Journal of Telecommunications and the Digital Economy

An Analysis of the Optus National Outage

Mark A. Gregory
RMIT University

Abstract: On Wednesday, 8 November 2023 at about 4am, approximately 10 million Optus retail and 400,000 business customers lost network access as a result of the IP Core network shutdown. Optus stated that the cause of the network outage was a routine software upgrade that led to routing information updates from an international peering network causing key routers to disconnect from the network. This paper provides an analysis of the national outage, what information is needed to fully understand what occurred and considers the lessons that might be learned.

Keywords: Telecommunications, Outage, Border Gateway Protocol, Internet Protocol Core Network, Resiliency

Introduction

On Wednesday, 8 November 2023 about 4.05am, Australia's second largest telecommunications company (Optus, 2023a), Optus suffered a nationwide network outage that lasted more than 12 hours (Gregory, 2023a). At 4pm on the same day, Optus declared (Williams, 2023) the network outage had been resolved.

There were three key activities undertaken by Optus as the day unfolded (Optus, 2023a). The first was to identify and rectify the cause of the outage. The second was interacting with the Government and regulatory bodies and the third was customer interaction.

In the days that followed, Optus appeared to be unsure of how much information it should provide publicly (Haskell-Dowland, 2023) and privately to Government and the regulators about what had occurred, what was being done to resolve the problem and how it would compensate customers affected by the outage.

About three hours after the commencement of the national outage, Optus notified the Australian Communications and Media Authority (ACMA) that the network outage was "adversely affecting the carriage of emergency calls over the Optus network" (Optus, 2023a).

http://doi.org/10.18080/jtde.v3n2.X

On 9 November 2023, Optus indicated that it would provide eligible customers with 200GB of additional data as compensation (Optus, 2023c) (Ainsworth, 2023). Media reports indicated that "customers were outraged" with the compensation offered by Optus and News.com.au reported that one customer had "shared a hack" that could be used by some affected customers to exchange the data for a plan charge reduction (Whelan, 2023).

On 13 November 2023, in a media alert (Appendix 1), Optus appeared to indicate that the outage may have been partially due to a third party "international peering network" (Optus, 2023b), which appears to have been the Singtel Internet Exchange (STiX), operated by Singtel, the parent company of Optus.

At a Senate hearing on 17 November 2023, an Optus representative stated "We have applied the necessary protection to ensure that none of our peering partners could create a situation where a repeat of the outage could happen again." (Senate, 2023).

On 16 November 2023, Singtel denied responsibility for the outage (Evans, 2023).

Comparison with Meta Outage

On 4 October 2021, at about 15:40 UTC routing announcements and withdrawals occurring from the Meta network hosting Facebook, Whatsapp and Instagram (Facebook), peaked leading to Meta's Domain Name System (DNS) servers going offline (Martinho, 2021).

CloudFlare (CloudFlare, 2023a) describes the DNS as "the phonebook of the Internet." CloudFlare goes on to provide the description:

> "When users type domain names such as 'google.com' or 'nytimes.com' into web browsers, DNS is responsible for finding the correct IP [Internet Protocol] address for those sites. Browsers then use those addresses to communicate with origin servers or CDN edge servers to access website information. This all happens thanks to DNS servers: machines dedicated to answering DNS queries."

The Facebook Border Gateway Protocol (BGP) updates and announcements for the period 14:00 UTC (01:00 AEDT) to 18:30 UTC (05:30 AEDT) on 4 October 2021 are shown in Figure 1.

http://doi.org/10.18080/jtde.v3n1.X

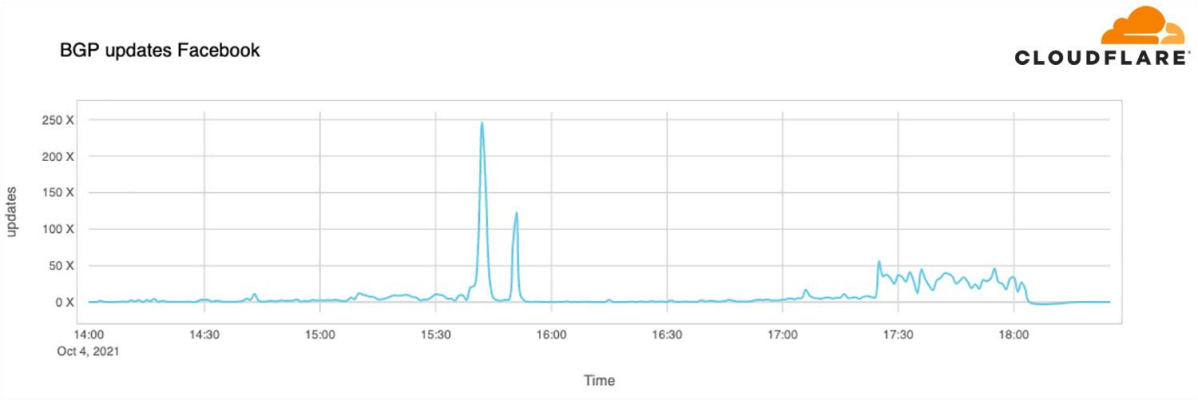

Figure 1. BGP Updates Facebook (Time: UTC) (Martinho, 2021)

At 17:00 UTC (4am AEDT) on 7 November 2023, CloudFlare (CloudFlare, 2023b) reported a significant increase in BGP announcements from the Optus network, as shown in Figure 2, that led to the Optus routers disconnecting from its Core network due to "preset safety levels" (Gregory, 2023a).

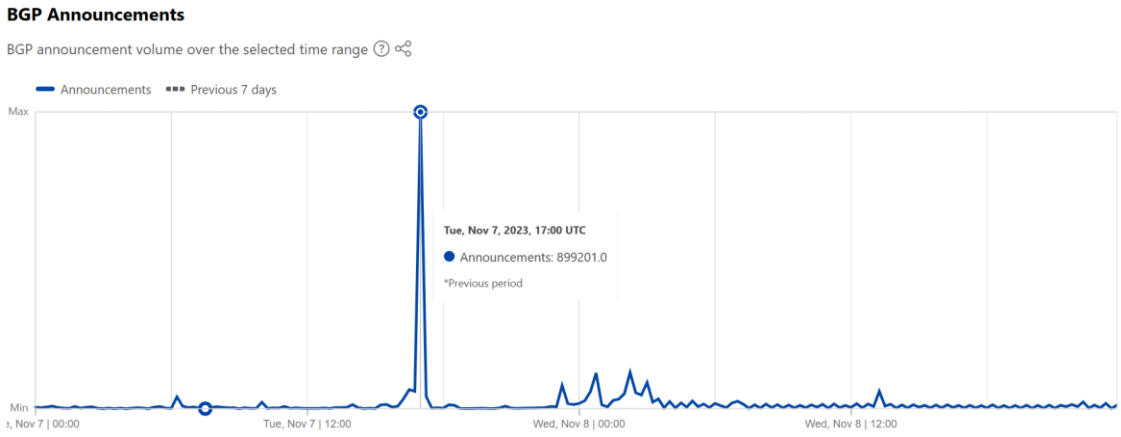

Figure 2. BGP Announcements Optus (Time: UTC) (CloudFlare, 2023b)

Network failures due to BGP are not uncommon, and incorrect BGP configuration will typically affect DNS and routers, followed by gateway and firewall devices.

The explanation provided by CloudFlare (Martinho, 2021) of the Facebook outage provides a starting point for understanding what happened to Optus. A flood of BGP announcements can cause devices (DNS servers, routers, etc.) to disconnect effectively bringing traffic flows to a halt.

Internet Protocol Core Network

It has become clear that the Optus outage was the result of a fault in the "core network" (Haskell-Dowland, 2023) that affected approximately 10 million retail and 400,000 business customers.

http://doi.org/10.18080/jtde.v3n1.X

Journal of Telecommunications and the Digital Economy

The internet is complex, so most carriers, including Optus, use the concept of the "three layer network architecture" (Cisco, 2023) to explain it. This abstraction splits the entire network into layers, as shown in Figure 3.

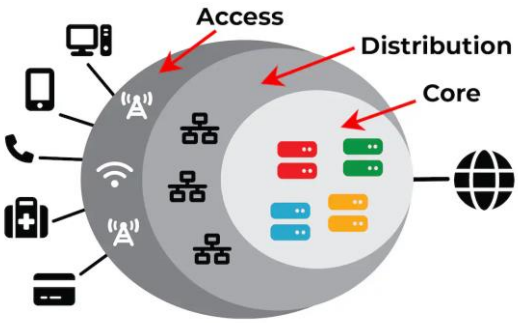

Figure 3. This architecture is just one of many different ways of modeling complex networks. CC BY-SA (Gregory, 2023c)

The access layer

This layer consists of the devices you use to connect to the internet. They include the customer equipment, National Broadband Network firewalls and network termination devices, routers, mobile towers, and the wall sockets you plug into. Figure 4 shows an access network firewall, cable and mobile tower.

Figure 4. The access layer is what people interact with most often. CC BY-SA (Gregory, 2023c)

http://doi.org/10.18080/jtde.v3n1.X

This layer generally isn't interconnected, meaning each device sits at the end of the network. If you want to call a friend, for example, the signal would have to travel deeper into the network before coming back out to your friend's phone.

An outage in the access layer might only affect you and your local neighbourhood.

The distribution layer

This layer interconnects the access layer with the core network (more on that later). Remember that the access layer regions aren't connected to each other directly, so the distribution layer is the interconnecting layer.

Another term for the interconnection cables is "backhaul." Backhaul is to the internet like the main water pipes that travel between suburbs and towns are to a plumbing network.

It is a bit more abstract but generally includes large switches in local exchange buildings, and the cabling that joins them together and to the core network.

Local exchange buildings, similar to that shown in Figure 5, are being turned into network edge (Crozier, 2020) data centres to support distributed Cloud applications and services (Telstra, 2023a).

Figure 5. An exchange building in Bendigo, Victoria. Google maps, CC BY-SA (Gregory, 2023c)

The main purpose of the distribution layer is to route data efficiently between access points. An outage in this layer could affect whole suburbs or geographic regions.

http://doi.org/10.18080/jtde.v3n1.X

The core layer

The core layer is the most abstract. It is the central backbone of the entire network and connects the distribution layers together and connects telecommunication carrier networks with the global network.

While physically similar to the distribution layer, with switches and cables, it is larger and much faster, contains more redundancy and is the location on the carrier's network where device and customer management systems reside. The carrier's operational and business systems are responsible for access, authentication and network security, traffic management, service provision and billing.

Figure 6 shows a typical data centre, including infrastructure that is used to support and host Cloud applications and services.

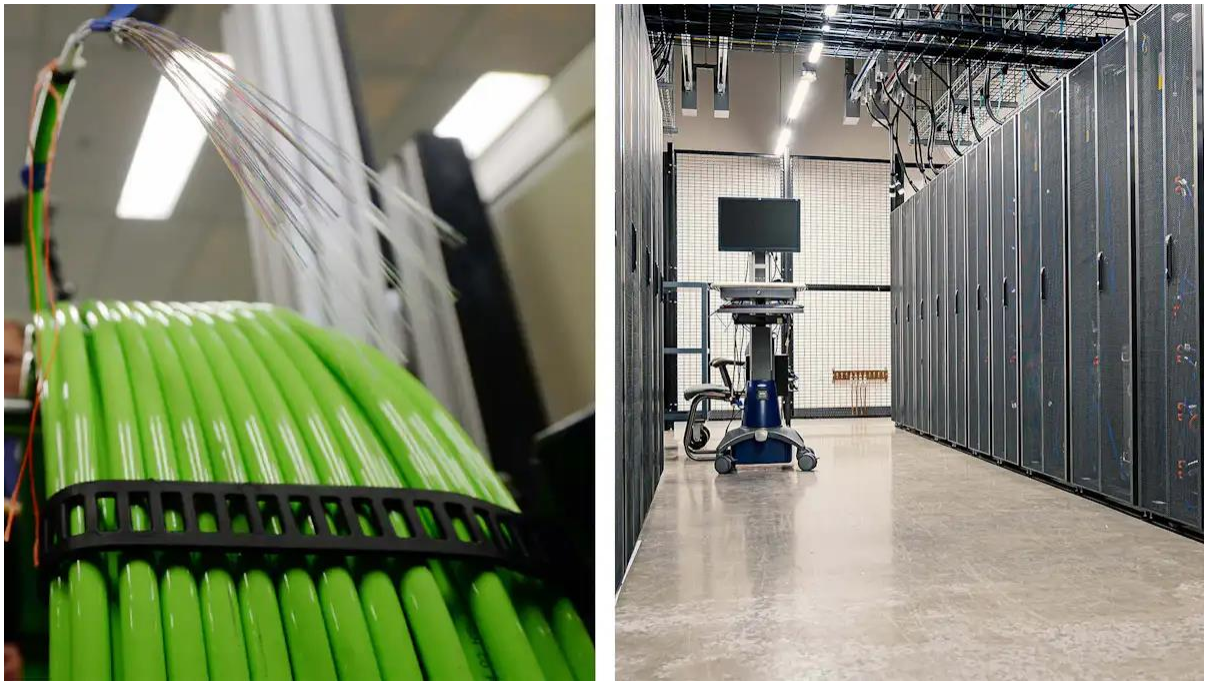

Figure 6. The core layer is abstract but includes fibre optic cables and datacentres. Pexels, Lukas Coch/AAP, CC BY-SA (Gregory, 2023c)

The core layer's primary function is volume and speed. It connects data-centres, servers and the world wide web into the network using large fibre optic cables.

An outage in the core layer affects the entire country, as occurred with the Optus outage.

Why three layers?

A big problem with networking is how to keep everyone connected as the network expands.

http://doi.org/10.18080/jtde.v3n1.X

In a small network it may be possible to link everyone together but as a network grows this would be unwieldy, as shown in Figure 7, so the network is divided into layers based on function.

The three layer model provides a functional description of a typical carrier network. In practice, networks are more complex, but we use the three layer model to assist with the understanding of where equipment and systems are found in the network, e.g., mobile towers are in the access layer.

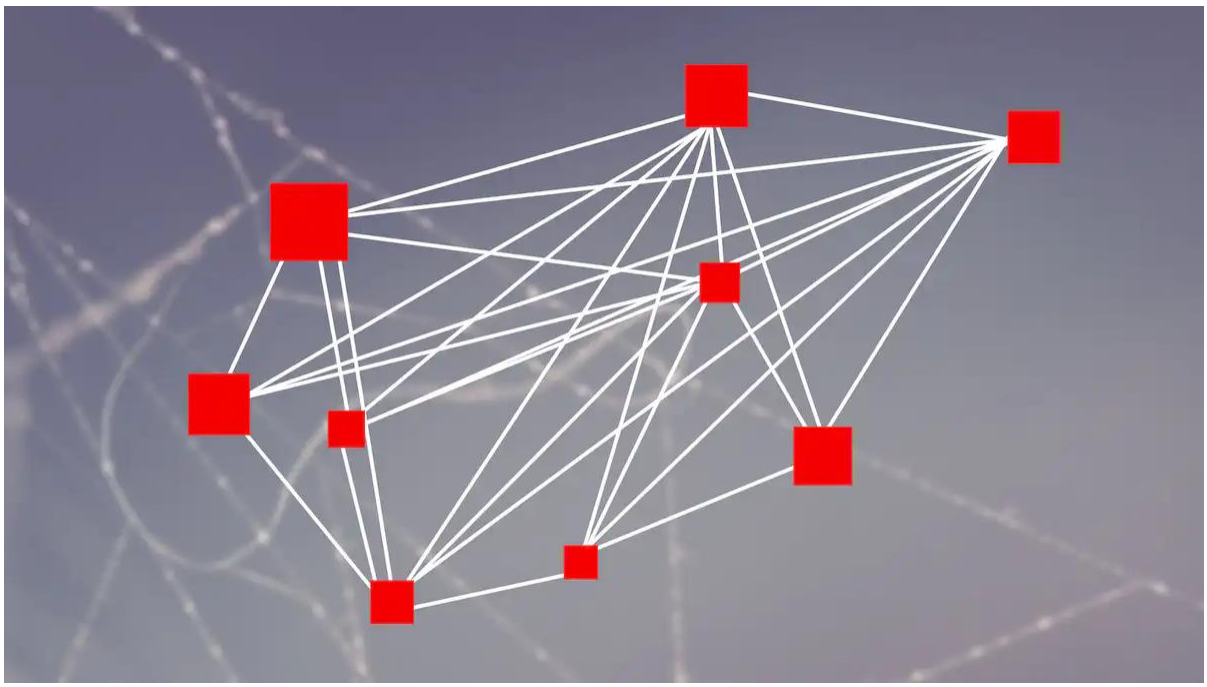

Figure 7. A network of nine people would have 36 connections to link them to each other. The Conversation/Pexels, CC BY-SA (Gregory, 2023c)

The core layer is designed to ensure that access layer traffic coming from and going to the Internet or data-centres is processed and distributed quickly and efficiently, as shown in Figure 8. Today many terabytes of data moves through a typical carrier core network daily.

http://doi.org/10.18080/jtde.v3n1.X

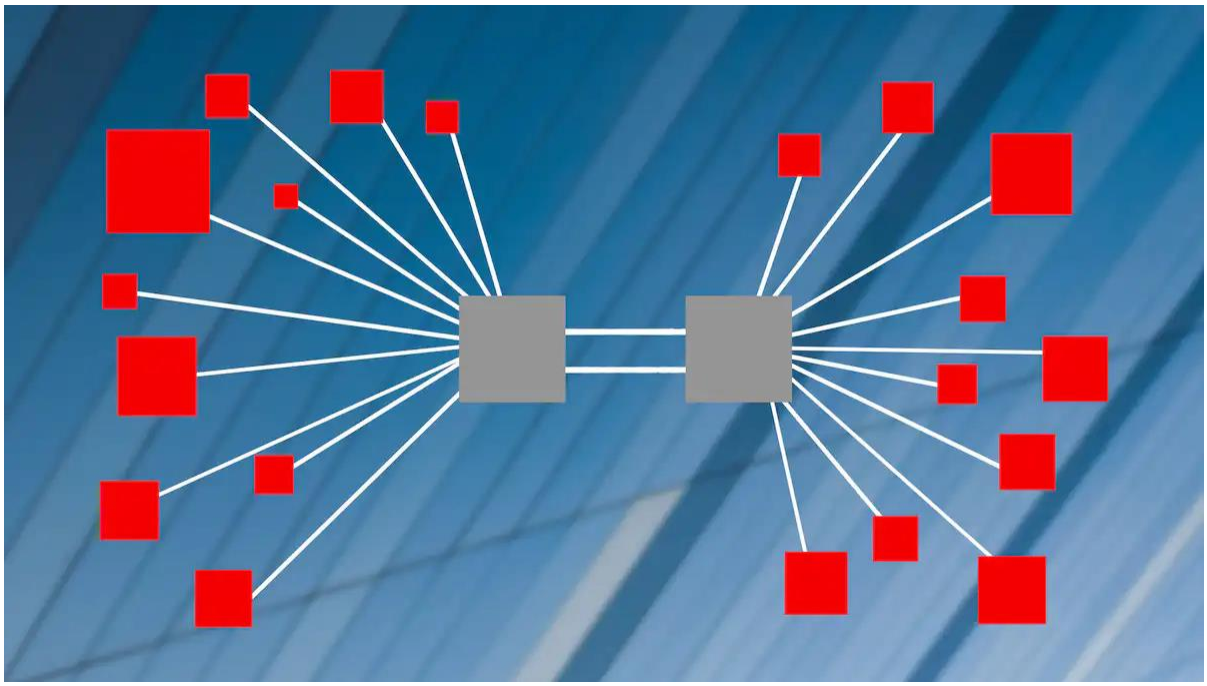

Figure 8. Now a network of 20 people only needs 20 connections to a deeper layer. The Conversation/Pexels, CC BY-SA (Gregory, 2023c)

A failure in the core, caused by routers or DNS servers disconnecting, can affect an entire network.

However, a central premise of the design of the internet from the beginning has been to include multiple paths of core network redundancy to provide alternate routes for traffic to reach its destination if one or more primary routes has failed or becomes congested. When multiple routes of primary and redundancy pathways fail simultaneously, causing widespread outages, questions arise as to whether there may be fundamental flaws in the design of the core network architecture.

Analysis

Information in the public domain about the Optus network outage does not provide a clear understanding of what occurred and why. Questions remain about the network design, redundancy and resilience.

The Optus outage was the result of human error and not infrastructure failure nor a cyber incident. From what we know now, the Optus outage was preventable and has highlighted deficiencies in the Optus network design.

In this section selected aspects of the Optus network outage will be discussed.

http://doi.org/10.18080/jtde.v3n1.X

Critical infrastructure

The impact of the Optus outage was significant. The cost to customers and the nation is anticipated to be approximately $2 billion or more in economic activity.

The most important service to become unavailable was the Triple Zero emergency call service (Bolger, 2023)(Gregory, 2023a). Optus reported that 228 calls to the emergency call service were unable to be connected (Vidler, 2023).

This raises the question of whether Government should deem the IP Core networks of the three national carriers to be 'critical infrastructure'. By doing so the Government would ensure, through legislation, regulations, and cooperative network analysis amongst key industry players, that a similar outage would not happen again.

By deeming the three carrier IP Core networks to be critical infrastructure the Government could require through regulations that there is more transparency, and improved reporting to the regulator, the Australian Communications and Media Authority (ACMA), on network design, management practices, redundancy and resiliency.

Recommendation 1. Government deem carrier networks to be critical infrastructure.

Recommendation 2. Government to introduce legislation and regulations regarding the minimum requirements for redundancy and resiliency of carrier networks.

Network design and implementation

The Optus IP Core network outage appears to indicate that the Optus network is not segmented into service domains and the cascading failure caused when the Core network routers disconnected appears to have caused the entire network to cease operation about 4.05am on Wednesday 8 November 2023.

Optus has not released sufficient technical information for third parties to gain a clear understanding of its Core network architecture, however, it appears to be based on a centralised data centre with supporting edge data centres located around Australia.

We gain an insight into this architecture when Optus indicated that it needed to send technical staff to reset "100 devices in 14 sites across the country" (Williams, 2023).

In the Optus media release sent out on November 13 (Appendix 1), Optus states that it would "work with our international vendors and partners to increase the resilience of our network."

This raises questions:

http://doi.org/10.18080/jtde.v3n1.X

1. Is Optus the design authority over its IP Core network or has the IP Core network architecture, implementation or operation been outsourced to an external equipment and solutions vendor?
2. What percentage of the technical staff supporting the Optus IP Core network are Optus employees?
3. What percentage of the technical staff supporting the Optus IP Core network are contractors or the employees of "international vendors and partners."
4. What percentage of the technical and operational staff supporting the Optus IP Core network have accredited Australian Engineering or Computer Science qualifications and what percentage are on the National Engineering Register. This goes to competence.
5. Whether or not Singtel, the parent company of Optus, has any direct involvement with the architecture or operation of the Optus Core IP network. This goes to potential foreign interference with critical infrastructure and cyber-security.

Recommendation 3. Government to introduce regulations that provide minimum requirements for the control and operation of carrier networks.

Recommendation 4. Government to introduce regulations that provide minimum requirements for the competency of employees responsible for carrier networks.

Recommendation 5. Government to introduce regulations that specify the minimum requirements for carriers to maintain an Australian workforce that is responsible for the architecture, implementation and operation of carrier networks.

Domestic mobile roaming

Temporary domestic mobile roaming during an emergency is currently being investigated by Government (Rowland, 2023). The Government Ministers have tasked the Department of Infrastructure, Transport, Regional Development, Communications and the Arts (DITRDCA) and the National Emergency Management Agency (NEMA) to identify an emergency mobile roaming capability in collaboration with mobile carriers and to report back to Government by March 2024.

This activity comes after the Australian Competition and Consumer Commission (ACCC) completed an eighteen month inquiry into the feasibility of temporary mobile roaming during an emergency. The ACCC concluded that it was "technically feasible" (ACCC, 2023).

The outcome of the ACCC inquiry was unremarkable, as domestic mobile roaming occurs in many countries and across Europe.

http://doi.org/10.18080/jtde.v3n1.X

In Australia, as in other countries, carriers are typically not in favour of domestic mobile roaming as there is a perception that it reduces competition.

In response to the Optus network outage, Telstra again reaffirmed its position that it is against network sharing, even during an emergency (Telstra, 2023b).

Importantly, domestic mobile roaming implemented with the carrier Core IP networks being traversed for device and customer authentication would not be a solution for the Optus network outage. In this scenario, the Optus customer devices would not be able to connect to another carrier's network.

Domestic mobile roaming implemented with a shared replicated authentication system to provide seamless domestic mobile roaming can be implemented despite statements by the carriers that it is unfeasible. Arguments that the cost is prohibitive have not been tested publicly.

Domestic mobile roaming should have been introduced in Australia in 1997. Efforts to achieve this outcome are ongoing. There are many positive reasons for doing so, and no negatives other than the carriers being required to adopt an adjusted business model. In recent years the carriers have sold off large amounts of infrastructure, so the previous arguments about infrastructure being vital to competition are no longer sustainable. Unfortunately, new arguments that are equally unsustainable are now being put forward.

Implementing a shared replicated authentication system would be a secondary solution to ensuring that the carrier IP Core networks have appropriate redundancy and resiliency, however, with the light-touch regulatory environment currently in place in Australia there is no transparency related to this matter.

Recommendation 6. Government launch a public inquiry into the technical implementation and cost for shared replication of device and user authentication

Core IP network redundancy and resilience

The Optus network outage was surprising because Optus appears to indicate that the Core IP network is not segmented into service domains, redundant devices do not exist or were inoperable and separated control networks are not implemented or were inoperable.

If any of these was indeed the case, then this highlights serious flaws in the Optus network design.

http://doi.org/10.18080/jtde.v3n1.X

The requirement to send field technicians to reset routers in location is surprising, as centrally controlled power solutions capable of initiating remote resets have been available for more than 30 years.

It should be anticipated that key network devices, such as DNS servers, routers, gateways and security appliances have their console ports connected to console servers that are connected to a separate protected control network.

It should be anticipated that key routers, DNS servers and other network devices have collocated redundant devices that are running the previous configuration to that running on the operational device. In the event of an outage due to a network software upgrade or misconfiguration it should be possible for an intelligent network to disconnect the misbehaving device from the network and to bring up the redundant device before a catastrophic network outage occurs.

BGP is one of the original Internet protocols and as such there is considerable knowledge about how to implement BGP and to protect BGP appliances from flooding (update and announcements), hijacking, cyber attacks and other problems (Cisco, 2018)(Cisco, 2019).

This raises the question as to the suitability of the Optus IP Core network architecture and implementation. Whilst Optus has stated that it is taking steps to ensure that the outage will not occur again, what can be seen of the Optus IP Core network raises concerns that it is fragile and could be subject to the same or other failures in the future.

Recommendation 7. Government regulate that independent accredited registered engineers carry out annual audits of the carrier IP Core networks and provide reports to the regulator.

In Australia there is a requirement that the financial statements of most major corporations be audited annually, yet there appears to be a reluctance to audit critical infrastructure.

The hands-off approach to regulation, also known as self-regulation, has resulted in more than one catastrophe in Australia in recent memory. This regulatory failure leaves the nation at risk of unwanted and unjustifiable outcomes.

Conclusions

It is reasonable to conclude that the Optus network was not fit for purpose leading to a national outage on 8 November 2023.

A human error should not have brought the entire Optus network down and the length of time taken to rectify the outage was excessive and required manual intervention at sites around the nation.

http://doi.org/10.18080/jtde.v3n1.X

The extent of the problem is not fully understood and there is a need for Government to take action to ensure that similar failures to critical infrastructure do not occur in the future.

Government can improve legislation and regulation of critical infrastructure to ensure there are minimum requirements regarding transparency, redundancy, resiliency, accredited nationally registered employees, competency and network design and implementation practices. There is a need to introduce auditing of critical infrastructure and reporting.

The argument put forward by carriers that solutions are technically unfeasible and costly must be justified and balanced against the cost to customers, the nation and more importantly people imperiled by critical infrastructure failures.

References

ACCC. (2023). Regional mobile infrastructure inquiry 2022-23. Australian Communications and Consumer Commission. Australian Government. 23 October 2023. Accessed online https://www.accc.gov.au/inquiries-and-consultations/regional-mobile-infrastructure-inquiry-2022-23

Ainsworth, K. (2023). Optus offers customers 200GB of free data as compensation for nationwide outage. Australian Broadcasting Corporation. 9 November 2023. Accessed online https://www.abc.net.au/news/2023-11-09/optus-offers-customer-200gb-as-outage-compensation/103087168

Bolger, R. (2023). Optus outage prompts calls to force telcos to switch customers onto other networks when one fails. Australian Broadcasting Corporation. 8 November 2023. Accessed online https://www.abc.net.au/news/2023-11-08/optus-outage-roaming-customers-switch-to-networks-fail/103080582

Cisco. (2018). BGP Fundamentals. Cisco Press. 1 January 2018. Accessed online https://www.ciscopress.com/articles/article.asp?p=2756480&seqNum=5

Cisco. (2019). IP Routing: BGP Configuration Guide, Cisco IOS XE Gibraltar 16.11.x. Cisco. 25 September 2019. Accessed online https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bgp/configuration/xe-16-11/irg-xe-16-11-book.html

Cisco. (2023). Cisco three-layer hierarchical model. Cisco. 17 November 2023. Accessed online https://study-ccna.com/cisco-three-layer-hierarchical-model/

CloudFlare. (2023a). What is a DNS server? CloudFlare. 17 November 2023. Accessed online https://www.cloudflare.com/learning/dns/what-is-a-dns-server/

http://doi.org/10.18080/jtde.v3n1.X

CloudFlare. (2023b). Routing Information from AS4804. CloudFlare. 17 November 2023. Accessed online https://radar.cloudflare.com/routing/as4804?dateStart=2023-11-07&dateEnd=2023-11-08

Crozier, R. (itnews). Telstra's edge compute network to comprise 650 repurposed exchanges. Itnews. 31 November 2020. Accessed online https://www.itnews.com.au/news/telstras-edge-compute-network-to-comprise-650-repurposed-exchanges-555827

Evans, D. (2023). Optus parent company SingTel denies responsibility for outage. *News.com.au. News Corp Australia*. Accessed online https://www.news.com.au/technology/online/optus-parent-company-singtel-denies-responsibility-for-outage/news-story/4f3afcb0155f05c50a3f00e9c1ec4827

Gregory, M.A. (2023a). Optus has revealed the cause of the major outage. Could it happen again? *The Conversation*. 14 November 2023. Accessed online https://theconversation.com/optus-has-revealed-the-cause-of-the-major-outage-could-it-happen-again-217564

Gregory, M.A. (2023b). Explainer: what is the 'core network' that was crucial to the Optus outage? The Conversation. 9 November 2023. Accessed online https://theconversation.com/explainer-what-is-the-core-network-that-was-crucial-to-the-optus-outage-217375

Haskell-Dowland, P., Gregory, M.A., Ahmed, M. (2023). Optus blackout explained: what is a 'deep network' outage and what may have caused it? *The Conversation*. 8 November 2023. Accessed online https://theconversation.com/optus-blackout-explained-what-is-a-deep-network-outage-and-what-may-have-caused-it-217266

Martinho, C., Strikx, T. (2021). Understanding how Facebook disappeared from the Internet. CloudFlare. 5 October 2021. Accessed online https://blog.cloudflare.com/october-2021-facebook-outage/

Optus. (2023a). Submission to Senate Standing Committee on Environment and Communications. *Optus*. November 2023. Accessed online https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Environment_and_Communications/OptusNetworkOutage/Submissions

Optus. (2023b). Media Alert: Update on Optus outage. Optus. 13 November 2023.

Optus. (2023c). We're very sorry for the outage. Optus. 9 November 2023. Accessed online https://www.optus.com.au/notices/outage-response

Rowland. M. (2023). Government to scope emergency mobile roaming capability during natural disasters. Australian Government. 23 October 2023. Accessed online

http://doi.org/10.18080/jtde.v3n1.X

https://minister.infrastructure.gov.au/rowland/media-release/government-scope-emergency-mobile-roaming-capability-during-natural-disasters

Telstra. (2023a). Enhance your performance at the Edge. Telstra Corporation. 17 November 2023. Accessed online https://www.telstra.com.au/business-enterprise/products/cloud/solutions/telstra-edge

Telstra. (2023b). Submission to Senate Inquiry: Optus Network Outage. Telstra Corporation. 17 November 2023. Accessed online https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Environment_and_Communications/OptusNetworkOutage/Submissions

Vidler, A. (2023). Hundreds of triple zero calls failed during Optus outage, CEO reveals while dodging questions over future. Nine.com.au. 17 November 2023. Accessed online https://www.9news.com.au/national/optus-ceo-kelly-bayer-rosmarin-to-face-senate-over-network-crash/d8786be0-7b81-420e-8b2c-3c87bd991670

Whelan, C. (2023). Optus outage compensation: Trick to turn 200GB data into cash. News.com.au. News Corp Australia. 15 November 2023. Accessed online https://www.news.com.au/technology/online/internet/optus-outage-compensation-trick-to-turn-200gb-data-into-cash/news-story/7a810d3972233a5b20cf051a8b8c96fb

Williams, T. (2023). Two weeks since the Optus outage, documents show backroom scrambling and urgent meetings occurred as the emergency played out. *ABC News*. 22 November 2023. Accessed online https://www.abc.net.au/news/2023-11-22/optus-outage-documents-behind-the-scenes-two-weeks-since/103130998

Appendix 1

From: Optus Media Centre <media@optus.com.au>

Sent: Monday, November 13, 2023 1:14 PM

To: Optus Media Centre <media@optus.com.au>

Subject: [EXTERNAL] Media Alert: Update on Optus outage

Good afternoon,

Please find additional details below on the cause of last week's outage:

Optus Media Alert

http://doi.org/10.18080/jtde.v3n1.X

We have been working to understand what caused the outage on Wednesday, and we now know what the cause was and have taken steps to ensure it will not happen again. We apologise sincerely for letting our customers down and the inconvenience it caused.

At around 4.05am Wednesday morning, the Optus network received changes to routing information from an international peering network following a routine software upgrade. These routing information changes propagated through multiple layers in our network and exceeded preset safety levels on key routers which could not handle these. This resulted in those routers disconnecting from the Optus IP Core network to protect themselves.

The restoration required a large-scale effort of the team and in some cases required Optus to reconnect or reboot routers physically, requiring the dispatch of people across a number of sites in Australia. This is why restoration was progressive over the afternoon.

Given the widespread impact of the outage, investigations into the issue took longer than we would have liked as we examined several different paths to restoration. The restoration of the network was at all times our priority and we subsequently established the cause working together with our partners. We have made changes to the network to address this issue so that it cannot occur again.

We are committed to learning from what has occurred and continuing to work with our international vendors and partners to increase the resilience of our network. We will also support and will fully cooperate with the reviews being undertaken by the Government and the Senate.

We continue to invest heavily to improve the resiliency of our network and services.

###

http://doi.org/10.18080/jtde.v3n1.X