Navigating the Rough Waters of Modern Networking Protocols

Micah Thornton, Bobby Santoski, Ryan Sligh
{mathornton, rsantoski, rsligh}@smu.edu

March 18, 2014

Abstract

This paper examines the impact that network protocols and standards have on the average start-up. We discuss three different examples of when protocols might present difficulties in attempting to form a new company. The first of the three focuses specifically on the current IP version update that is taking a toll on current businesses, and anyone who attempts to enter. Secondly, we look at Security protocols and their adaptation in the market place. We examine how these protocols are used to secure corporate secrets, as well as create boundaries to entry for smaller less tech-savvy firms. Lastly we look at expanding a company to multiple regions, or starting up in a region that doesn't conform to modern network protocols, making it difficult to do business. We conclude by stating the inherent trade off between a widely accepted protocol and a good sound protocol; and show that although protocols might not always help a new firm trying to get started, they are 100 % necessary to conduct business.

1 Introduction

The organization of this paper is as follows. There will be a brief introduction where the paper's format, framing, topics, and previous work will be introduced. Next will be a general discussion of different networking protocols and standards with corresponding case studies. The topics to be discussed are network-size increase and the IP address space problem, current efforts

in creating and adapting security protocols, and global networking in regions that don't conform to protocols. We conclude by examining the effects network protocols have on new businesses entering a market.

The focus of our research regards the relative ease or difficulty an entrepreneur faces when deciding to enter a market place saturated with technological protocols. Because of the rapid advancement in networking technologies that mankind made in the past century, protocols have become more and more complex.

Modern networking touches almost every aspect of a successful business; from marketing and advertisement to accepting payment and collecting customer data. Hence it becomes necessary to inspect the costs and benefits of protocols before considering entrance into a market place.

There is much interest in the overall sustainability of certain networking protocols[5]. In our paper we examine the impact of exponential network growth and problems that are posed with IP addressing on an expanding market. There has also been work done on analyzing the development of protocols [13] and relaying older protocols to new uses [8]. New protocols are always under development as well[1].

2 Exponential Address Space Increase

There are both good aspects and bad ones of an increasing network size on the Internet. More devices on the Internet means that your advertisements will reach a larger audience. It also means you will get more business if you are running an on-line shop. But under the hood of the Internet this rapid growth is causing major problems.

The fundamental standard upon which the Internet is based is known as the Internet Protocol, or IP for short. The IP works by assigning a unique address to every device connected to the Internet. The address assigned to a particular device is that device's IP address. The reason that this protocol exists is to make communication between two devices called the client and the host possible.

The IP was first introduced in 1981 by DARPA[11], based on previous work by Vint Cerf and Bob Khan[2]. Back in 1981 it was assumed that an address of 32 bits (1's and 0's) was large enough to assign a unique IP address to all devices connected to the Internet for the foreseeable future. An address of this length can accommodate roughly 2^{32} or about 4 billion

devices. Unfortunately we live in an age when the number of networked devices is beginning to exceed this limit.

In it's original introduction with the 32-bit addresses IP was widely adopted. The form of IP that was adopted at that point in time was known as the Internet Protocol version 4 (or IPv4). Since then a new form of IP has been proposed[3][4] and deployed in some cases. IPv6 has an address field of 128 bits. This corresponds to approximately 3.4×10^{38} addresses. It is estimated that there are about 10^{24} stars in the universe, just to put this in perspective.

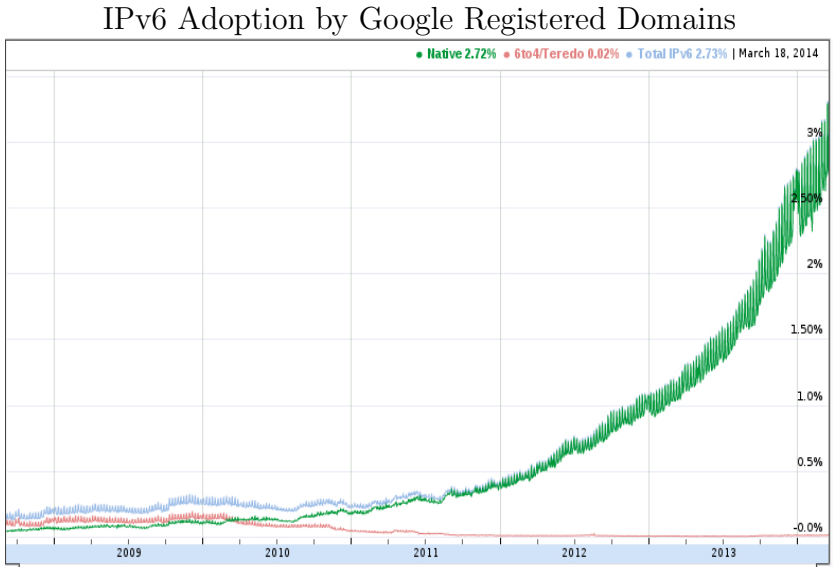

Figure 1: this figure was taken from Google's IPv6 Statistic page[6]

IPv6 has been deployed, but as of March 2014 has only seen a 3.4 % deployment.[6] Google takes statistics on domains that register IPv6 addresses in order to monitor the deployment.

The case study we use to exemplify why this Protocol adoption rate can be a problem for businesses was proposed by Lawerence Hughes in his article[7]. We examine the well known company "Skype". Skype is a company that allows its users to make "phone calls" from their computer to any registered phone number (if they buy "Skype Credits"). Unfortunately for Skype, they rely on the old IPv4 and will have a lot of trouble updating their infrastructure to accommodate IPv6. It is understandable that Skype would rely on this older protocol though. IPv4 is widely distributed, and

allows Skype to take full advantage of the Internet. This business model, of relying on older protocols is unsustainable but more cost effective initially, and makes entrepreneurs much more cautious of the protocol they choose to rely on.

3 Security Protocols

Standards are an important in all parts of networking. They are especially important when it comes to network security protocols. Standards in security have both an upside and a downside. One of the main upsides is that standard protocols allow for virtually any business that is looking to create a product using network features to secure them without doing much research or development on their own. Utilizing a standard security protocol also means that if you are creating a product for the general public your device will be able to interface more easily with those created by other businesses. Standardized protocols also have the benefit of being well tested because they are used in so many places. The fact that they are widely used means that more work goes into making sure they are secure. This benefit also has a flip side that produces one of the major drawbacks from network security protocols being standardized. The ubiquity of these standard security protocols also means that they are widely known to the general public, not just to the businesses using them. This means that the risk of a widely known protocol being broken and the security of systems using that protocol at risk is much higher than a security protocol a company develops on their own. A standard protocol therefore is always at risk of being compromised.

One such set of network security protocols are those for wireless networks. The two main protocols for wireless connectivity are WEP (Wired Equivalent Privacy) and WPA (Wi-Fi Protected Access). WEP was the original wireless security standard when Wi-Fi first gained popularity. Multiple security issues were found with WEP due to the fact that WEP used static shared secrets keys for long periods of time. This left networks vulnerable once the secret keys were decrypted and showed signs that improvements needed to be made to the protocol[12]. WEP2 was introduced as a potential successor to WEP and tried to fix the security problems with the original standard. WEP2 however proved to be deficient as well and it was concluded that the entire WEP algorithm was not sufficient enough to stand up as the standard wireless network security protocol[9]. WPA was then introduced as

the successor to WEP. WPA became the standard wireless networking protocol because it solved many of the cryptographic issues that WEP had. WPA uses a more complex encryption algorithm known as TKIP (Temporal Key Integrity protocol)[9]. WPA also includes a message integrity check, a per-packet mixing function, and a re-keying mechanism that all address specific problems that WEP had. In the case of wireless network security protocol standards we see that a standard was made and widely used, but ran into security issues because it had become so known. As a response to this the standard evolved and was able to improve upon the specific problems that the last iteration of the standard had run into. This shows how that while having a network standard can be hazardous to security it can also help to refine and develop the protocols, as long as the market and businesses are willing to adapt and push the standard forward.

4 Regional Protocol Adaptation

New networking protocols hardly ever gain traction. Businesses are not likely to use a new protocol if its benefits depend on whether both the host and the receiver have implemented the new protocol, especially if the protocol requires new infrastructure. Host Identity Protocol (HIP) suffers from this problem, leading to limited use of the protocol. "HIP secures network data flows of applications, works well with IPv6 and NAT traversal, and allows seamless switching between difference networks, which keeps data streams from being disrupted during the transition" [10].

None of its features are completely new, but it is the only protocol that supports all those features in one package. Even though many businesses may have benefited from the widespread adoption of HIP (especially in mobile communications), HIP was not able to make it past several initial barriers to adoption. Businesses could get similar functionality from using several different protocols that were already in widespread use, and HIP needed both the sender and receiver to support HIP in order for it to actually have any benefits over other protocols.

Though HIP had a more complete feature set that could of potentially benefited businesses more than other protocols, Hip was unable to compete against existing protocols that were more useful because they were more widely adopted, a phenomenon known as the "network effect" [10]. This "network effect" is the reason most new networking protocols fail to gain

traction.

This often is a good thing because switching protocols is a big change, and can cause fragmentation of standards. But there is a downside: if a better protocol is developed, it is often ignored because its capabilities cannot be realized until enough people adopt it. There are however, some ways of deploying a new protocol where the lack of widespread adoption doesnt matter.

HIP is used by Boeing to "secure traffic (and identify machines) with moving robots at their airplane factory" [10]. The features of HIP were able to be utilized in a relatively small setting even though it was not a popular protocol. New protocols can use these very specific implementations like this one to showcases what make makes it valuable without it needing universal conformity.

5 Conclusion

In this paper we examined three specific kinds problems that relate to Network Protocols and the effects that they have on persons wishing to enter the market place. We first examined how the new business owner is faced with an initial trade off in choosing a protocol, in terms of breadth vs. sustainability. We used the example of the increasing address space and Skype to exemplify how a companies future, and initial success is almost completely reliant upon choosing the right protocol to use. We next focused our efforts on the influx of security protocols that have made an appearance in the past twenty years. We examined the evolution of the wifi security protocols WEP and WPA. We concluded that these policies can contribute to an early stage company in several good ways if they are used correctly. For example, a company owner who purchases bandwidth from his local area provider can use these Wi-Fi security protocols in order to protect their asset from theft. However if used incorrectly (I.e. using a bad password) these protocols are almost certainly only going to result in user frustration and lost work-hours. Finally we looked at protocols that aren't widely adapted, and vary in adaption rate largely from region to region. We specifically focus on HIP. We note that the variance in adoption rate among different geographical regions can pose both economic, and technical problems to the early entrepreneur.

In conclusion we would like to note that it would be completely impossible to conduct business of any kind without protocols. We even use protocols

when we speak to one another. There is no avoiding them, the focus of our paper was just on how they might cause difficulties for an early business start up.

References

[1] W.N.A.W. Ali, A.H.M. Taib, N.M. Hussin, R. Budiarto, and J. Othman. Distributed security policy for ipv6 deployment. In *Sustainable Energy Environment (ISESEE), 2011 3rd International Symposium Exhibition in*, pages 120–124, June 2011.

[2] V. Cerf and R.E. Kahn. A protocol for packet network intercommunication. *Communications, IEEE Transactions on*, 22(5):637–648, May 1974.

[3] S. Deering and R. Hinden. Internet Protocol, Version 6 (IPv6) Specification. RFC 1883, Internet Engineering Task Force, December 1995.

[4] S. Deering and R. Hinden. Internet Protocol, Version 6 (IPv6) Specification. RFC 2460, Internet Engineering Task Force, December 1998.

[5] R. Gardner and F. Garcia. Bulk transfer capacity estimation in ipv6 networks. In *Computing in the Global Information Technology, 2006. ICCGI '06. International Multi-Conference on*, pages 6–6, Aug 2006.

[6] Google. Ipv6 statistics. electronic, March 2014. Accessed: 2014-03-20.

[7] Lawrence Hughes. Running ipv6-only. electronic, 2014. Accessed: 2014-03-20.

[8] M. Jung, C. Reinisch, and W. Kastner. Integrating building automation systems and ipv6 in the internet of things. In *Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2012 Sixth International Conference on*, pages 683–688, July 2012.

[9] A.H. Lashkari, M.M.S. Danesh, and B. Samadi. A survey on wireless security protocols (wep, wpa and wpa2/802.11i). In *Computer Science and Information Technology, 2009. ICCSIT 2009. 2nd IEEE International Conference on*, pages 48–52, Aug 2009.

[10] Tapio Levä, Miika Komu, Ari Keränen, and Sakari Luukkainen. Adoption barriers of network layer protocols: The case of host identity protocol. *Comput. Netw.*, 57(10):2218–2232, July 2013.

[11] J. Postel. Internet Protocol. RFC 0791, Internet Engineering Task Force, September 1981.

[12] R. Shukla, S.S. Kolahi, R. Freeth, and A. Kumar. Educational institutes: Wireless network standards, security and future. In *Computer Sciences and Convergence Information Technology (ICCIT), 2010 5th International Conference on*, pages 76–82, Nov 2010.

[13] Jianping Wu, Gang Ren, and Xing Li. Source address validation: Architecture and protocol design. In *Network Protocols, 2007. ICNP 2007. IEEE International Conference on*, pages 276–283, Oct 2007.