderson, "Studying Black Holes in the Internet with Hubble," in *Proc. USENIX NSDI*, 2008.

[4] E. Katz-Bassett, C. Scott, D. R. Choffnes, I. Cunha, V. Valancius, N. Feamster, H. V. Madhyastha, T. Anderson, and A. Krishnamurthy, "LIFEGUARD: Practical Repair of Persistent Route Failures," in *Proc. ACM SIGCOMM*, 2012.

[5] D. Turner, K. Levchenko, A. Snoeren, and S. Savage, "California Fault Lines: Understanding the Causes and Impact of Network Failures," in *Proc. ACM SIGCOMM*, 2010.

[6] Z. Zhang, Y. Zhang, Y. C. Hu, Z. M. Mao, and R. Bush, "iSPY: Detecting IP Prefix Hijacking On My Own," in *Proc. ACM SIGCOMM*, 2008.

[7] A. Lakhina, M. Crovella, and C. Diot, "Diagnosing Network-wide Traffic Anomalies," in *Proc. ACM SIGCOMM*, 2004.

[8] R. Hiran, N. Carlsson, and P. Gill, "Characterizing Large-scale Routing Anomalies: A Case Study of the China Telecom Incident," in *Proc. PAM*, 2013.

[9] S. Sundaresan, N. Feamster, R. Teixeira, and N. Magharei, "Measuring and Mitigating Web Performance Bottlenecks in Broadband Access Networks," in *Proc. IMC*, 2013.

[10] A. Finamore, M. Mellia, M. Meo, M. M. Munafò, and D. Rossi, "Experiences of Internet Traffic Monitoring with tstat," *IEEE Network*, vol. 25, no. 3, pp. 8–14, 2011.

[11] "Traffic at a University Campus During Provider Failures," http://netlab.ice.ufjf.br/tracesRNP/.

[12] I. Poese, S. Uhlig, M. A. Kaafar, B. Donnet, and B. Gueye, "IP Geolocation Databases: Unreliable?" *SIGCOMM Comput. Commun. Rev.*, vol. 41, no. 2, pp. 53–56, 2011.

[13] D. Zats, T. Das, P. Mohan, D. Borthakur, and R. Katz, "DeTail: Reducing the Flow Completion Time Tail in Datacenter Networks," in *Proc. ACM SIGCOMM*, 2012.

[14] S. Stefanov, "YSlow 2.0," in *CSDN SC2C*, 2008.

[15] H. Madhyastha, T. Isdal, M. Piatek, C. Dixon, T. Anderson, A. Krishnamurthy, and A. Venkataramani, "iPlane: an Information Plane for Distributed Services," in *Proc. USENIX OSDI*, 2006.

[16] D. Watson, F. Jahanian, and C. Labovitz, "Experiences with Monitoring OSPF on a Regional Service Provider Network," in *Proc. of IEEE ICDCS*, 2003.

[17] L. Quan, J. Heidemann, and Y. Pradkin, "Trinocular: Understanding Internet Reliability Through Adaptive Probing," in *Proc. ACM SIGCOMM*, 2013.

[18] A. Dhamdhere, R. Teixeira, C. Drovolis, and C. Diot, "NetDiagnoser: Troubleshooting Network Unreachabilities Using End-to-end Probes and Routing Data," in *Proc. ACM CoNEXT*, 2007.

[19] N. Duffield, "Network Tomography of Binary Network Performance Characteristics," *IEEE Trans. on Inf. Theory*, vol. 52, no. 12, pp. 5373–5388, 2006.

[20] E. Katz-Bassett, H. Madhyastha, V. Adhikari, C. Scott, J. Sherry, P. van Wesep, A. Krishnamurthy, and T. Anderson, "Reverse Traceroute," in *Proc. USENIX NSDI*, 2010.

[21] K. Keys, Y. Hyun, M. Luckie, and k. claffy, "Internet-Scale IPv4 Alias Resolution with MIDAR," *IEEE/ACM Trans. Netw.*, vol. 21, no. 2, pp. 383–399, 2013.

[22] R. Potharaju and N. Jain, "Demystifying the Dark Side of the Middle: a Field Study of Middlebox Failures in Datacenters," in *Proc. IMC*, 2013.

[23] P. Gill, N. Jain, and N. Nagappan, "Understanding Network Failures in Data Centers: Measurement, Analysis, and Implications," in *ACM SIGCOMM Computer Communication Review*, vol. 41, no. 4, 2011, pp. 350–361.

[24] N. Feamster, D. Andersen, H. Balakrishnan, and F. Kaashoek, "Measuring the Effects of Internet Path Faults on Reactive Routing," in *Proc. ACM SIGMETRICS*, 2003.

[25] Y. Zhang, Z. Mao, and J. Wang, "A Framework for Measuring and Predicting the Impact of Routing Changes," in *Proc. IEEE INFOCOM*, 2007.

[26] J. Li and S. Brooks, "I-seismograph: Observing and Measuring Internet Earthquakes," in *Proc. IEEE INFOCOM*, 2011.

[27] R. Banerjee, L. Chiang, A. Mishra, A. Razaghpanah, V. Sekar, Y. Choi, and P. Gill, "Internet Outages, the Eyewitness Accounts: Analysis of the Outages Mailing List," in *Proc. PAM*, 2015 (to appear).

[28] A. Dainotti, C. Squarcella, E. Aben, K. C. Claffy, M. Chiesa, M. Russo, and A. Pescapé, "Analysis of Country-wide Internet Outages Caused by Censorship," in *Proc. IMC*, 2011.