

IPv6: Transforming the Way You Network

IPv6 is increasingly becoming the new “hot topic.” Japan has long been seen as a leader in IPv6 research and development, with South Korea and Taiwan moving forward with their own initiatives. Sophisticated IPv6-based research and development networks such as Geant and Abilene have sprung up across Europe and North America. And with the recent announcement by the U.S. Department of Defense that all network and computing equipment purchased after 2003 must be IPv6-capable, there is a sudden surge of interest in that country, previously known for its ambivalence toward IPv6.

Yet even with this growing attention, questions and skepticism still abound throughout the industry. Carriers and ISPs, hesitant to invest in a new technology, await customer demand or a solid business case. Developers wonder whether they should bother making applications IPv6 capable when there is as yet limited commercial connectivity available.

In this article, I will briefly explore some of the reasons why IPv6 is not just desirable, but is in fact necessary for the continuing growth and evolution of the Internet.

IPv4: An Exhausted Resource

There are several attractive features of IPv6, but the only compelling reason for adopting the protocol is the reason it was originally developed: For an increased number of globally unique IP addresses. IPv6 addresses are four times as large as IPv4 addresses, and this translates into an exponentially larger total address space. To put this into perspective, there are approximately 1.3 billion IPv4 globally unique IPv4 addresses still available for allocation. Giving just one globally unique address to each and every person in the People’s Republic of China will deplete all of these remaining IPv4 addresses. In contrast, IPv6 provides enough addresses for every person on the planet to have well over 53 trillion trillion addresses.

The growing scarcity of IPv4 addresses is reflected in the difficulty involved in acquiring new addresses. Enterprises and ISPs alike must provide careful justification when applying for new address blocks. If you are a small business or home user, it is unlikely that you can get a static IPv4 address at all. If you can, you will probably be charged a significant fee for its use. Scarce commodities are expensive.

Cheaper Networks, Cheaper Applications

Network Address Translation (NAT) has long been the solution to IPv4 address depletion, allowing many devices to share a single or a few global IPv4 addresses. NAT has become so accepted as a part of almost all enterprise networks and many home and small office networks, that many question why this solution cannot continue to be used into the foreseeable future.

But NAT introduces hidden costs into your network. Operational expenses are increased by the added complexity of NAT devices and associated address pool management.

Security expenses are increased due to the challenges of making security protocols such as IPSec work properly through NAT. And applications are more expensive because developers must often include “tricks” to make the applications work through NAT. Further, the stateful nature of NAT strictly limits traffic patterns in and out of multihomed networks, and presents an easy target for attackers.

But perhaps the biggest expense introduced by NAT is not in what we presently have, but in what we cannot have due to the limitations of NAT-based networks. Client-server applications tend to work well through NAT, but new kinds of applications are increasingly focused on peer-to-peer (P2P) communications. Without the easy availability of global IP addresses, P2P will continue to present a very limited range of possibilities.

It is often argued that IPv6 needs a “killer application” to spur its acceptance. This logic is a bit inside-out, though. NAT represents a barrier to the introduction of new and innovative applications, and is inhibiting the evolution of networks and the Internet as a whole.

Security? What Security?

Security experts will tell you that the Internet and enterprise networks are dreadfully insecure. The problem lies with our current security model, which is based on a “Maginot Line” mentality. That is, we hide our networks behind firewalls that, once compromised, expose the entire network. What we are in desperate need of is a new security model, one that collapses the security perimeter down to the individual device for true end-to-end security.

IPv6 is not essentially any more secure than IPv4. But two essential components of end-to-end security—authentication and encryption—are integrated components of the protocol, whereas they are “add-ons” in IPv4. Therefore security should be easier and more consistent with IPv6.

More importantly, IPv6 offers us the opportunity to evolve to an end-to-end security model as we migrate our networks to this new protocol.

The Internet is Ready for Meltdown

Routing table “explosion”—the steadily growing size of the Internet routing table—is often cited as one of the major concerns with the Internet today. But, today’s core routers can handle tables several times larger than the present Internet routing table. The larger and more immediate concern is the stability of the routing tables. Whenever a route “flaps,” or changes state, BGP processes throughout the Internet backbone must recalculate. Large numbers of route flaps can destabilize the entire Internet, and this happens on a daily basis.

The primary cause of both uncontrolled routing table growth and routing table instability in the Internet is our poor multihoming practice. When an enterprise or ISP connects to multiple upstream providers, those providers have no choice but to “leak” the long prefix

associated with the multihomed network. That means both that route aggregation does not control the size of the Internet routing table as well as it should, and more importantly, instabilities in these downstream networks are visible throughout the Internet.

There is nothing inherent in IPv6 that changes our current multihoming practice. But, as with security, the very act of transitioning our networks offers the opportunity to improve the way we multihome. Multiple mechanisms have been proposed for multihoming IPv6 that will result in better address aggregation and, in turn, much better stability.

Conclusion

The answer for IPv6 skeptics is an easy one. We can continue to muddle along, making do with scarce and expensive IPv4 addresses, severely inhibited applications, complex and expensive network operations, poor security, and an increasingly unstable Internet. Or, we can begin to transform the way we network and open up an entirely new world of possibilities for how we use—and profit from--those networks.