Controlled Internet Outage Monitoring

Christian Köpp
Supervisor: Lukas Schwaighofer
Seminar Future Internet WS12/13
Chair for Network Architectures and Services
Department of Computer Science, Technical University of Munich
Email: christian.koepp@cs.tum.edu

ABSTRACT

This paper is about the measurement of Internet outages with a focus on the Border Gateway Protocol, as one of the most common routing protocols. First some background information about the protocol and its tasks are described, followed by a concrete example of last year's events in Egypt. Thereafter a self-made analysis regarding the earthquake in New Zealand in 2011 is presented. Finally a conclusion about Internet outages and their monitoring with data collected by the Border Gateway Protocol is given. The conclusion also includes a short passage about recent papers and methods involving Internet outage monitoring in current academic research with a focus on the role of BGP within those.

Keywords

Inter-Domain Routing, Outages, Connectivity Disruption, Border Gateway Protocol, BGP, Earthquake, Censorship

1. INTRODUCTION

Routing protocols are indispensable on the Internet nowadays. Their goal is to guarantee the ability of communication between different networks and they attempt to find an efficient way to get packages from its source to its destination. Furthermore modern routing protocols often counteract events like natural disasters and even political censorship actions, as they are designed to be resilient against communication interruptions. Due to this routing protocols are trying to circumvent these interruptions and to establish new paths to those effected networks. Nevertheless there are events, either triggered by political or natural issues, which lead to serious connectivity disruptions or even result in an outage of a whole geographical area.

Natural disasters like the massive earthquake in Japan with 8.9 magnitude on March 11th of 2011 can lead to outages. For example the mentioned earthquake caused the destruction of technical equipment, especially undersea cables necessary for connecting the Japanese islands with the Asian coastline [1]. But also smaller and more regional events like bad weather can lead to a temporary Internet outage in smaller areas [2].

But natural incidents are not the only events that can cause such critical Internet outages. Governments and dictatorships are able to force (state-owned) providers to cut their lines and to disable their services as a method of censorship. Political issues like these were, for example, observed during the uprising in Egypt and Libya at the beginning of 2011 [3]. Another incident happened in 2008 during Pakistan's try to deny access to YouTube. During this operation a Pakistani Internet service provider unintentionally announced routes globally and hijacked the YouTube traffic [4]. The most recent example is the ongoing civil war in Syria, which led to a temporary Internet outage of Syria in June 2012 [5].

In this paper we will only have a look at events related to the Border Gateway Protocol and its behaviour. BGP is the major protocol for inter-domain-routing between international providers. Due to the popularity of BGP, official Autonomous Systems are expected to be able to communicate with BGP. This is the reason why changes made through the protocol can get propagated throughout the world and therefore lead to global scale changes of routing decisions of core networks. Finally such path changes through BGP can result in different packet flows and connectivity of Internet hosts all around the world.

2. BACKGROUND

This chapter describes the techniques, protocols and standards of the major routing and reachability information sharing issues currently used on the Internet.

2.1 Autonomous Systems

Nowadays the Internet is a giant interconnected network consisting of a huge amount of independent networks with different sizes and geographical locations. An Autonomous System (AS) is a network, which consists of a collection of Internet Protocol routing prefixes under the control of at least one network operator [6]. Typically providers of such networks are Internet Service Providers (ISP) and big companies with multiple connections to different networks. As part of the official process to get registered as an AS, an organisation has to request an Autonomous System Number (ASN). This 32 bit ASN [7] is used to uniquely identify an AS and is assigned to an organisation by the Internet Assigned Numbers Authority (IANA) and its regional representatives, the Regional Internet Registries (RIR).

2.2 Border Gateway Protocol

The Border Gateway Protocol is a protocol for exchanging network layer reachability information (NLRI) between and within autonomous systems. The first version of BGP was introduced in 1989. Until now there have been several changes to the standard and therefore different versions of BGP with version 4 being the current one [8].

doi: 10.2312/NET-2013-02-1_02

Routers communicating through BGP are called peers as they are equally privileged participants during the communication. To establish a certain reliability of the messages, BGP makes use of the Internet Protocol and the Transport Control Protocol (TCP/IP). Traditionally BGP can be found on TCP port 179.

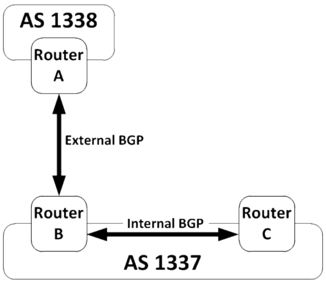

Figure 1: Difference between EBGP and IBGP

If the Border Gateway Protocol is used to share NLRI between autonomous systems it is called External BGP (EBGP). Naturally those exterior exchanges are done between edge routers of different AS while interior information exchanges do not necessarily happen only between edge routers of an AS. An exchange within an AS and between its routers is called Internal BGP (IBGP) like figure 1 demonstrates. This paper is focusing on EBGP as it analyses outages of whole IP ranges within a global scale.

2.2.1 *Making routing decisions with BGP4*

A BGP4 router is equipped with a special kind of database, the Routing Information Base (RIB) which is made up of two different parts. The central database within the RIB is the routing table. This is the place where all the information needed for making routing decisions is stored. A policy, referred to as local RIB, defines how incoming information of adjacent routers is treated and which information is passed on to other adjacent peers afterwards. The local RIB is also responsible for writing received information to the routing table. Therefore it is possible to call the local RIB a kind of configuration for a router. Figure 2 explains the relations of the different sections involved in routing decisions in a graphical way. Since companies typically try to minimize their costs, this configuration is often not purely based on technical facts but on economical reasons. These costs are usually based on the amount of traffic transmitted to another network and can therefore lead to slower but more economical routing decisions [9]. Due to this reason not all routes learned through BGP are automatically stored within the routing table itself. Furthermore, there is always exactly one route to an unique IP prefix stored in the routing table.

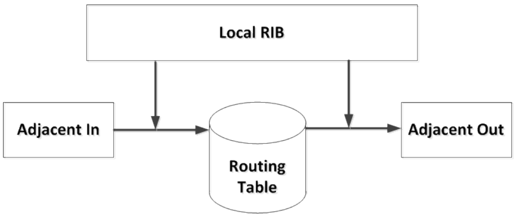

Figure 2: Scheme of the Routing Information Base

Another fundamental rule which all routing decisions are based on is the usage of the most specific IP prefix available. Technical manuals are calling this strategy the longest prefix match [10]. The length of the prefix can easily be determined by looking at the length of the subnet-mask of an entry in the RIB. Figure 3 shows an example usage of this strategy.

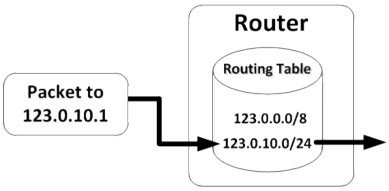

Figure 3: Example usage of the longest prefix match

2.2.2 *Information exchange through BGP4*

Every BGP message, regardless of its type, consists of a 19-byte header followed by a payload of variable length. Within the header block there is a type field which contains one out of five defined BGP message types. In this paper just the types `OPEN`, `UPDATE`, `NOTIFICATION` and `KEEPALIVE` are of particular interest [8]. Therefore the `ROUTE-REFRESH` message type is not explained nor used in this paper [11].

The first action two peers have to do to exchange reachability information is the establishment of a TCP channel between them. The peers try to keep this connection alive during their whole uptime. If a BGP session between two peers exists they are called neighbours. After the TCP handshake is done the initiator of the BGP session sends an `OPEN` message to the other peer. In the payload of the message there is the unique ASN of which the source router is part of. It also contains a unique ID of the sending router. Usually the router ID is the IP address of the router if BGP is used in combination with TCP/IP. An accepted `OPEN` message is indicated by responding with a `KEEPALIVE` message as this message type consists only of the header block and an empty payload. If both peers sent their `OPEN` messages and received an `KEEPALIVE` message afterwards, the exchange of reachability information is able to start.

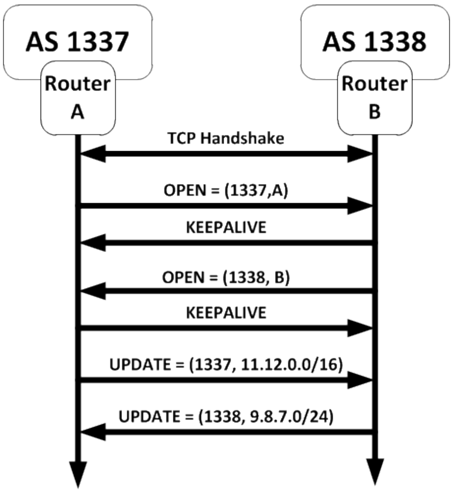

Figure 4: Example BGP session

But the KEEPALIVE messages do have another important function within the protocol. They are used as a kind of heartbeat message between two peers. If a peer doesn't receive a KEEPALIVE message in a certain defined timespan the other peer is assumed to be not available. As a result of this, all routes announced by this peer that were stored in the RIB are treated as invalid and are not used anymore. The router immediately tries to figure out the best route to the affected IP ranges. If there is an alternative route available the router propagates this new route to its neighbours. If the router was not able to find another route a withdrawal is sent to the neighbours as the router is not able to forward packages to this IP range any more.

With the UPDATE message type it is possible for a router to announce new routes to a certain IP range. Included in the message there is always a detailed path-information with all AS on the way to the destination IP range. So other routers can use the whole path to determine if the newly announced route is better than their current one. Therefore an UPDATE message can also be seen as the promise of a peer to forward any datagrams towards the announced prefix.

Furthermore, the UPDATE message can also be used to withdraw previously announced routes. Due to different fields within those messages, it is perfectly valid and possible to withdraw routes and announce new ones in one single message. IP ranges are always given in CIDR [12] notion like 127.0.0.0/8. It is also possible to do an implicit withdrawal which is done when a new route to an IP range is announced even if there still is an existing one stored on the router. In this case the old route is overwritten with the new one.

A NOTIFICATION message is only sent from a peer to indicate that there was some kind of error in either receiving or processing the last BGP message. Therefore this message type contains fields like error code, error subcode and optional information about the reason of sending this message. Some critical errors can also lead to a truncation of the session.

3. ANALYSIS

In this section two events are analysed. One being an event triggered by political issues, the other one was caused by a natural disaster. Both events left traces detectable by having a closer look at publicly available BGP archives. The analysis of the political motivated censorship observed in January 2011 in Egypt is based on existing papers and articles. Contrastingly, the analysis of the earthquake near Christchurch in New Zealand in February 2011 is done by the author in coordination with his supervisor.

3.1 Uprising in Egypt in 2011

During the so called "Arab Spring" there have been several uprisings in African and Arabic countries including Egypt as one of the first countries where protests started [13]. These Egyptian protests were organized using social networks and messaging services on the Internet [14]. Over time the uprising in the capital Cairo became regular and increased in numbers and even similar events started to happen in other major cities of Egypt. Finally those events resulted in the resignation of the Egyptian President Hosni Mubarak on the 11th of February and in massive changes in the political system of Egypt [15].

Nevertheless the former government decided to take actions against the protests in form of blocking the communication infrastructure of the demonstrating people. The government censored access to social media portals and messaging services for Egyptian Internet users on January the 25th 2011 [3]. Although the government officially denied the existence of an order to block services like Twitter and Facebook [16], there were users that verified the blocking of services [17] and even Facebook announced a drop in user activities of its Egyptian users during this time [18].

3.1.1 BGP as a method of censorship

Because the blockade of websites did not stop the protests from happening and even increased them throughout Egypt the government ordered a complete blockade of all Internet traffic for Egyptian people. Due to this decision a whole country including 20 million Internet users [19] temporarily vanished from the Internet for about four days.

To understand how this massive blockade of nearly all Internet-based communication happened, it is necessary to have a look at the Egyptian Internet infrastructure which is dominated by a few big players with the Ramses Exchange being the major hub for their international Internet communication. The Ramses Internet Exchange is one of the biggest Internet exchange points in Northern Africa and the Middle East, connecting Egypt with other countries through submarine cables in the Suez canal [20]. Sources claim that all those big ISPs and of course the Ramses Exchange are controlled by the state [21].

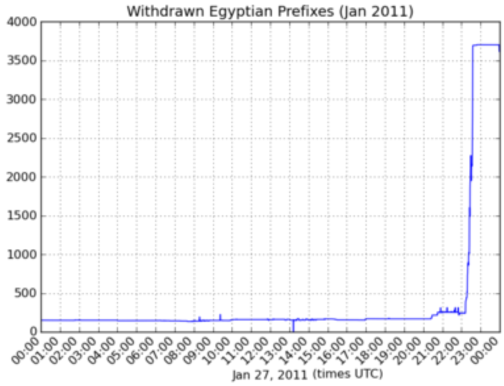

Figure 5: Announced Egyptian IPv4 prefixes as seen from AS20928 on the 27th of January 2011

Keeping this information in mind, it is easier to understand how the simultaneous withdrawal of nearly all Egyptian IPv4 prefixes at around 22:34 UTC on the 27th of January 2011 could happen [22]. Other outage measure methods like the Internet Telescope also observed a significant drop of traffic from Egypt hosts during this time [3]. Figure 5 was created by James Cowie [22] and shows the approximate time of the withdrawals made by Egyptian ISPs through BGP. In the first hours of the 28th of January there were only a few IPv4 prefixes left announced. Nevertheless it was reported that the Egyptian Stock Exchange was still accessible via AS20928 (Noor Group) after nearly all Egyptian IPv4 prefixes were withdrawn [22].

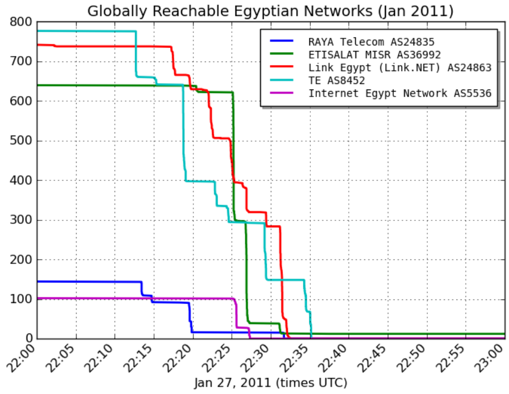

Figure 6: Detailed time-line of the withdrawals of all major Egyptian ISPs

Figure 6 shows a timeline including the exact minutes of the withdrawals made by the major Egyptian ISPs, which was published by James Cowie of Renesys [22]. According to Cowie the national ISP, Telecom Egypt (AS8452) started to withdraw its previously announced IPv4 prefixes at 22:12 UTC with Raya Telecom acted similar at 22:13 UTC. Exactly four minutes later, at 22:17 UTC, Link Egypt (AS24863) began to withdraw their prefixes, too. They were followed by Etisalat Misr (AS32992) at 22:19 UTC and Internet Egypt (AS5536) at 22:25 UTC. Converted to Egyptian local time the withdrawals started at midnight. These observed facts lead to the assumption, that all those ISPs received some kind of order from state officials to take down their services. Considering the few minutes between their actions, the order was maybe transmitted in form of a phone call. Few days later Vodafone Egypt confirmed in a press release that their services were shut down on demand of the Egyptian authorities [24].

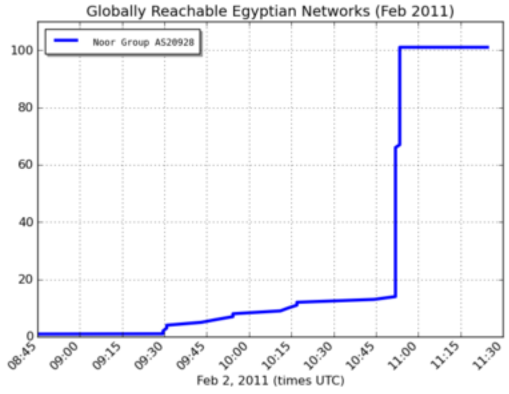

Figure 7: Announced Egyptian IPv4 prefixes as seen from AS20928 on the 2nd of February 2011

The total denial of virtually every Internet communication within Egypt lasted until the 2nd of February. At around 9:30 UTC the first IPv4 prefixes were announced again and a few hours later, at around 11:30 UTC, all Egyptian ISPs returned Internet access to all their customers. Figure 7 was also created by Renesys [23] and visualizes the return of the Egyptian IPv4 prefixes and therefore the end of the massive Internet outage in Egypt.

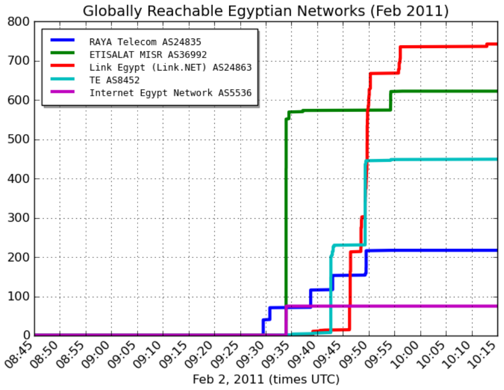

Figure 8: Detailed time-line of announcements made by major Egyptian ISPs

Figure 8 was also created by James Cowie of Renesys [23] and shows the detailed time-line of the readvertisements of routes to their IPv4 prefixes made by the Egyptian ISPs at February 2nd. The fact that all ISPs announced their routes at approximately the same time also indicates a governmental order to end the censorship actions.

3.2 Christchurch earthquake in 2011

In 2011 one of the strongest earthquakes seen in New Zealand hit the city of Christchurch killing 185 people [25]. A magnitude of 6.1 was measured during the quake which was located 10 kilometres south-west of the city of Christchurch [26]. The second largest city of New Zealand was struck by a first quake at 12:51 local time on the 22nd of February 2011 (February 21st 23:51 UTC). A first aftershock was experienced 13 minutes later at 00:04 UTC with a magnitude of 5.8. Thereafter two more aftershocks were observed at 01:50 UTC and 01:51 UTC, both with a magnitude greater than 5. The last shock had a magnitude of 5.0 and was detected at 03:01 UTC, which was 193 minutes after the major earthquake [27].

Those quakes did not only affect buildings and people, but also technical infrastructure like power lines and the water systems were damaged and unusable in some of the suburban parts of the city [29]. Power outages were affirmed in over 80 percent of the city affecting approximately 160,000 people. Within five days the power cuts were repaired and 82 percent of the affected households had power again. Nevertheless some central parts of the city were without power until May 1st [28]. Even with the local electrical companies solving the problem in a rather short timespan, there could still be visible damage in global Internet communication during the earthquake. In the next paragraph of this paper the effect of the earthquake on the announced prefixes of Christchurchs Internet is described in detail.

3.2.1 Geo-location of IPv4 ranges

To determine the effect of the quake on the Internet of Christchurch the first thing that needs to be done is to define the structure and size of Christchurchs Internet. Therefore it is assumed that all IP addresses related to the city of Christchurch by a geo-location database can be seen as the

"Internet of Christchurch". This approach leaves out that these networks are maybe not directly connected with each other within the geographical area of Christchurch, but similar approaches are used in papers by various researchers [1, 3, 2]. To get the data needed to assign IP addresses to geographical locations the GeoLite City Database of MaxMind was used [30]. The comma separated files (CSV) were imported to a SQL-powered database. By querying this database also more complex requests were possible to determine the location of certain IPv4 addresses or even whole IPv4 ranges. Doing this resulted in exactly 320 IPv4 ranges that MaxMind believes to be located in New Zealand's second largest city.

3.2.2 *Allocation of IPv4 ranges to AS*

As those IP ranges are not always announced as a separate range through BGP, but as part of a bigger range, it was necessary to find out which announced IP prefixes those ranges belong to. This was done by calculating the smallest IP address possible laying within an IP range and probing which route a packet destinated to this address would be going. By using routing tables the AS responsible for certain IP ranges can be easily determined. In this paper the publicly available BGP dumps of RIPE NCC were used [31]. By doing this a list with 146 IP ranges has been created. This number means that the 320 ranges found in the geo-location database can be summarised to 146 bigger ranges actually propagated with BGP. Those ranges were announced by 25 different AS with AS4771 (Telecom New Zealand) being the biggest amongst them with 117 announced prefixes. A total of 4 prefixes of the geo-location database were not in use. Figure 9 visualizes the results of this part of the analysis.

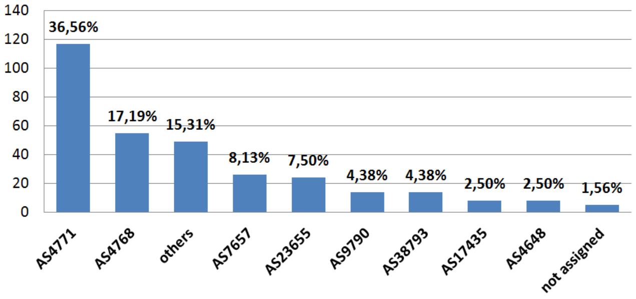

Figure 9: Amount of announced IPv4 prefixes located in Christchurch segmented on base of ASNs

3.2.3 *Analysis of BGP data dumps*

To analyse what actually happened during the earthquake and in the hours later, BGP dumps were necessary. RIPE NCC publishes a complete and uncensored dump of the BGP data received by their routers all around the world [31]. Quite a lot of Christchurch's AS are either directly or indirectly peered with Netgate (AS4648) [32] as is the Telecom New Zealand, as the biggest ISP in Christchurch. Netgate itself is peered with certain members of London Internet exchange point (LINX), like Easynet Global Services (AS4589) and Hurricane Electric (AS6939) [32, 33]. This is why the raw BGP data dumps of a router based within LINX in London was used as source for further analysis [34]. After converting the raw BGP data dumps with `libbgpdump` [35] developed by RIPE, it was possible to perform a detailed search about any announcements or withdrawals made, involving one of the prefixes of Christchurch. A timespan of four hours, from 23:00 UTC on 21st until 04:00 UTC on 22nd of February 2011, was regarded in this analysis.

The results of analysing the BGP dumps showed that the impact of the earthquake on the Internet was quite small. Of all 146 IPv4 prefixes checked there were only three subject to route-changes or withdrawals in the timespan analysed. Figure 10 displays the exact timestamps of the earthquakes according to the Earthquake Commission of New Zealand [36] and the withdrawals as seen at LINX in London.

Due to this it can be assumed that the undersea cables connecting New Zealand with the rest of the world were not badly damaged. The events triggered by such a damage to important core infrastructure could be observed during the massive earthquake in Japan on March 11th of 2011. During the hours after the Japanese quake there were several announcements changing routes to Japanese prefixes observed [1]. Nevertheless, during the first hours after the quake at Christchurch there were no such changes in routing detectable, at least not for IPv4 prefixes based in the city of Christchurch.

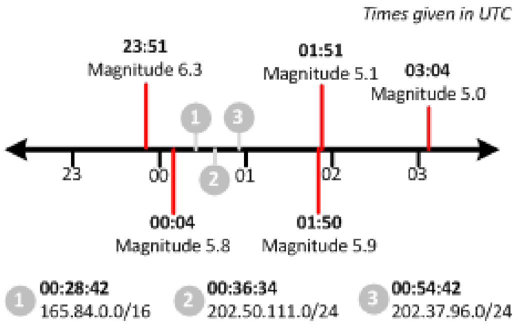

Figure 10: Timeline visualizing the quakes and BGP withdrawals during the earthquake in Christchurch

Christchurch Polytechnic Institute. The first organisation experiencing a total withdrawal of all routes during the earthquake was Christchurch Polytechnic Institute. The Institute is registered with an own ASN, AS45138 [37]. Their IPv4 prefix `165.84.0.0/16` was originally announced by this AS. So no more actions were needed to confirm the property of this IPv4 range. Furthermore, it was the first one affected by withdrawals at 00:28:24 UTC. It seems that there was a serious interruption to New Zealand as seen from Verizon Business (AS701) and Telstra Global (AS4637), which had effects on paths to the mentioned prefix. On 00:30:12 UTC the last path was withdrawn and the Polytechnic Institute of Christchurch vanished from routing tables based at LINX in London. Considering the BGP timeouts which can last up to three minutes, the first withdrawal affecting the prefix was about 20 minutes after the major quake hit Christchurch. Nevertheless major damages on the Polytechnic Institute were reported [38].

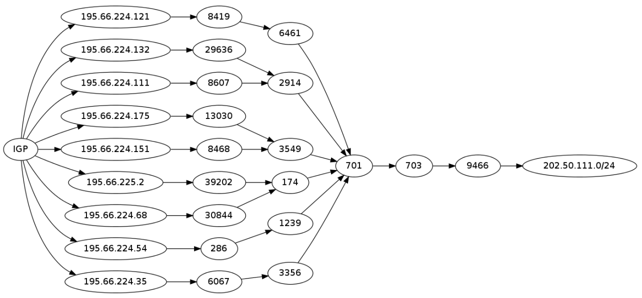

Figure 11: Announced BGP routes to 202.50.111.0/24 as seen from LINX at 16:00 UTC on February the 21st 2011

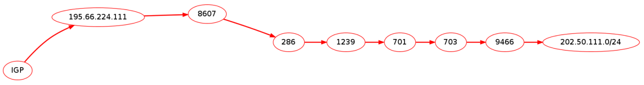

Figure 12: Last withdrawn route to 202.50.111.0/24 as seen from LINX at 00:38 UTC

MYOB Technology Limited. The second IPv4 prefix observed to go down was `202.50.111.0/24` which belongs to MYOB Technology Ltd, an Australian accounting, payroll and web-hosting provider. The data collected from a whois query at `whois.apnic.net` shows that the affected range belongs to their branch in Christchurch. The range was announced by Snap Internet Limited (AS23655) which also announced a total 7 percent of Christchurchs prefixes like figure 9 shows. The first withdrawal was propagated by a router of Catalyst2 Services (AS29636) at 00:36:34 UTC which was approximately half an hour after the second quake. The last route to the prefix was withdrawn on 00:38:21 UTC. The figures 11 and 12 display the routes and their withdrawal.

Tait Communications. Being the third and last IPv4 prefix withdrawn in the analysed timespan, `202.37.96.0/24` belongs to Tait Communications and their branch in Christchurch according to the whois record. Similar to the passage above the prefix was also announced by Snap Internet Limited (AS23655). The first withdrawal was received by KPN Internet Backbone (AS286) at 00:54:42 UTC and therefore about 50 minutes after a quake hit Christchurch. Until 00:57:21 UTC all routes to the prefix were withdrawn.

3.2.4 *Reannouncements and Downtime*

To get more information about the amount of time the mentioned IPv4 prefixes stayed unreachable, more data from the RIPE router at LINX was analysed. Until 19:00 UTC on the 22nd February 2011 there were no new announcements involving those prefixes. Due to this it is clear that these downtimes were not just a plain interruption in connectivity but a serious outage.

4. CONCLUSION

Although analysing BGP data collected by routers all over the world can be used as a measuring method for Internet outages, it is also limited to a rough view of events and their impact on global Internet communications. By using geo-location information events can get tracked down to geographical areas. So even if there were only three IPv4 prefixes down in Christchurch because of the earthquake, the overall traffic of the hosts dropped significantly according to current papers [39]. From this it follows that even if the central infrastructure in Christchurch was still available and worked during the first hours of the quake, a whole bunch of common hosts were offline because of the power outages and their lack of own power supplies.

Only looking at common BGP data dumps cannot determine the whole extent of natural events as big ISPs usually make expensive efforts to save their core infrastructure from failing. Small and medium companies, private households and governmental offices usually do not have such fail-safe strategies for their IT infrastructures and computers. Due to this a core router in the ISPs network may be still alive and communicating through BGP with its neighbours, but there is hardly any traffic to be routed. This very issue can not be measured by BGP. Therefore the analysis of BGP data can only detect global scale outages of whole IP prefixes and because of this BGP analysis can be seen as a macroscopic view of the Internet as a collection of different networks exchanging information with each other.

On the contrary to natural disasters where the core infrastructure can still be alive without its previous hosts and its smaller adjacent networks, total outages due to governmental orders can be detected by using BGP data. Not only Egypt experienced these facts, but also Libya and currently Syria [3]. Tunnelling of different communication streams and using all kinds of creative workarounds [40] make it hard for political organisations to control the information flow and content of communication within the Internet. So the only way to successfully deny information leaking into the Internet or to deny that information from the Internet is visible to people, is to force a total shutdown of the locale core infrastructure needed to communicate with the rest of the world. This is what happened in those three countries mentioned above.

But these most massive methods of censorship can usually be measured in BGP, as withdrawals are the easiest and cheapest way to make sure that whole networks are unable to communicate with the rest of the Internet. If there is no routing to a network no bidirectional communication can be established and therefore even physical connected networks are not usable for Internet-based communication any more. Furthermore by using withdrawals, it is also possible to leave certain networks, which are necessary or important, fully working. In analysis of BGP data those efforts can be seen and measured as recent papers proved [3].

4.1 Future Work

As described in this paper BGP alone can mostly be used as a part of a much more widespread analysis method to get a more detailed view on the impact of events. The first papers working with analysis of different technologies and techniques are published [3, 39]. Methods like measurements of the Internet Background Radiation (IBR) and advanced traceroute techniques can be used to have a really close look at networks and their behaviour in the interconnected Internet. Although these methods do also have their downsides as they can be disturbed by censorship issues on the data layer [39] so BGP will always be one part of a much more sophisticated measure facility using different sources to gather data and determine a detailed in-depth look at events involving Internet outages.

5. REFERENCES

[1] Liu, Yujing and Luo, Xiapu and Chang, Rocky K. C. and Su, Jinshu: *Characterizing inter-domain rerouting after japan earthquake*, In Proceedings of the 11th international IFIP TC 6 conference on Networking - Volume Part II, pages 124-135, Prague, Czech Republic, 2012

[2] Schulman, Aaron and Spring, Neil: *Pingin' in the rain*, In Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference, pages 19-28, Berlin, Germany, 2011

[3] Dainotti, Alberto and Squarcella, Claudio and Aben, Emile and Claffy, Kimberly C. and Chiesa, Marco and Russo, Michele and Pescapé, Antonio: *Analysis of Country-wide Internet Outages Caused by Censorship*, In Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference, pages 1-18, Berlin, Germany, 2011

[4] *YouTube Hijacking: A RIPE NCC RIS case study*, `http://www.ripe.net/internet-coordination/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study`, March 2008

[5] Cowie, James: *Syrian Internet Shutdown*, `http://www.renesys.com/blog/2011/06/syrian-internet-shutdown.shtml`, June 2012

[6] Hawkinson, John and Bates, Tony: *Guidelines for creation, selection, and registration of an Autonomous System*, Internet Request for Comments RFC 1930, Internet Engineering Task Force, March 1996

[7] Vohra, Quaizar and Chen, Enke: *BGP Support for Four-octet AS Number Space*, Internet Request for Comments RFC 4893, Internet Engineering Task Force, May 2007

[8] Rekhter, Yakov and Hares, Sue and Li, Tony: *A Border Gateway Protocol 4*, Internet Request for Comments RFC 4271, Internet Engineering Task Force, January 2006

[9] Levin, Hagay and Schapira, Michael and Zohar, Aviv: *Interdomain routing and games*, In Proceedings of the 40th annual ACM symposium on Theory of computing, pages 57-66, New York, USA, 2008

[10] Baker, Fred: *Requirements for IP Version 4 Routers*, Internet Request for Comments RFC 1812, Internet Engineering Task Force, June 1995

[11] Chen, Enke: *Route Refresh Capability for BGP-4*, Internet Request for Comments RFC 2918, Internet Engineering Task Force, September 2000

[12] Fuller, Vince and Li, Tony: *Classless Inter-domain Routing: The Internet Address Assignment and Aggregation Plan*, Internet Request for Comments RFC 4632, Internet Engineering Task Force, August 2006

[13] British Broadcasting Corporation: *Arab uprising: Country by country*, `http://www.bbc.co.uk/news/world-12482291`, September 2011

[14] British Broadcasting Corporation: *Egypt protests escalate in Cairo, Suez and other cities*, `http://www.bbc.co.uk/news/world-africa-12272836`, January 2011

[15] British Broadcasting Corporation: *Egypt's revolution: Interactive map*, `http://www.bbc.co.uk/news/world-middle-east-12327995`, September 2012

[16] Reuters: *Egypt government denies disrupting websites -cabinet*, `http://www.reuters.com/article/2011/01/26/egypt-web-idUSLDE70P28720110126`, January 26th, 2011

[17] Garret, S.: *"We can confirm that Twitter was blocked in Egypt around 8am PT today."*, `http://twitter.com/#!/twitterglobalpr/status/30063209247408128`, January 25th, 2011

[18] Reuters: *Facebook says has seen drop in traffic from Egypt*, `http://www.reuters.com/article/2011/01/27/facebook-egypt-idUSN2727880720110127`, Janurary 27th, 2011

[19] Ministry of Communication and Internet Technology, Arab Republic of Egypt: *ICT Indicators Report 2007-2011*, `http://www.mcit.gov.eg/Upcont/Documents/Publications_1382012000_Indicator%20E%202012-final2.pdf`, July 2012

[20] Packet Clearing House Research: *Cairo Internet Exchange* `https://prefix.pch.net/applications/ixpdir/detail.php?exchange_point_id=59`, September 2012

[21] Mahlknecht, Greg: *Greg's Cable Map*, `http://www.cablemap.info`, visited on August 17th, 2012

[22] Cowie, James: *Egypt Leaves the Internet*, `http://www.renesys.com/blog/2011/01/egypt-leaves-the-internet.shtml`, January 27th, 2011

[23] Cowie, James: *Egypt Returns to the Internet*, `http://www.renesys.com/blog/2011/02/egypt-returns-to-the-internet.shtml`, February 2nd, 2011

[24] Toonk, Andree: *Egypt falls off the Internet*, `https://bgpmon.net/blog/?p=450`, January 2011

[25] New Zealand Police: *Christchurch Earthquake - List of deceased*, `https://www.police.govt.nz/list-deceased`, February 2012

[26] Reuters: *New Zealand city of Christchurch hit by strong earthquake*, `http://www.reuters.com/article/2011/02/22/newzealand-quake-idUSWLF00502320110222`, February 2011

[27] National Earthquake Information Center of the United States: *Magnitude 6.1 - South Island of New Zealand*, `http://earthquake.usgs.gov/earthquakes/eqinthenews/2011/usb0001igm/`, February 2011

[28] Orion New Zealand Limited: *Orion earthquake response*, `www.oriongroup.co.nz/downloads/Position_statement_210311_1pm.pdf`, March 2011

[29] Stuff.co.nz: *Power restored to most households*, `https://www.stuff.co.nz/national/`

`christchurch-earthquake/4734825/Power-restored-to-most-households`, February 2011

[30] MaxMind: *GeoLite Databases*, `https://www.maxmind.com/app/geolite`, September 2012

[31] RIPE Network Coordination Centre: *RIS Raw Data*, `https://www.ripe.net/data-tools/stats/ris/ris-raw-data`, September 2012

[32] Hurricane Electric Internet Resources: *AS4648 - Netgate IPv4 Peers*, `http://bgp.he.net/AS4648#_peers`, September 2012

[33] RIPE Network Coordination Centre: *RRC01 - LINX, London Peer List*, `http://www.ris.ripe.net/peerlist/rrc01.shtml`, September 2012

[34] RIPE Network Coordination Centre: *rrc01.ripe.net at LINX, London*, `http://data.ris.ripe.net/rrc01/`, September 2012

[35] RIPE Network Coordination Centre: *libBGPdump repository*, `http://bitbucket.org/ripencc/bgpdump/wiki/Home`, September 2012

[36] Earthquake Commission of New Zealand: *New Zealand Earthquake Report*, `http://www.geonet.org.nz/earthquake/quakes/3468575g.html`, February 2011

[37] Hurricane Electric Internet Resources: *AS45138 - Christchurch Polytechnic Institute*, `http://bgp.he.net/AS45138`, September 2012

[38] Tiaki, Kai: *Earthquake 2011: the February 22 earthquake had a devastating impact on Christchurch Polytechnic Institute of Technology's central city campus, forcing more than 600 nursing students and staff to relocate to Lincoln University*, In Nursing New Zealand - Volume 17, page 10, Christchurch, New Zealand, 2011

[39] Dainotti, Alberto and Amman, Roman and Aben, Emile and Claffy, Kimberly: *Extracting Benefit from Harm: Using Malware Pollution to Analyze the Impact of Political and Geophysical Events on the Internet*, In ACM SIGCOMM Computer Communication Review - Volume 42, pages 31-39, New York, USA, 2012

[40] Andersson, Bjorn: *iodine - IP over DNS tunnel*, `http://code.kryo.se/iodine/`, February 2010