A Comparison of Public Policy Approaches to the IPv4-IPv6 Transition

Lee Howard. Time Warner Cable

Jesse Horton Sowell, Massachusetts Institute of Technology (MIT) - ESD

Abstract

IPv4 addresses are increasingly unavailable. In most areas, there is a market for addresses, which is or will be increasing the cost of providing Internet service [TCO of CGN], or driving the use of IPv4 address sharing technologies, which have well-documented limitations [rfc7021], such as interfering with peer-to-peer communication. IPv6 provides an alternative, but its adoption has been irregular, varying both by country and among web and consumer access providers. In this paper we survey countries where IPv6 adoption has been strongest, and some where it has been weak, to determine commonalities of policy or practice that have been most effective in promoting deployment of IPv6. We find evidence that government policies help in web deployment, and that IPv6 Internet access is more closely associated with a single company or small group. We also offer evidence that small groups are the most successful at raising deployment among both web and ISP measures.

Introduction

IPv6 has been available as the would-be substitute for IPv4 addresses since the mid-1990s. IPv4 scarcity and depletion of the free pool has increased the cost of ongoing support of IPv4. Continuing support of IPv4 will increase costs of providing Internet service [TCO of CGN], which is likely to be passed on to the consumer, making Internet access less attainable to citizens. IPv6 does require a different set of operational knowledge to deploy than IPv4. As a resource are addresses often considered assets.[1] Whereas IPv4 is becoming scarce and costly, IPv6 is neither scarce, nor are IPv6 address rights as costly to acquire as IPv4. Further, IPv6 has also been shown to be faster than IPv4, typically 10% faster [Huston, Bonus]. Since IPv6 is not as universally deployed as IPv4, IPv6 is not a perfect substitute--there are operational costs to transition. That said, IPv4 is only becoming more costly, despite efforts to encourage IPv6 adoption and ultimately substitution. A cheaper, faster Internet experience is desirable by both consumers and many government actors. This paper considers public, private, and hybrid policy efforts and incentives for navigating the IPv6 transition, and compares the effectiveness of each, to date.

Since the beginning of the commercial Internet, capital investment in equipment and operational development of processes and operational knowledge have all been built on IPv4. These are all sunk costs, and replacing them with IPv6 requires long term strategy development. The bulk of Internet traffic and websites have yet to make the transition. The primary alternative to IPv6 is IPv4 address sharing, whether as Carrier-Grade Network Address Translation (CGN, also called Large-Scale NAT or LSN, or NAT444) or Dual-Stack Lite or NAT64. All of these technologies place multiple users behind a single unique IPv4 address. This ensures ongoing participation in the IPv4 Internet, but introduces a number of limitations [rfc7021]. One limitation is that some applications only work with two native, live IPv4 addresses. Another limitation is poor performance and bottlenecks in NAT configurations. Yet another is the need for ongoing upgrades to NAT equipment to support additional users. Further, CGN complicates law enforcement investigations: most sources of evidence (such as web or mail servers) will provide only the externally facing IPv4 address, which could refer to any of multiple users. These technologies also complicate security. Blocking a single IPv4 address may cause collateral damage for all the actors behind a single address, not just those engaging in abusive activities.

Both consumer welfare and industry's dependence on an efficient and effective Internet infrastructure are compelling public interests for IPv6 adoption. A number of factors argue against CGN deployment and for IPv6 deployment. Internal to the firm, IPv6 deployment may prevent rising long-term costs. For both CGN and IPv6, operational costs will certainly be passed on to consumers. Long term CGN costs will increase with the need for additional CGN

[1] The asset is the (meaningful) bundle of rights delegated by an RIR conferring exclusivity for particular uses of set a of addresses. The most basic meaningful bundle of these particular uses comprises the right to originate routes to a particular set of addresses and the use of those addresses to identify hosts. Number rights and the debate over resource and property rights is a contentious issue in the operator community and in the literature; it is out of the scope of this particular paper.

equipment and will further compound performance loss from address mapping and potential bottlenecks. IPv6 eliminates the need for CGN. IPv6 supports end-to-end connectivity, in particular inbound connections to end users that are often limited by NAT. IPv6 addresses map to a single device rather than being shared among many, simplifying law enforcement investigations. As noted earlier, IPv6 provides a better user experience via lower latency [Huston].

Currently, native dual-stack (running both IPv6 and IPv4 using unique public addresses) provides the best connectivity, but it is a transition configuration. Native dual-stack should not be considered a permanent solution. Due to IPv4 exhaustion, dual-stack cannot be sustained indefinitely. Inconsistent connectivity may be a greater concern than rising connectivity costs, though they may be related if some citizens are able to reach hosts on both internet protocols and others are not. Markets are likely to drive the industry to IPv6 eventually, but, without coordination, the migration will be costly, error-prone (hurried), and may potentially lead to islands of connectivity (in which some hosts have IPv4-only, some have IPv6-only, and they are unable to reach each other).

A coordinated transition would reduce economic loss. The agent of that coordination, and how to effectively incentivize a transnational industry to forego short-term benefits for a long-term investment, have been unclear. Historically, the problem was equipment capabilities. Later, the problem was operational capability: companies have expressed fear of deploying due to lack of IPv6 knowledge [NRO-survey]. Yet another problem is that firms add support for IPv6 based on *local* decisions, without coordination, based on *parochial* decisions that interconnectivity is someone else's problem. Even if operational capability problems are solved through training, firms may not know how long it will take them to deploy IPv6, how to apply operational knowledge tactically and strategically. Firms may not be well informed about when it will be needed for their purposes, i.e. when it will contribute to their value proposition, then rush to deploy when it suddenly seems urgent.

In many cases, deployment takes years. Firms will need to replace equipment, primarily consumer modems and routers. Carrier equipment has generally had IPv6 support for years, with support gradually added to more and more specialized gear as customers have required it. Update provisioning and operational support systems (OSS) will also need to be modified.

Despite these challenges, new and existing institutions in these communities have taken up the task of providing training, highlighting the costs of prolonging IPv4 deployment through CGN technologies, and the tactical and strategic paths that have proven successful for navigating an IPv6 transition. The institutional mix includes public and private institutions acting on their own, and in concert.

To understand the institutional mix, this paper presents case studies of IPv6 deployment. Through the conventional regulatory lens, in terms of case studies, the unit of analysis is the nation state and government policies incenting IPv6 deployment. In the course of interviews,

other institutions came into view. In some cases, such as Singapore, state incentives appear to have constructive outcomes. In others, such as Slovenia, the state played the role of a convener, empowering private actors to share tactical and strategic knowledge on IPv6 deployment. In these cases, private actors may have been mobilized by or included institutions such as ISOC, RIRs, or special purpose IPv6 working groups such as the Go6 Institute in Slovenia. Yet another instance is the firm champion, who may have drawn information from external resources, but acted within a large firm to advocate and drive IPv6 deployment. Narratives from interviews and online documentation support these scenarios.

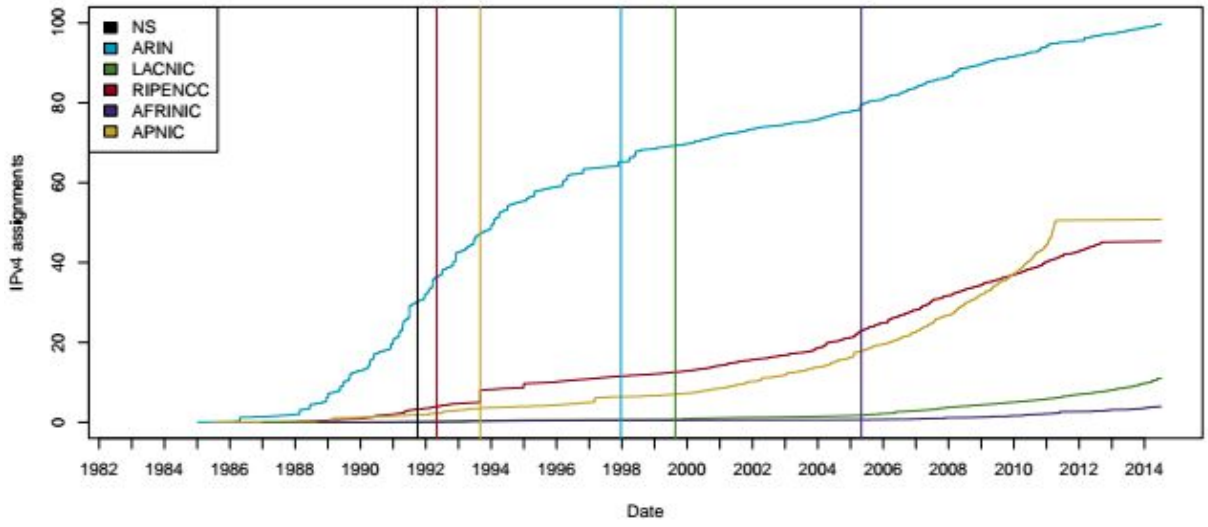
This paper describes who incents IPv6, under what conditions, and to what end. The next section, *Addressing Infrastructure Resources*, presents background information: IPv4 depletion, IPv6 statistics, the notion of an operational epistemic community, and the role of prestige in these communities. This lays the foundation for describing and explaining the case studies. The next section, Survey of IPv6 Deployment Incentives, describes efforts by combinations states and/or operator groups to incent IPv6 deployment. These include instances of the government acting as a convener of experts, case studies of hybrid and private institutions, and finally the role of the charismatic IPv6 champion. This section distills the patterns of IPv6 deployment by various institutions into context-specific hypotheses of IPv6 deployment incentives and strategies. The section entitled Explaining Incentive Structures elaborates the notions of an operational epistemic community to help explain the value of being an IPv6 policy entrepreneur in the community and how these policy entrepreneurs compare with conventional policy entrepreneurs in the state system. Finally, the section called Conclusions and Future work summarizes these strategies and outlines future work drilling into particular cases and data sets.

Background: Addressing Infrastructure Resources

Internet Protocol (IP) addresses are finite number resources. There are 2^{32} unique IPv4 addresses, most of which have been delegated. There are 2^{128} IPv6 addresses, relatively very few of which have been distributed. The following sections provide a brief overview of IPv4 depletion and the current state of IPv6 deployment amongst popular websites around the globe.

IPv4 Runout

Figure 1: IPv4 address allocation *The vertical lines indicate when each registry was created. The black line, labelled NS, represents Network Solutions. Delegations prior to that were managed by Jon Postel in his role as the IANA. Delegations along the blue line between NS and ARIN were delegated by NS; subsequent delegations were conferred by ARIN. For the RIPE NCC and APNIC, each assumed delegation responsibility for the delegations depicted after their respective verticals. The LAC region as managed by NS, then ARIN until the creation of LANIC. After the creation of ARIN, delegations in Africa were split between RIPE NCC (northern half) and ARIN (southern half) until the creation of AFRINIC in 2005.*



In the modern RIR system, IPv4 addresses are delegated to organizations by the RIRs. Addresses are ultimately assigned to end users and servers to facilitate unique identification of Internet hosts necessary for sending and receiving traffic. Early on, IPv4 addresses were delegated by Jon Postel fulfilling the role of the Internet Assigned Numbers Authority (IANA). That role has since evolved into the IANA, as the manager of the global pool, and a set of five regional Internet registries (RIRs) that delegate addresses to networks based in their region. At the outset, the Internet was simply an academic experiment--it was inconceivable that the small, close-knit community using the Internet would ever deplete the pool of 2^{32}, some 4,294,967,296 addresses.

The growth of the Internet in the 1990's and its transition to a global platform, jointly managed by the transnational set of private networks that provision its infrastructure, has led to substantively more demand for addresses as assets necessary for modern business communication and commerce. Figure 1 depicted aggregate historical IPv4 delegation trends.[2] In Figure 1, each line color indicates the aggregate delegations based on the RIR that presently manages those delegations, not the RIR that managed those numbers at the time; see the caption for details.

In the 1990's, other regions were also consuming IPv4 addresses, but not at nearly the rate as the North American region, in particular the US. Growth leveled off as a result of two changes: introduction of a finer-grained addressing scheme (Classless Inter-Domain Routing, CIDR) and change in the organization delegating addresses. Classless Inter-Domain Routing, CIDR, allows for finer grained delegation sizes that create blocks of addresses along power of 2 boundaries. These block sizes were a better fit for actual demand in contrast to the three classful size options (see Footnote 2 for details). On 22 December 1997 ARIN was founded as an independent, non-profit corporation responsible for delegating number resources in the North America and parts of the Caribbean region. ARIN is a member-run registry whose policies are created by the consensus of its members. These two events limited the rate of delegation. That said, demand for IPv4 continued to grow and has now nearly completely depleted the stock.

On 3 February 2011 IANA delegated its last five /8's (units of 2^{24} addresses), one to each of the RIRs. The first two RIRs to run out shifted to runout plans that delegate only one /22 (2^{10} addresses) to those requesting IPv4 addresses as an attempt to ensure (1) large actors do not quickly deplete the remaining IPv4 addresses and (2) new entrants can still get IPv4 addresses, at least enough to get started and ideally to transition to IPv6. This change in policy can be seen in the delegation rate shown in the figure below, a detail of the holistic view above.

[2] Early on, addresses were delegated in three sizes; later, more efficient mechanisms were developed.# A class A delegation comprised 2^{24} addresses, now referred to as a /8. A class B delegation comprised 2^{16} addresses, now referred to as a /16. A class C delegation comprised 2^{8} addresses, now referred to as a /24.

Figure 2: Detail of APNIC and RIPE NCC Fair Runout Transition

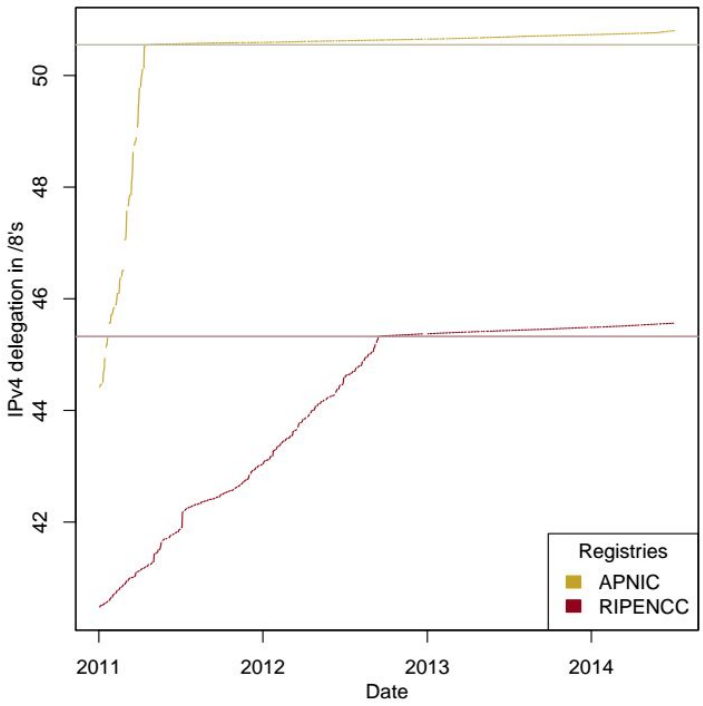


Figure 2 shows the transition from delegation rules based on justified need to a fair runout policy in APNIC and RIPE NCC, allocating only a single /22 per registry member requesting IPv4 space. While this will prolong the life of the IPv4 address space in these regions, once networks acquire their last block, their only options become CGN technologies or acquiring additional number rights on the transfers market.

One of the driving factors in IPv6 deployment is the two sided market for content and consumers. Content providers do not have incentive to transition if no one can get to content hosted on IPv6. Access providers do not have incentives to invest in IPv6 if content is not on IPv6. Further complicating matters, consumer electronics do not universally support IPv6; home gateways in particular have irregular support; some access providers provide equipment and others do not. A number of efforts have been made to incentivize IPv6 deployment by actors that will catalyze network effects in the IPv6 infrastructure market, essentially providing the global IPv6 platform necessary for a two-sided market atop IPv6. Trends in IPv6 deployment by popular websites are discussed in the following section.

IPv6 Deployment in Popular Websites

In the two-sided market framing, two groups have been targeted to catalyze IPv6 deployment: those producing content and those distributing content. This means content producers such as Google and Facebook and the content delivery networks that facilitate distributing that content, such as Akamai, Limelight, and recent startup CloudFlare. Eric Vyncke has been keeping track of popular websites' deployment of IPv6, documenting which of the Alexa top 50 in each nation state is available over IPv6. A summary of this data from early-May 2012 to early-August 2014 is depicted in the figure below.

Figure 3: Proportions of Popular Websites Available via IPv6

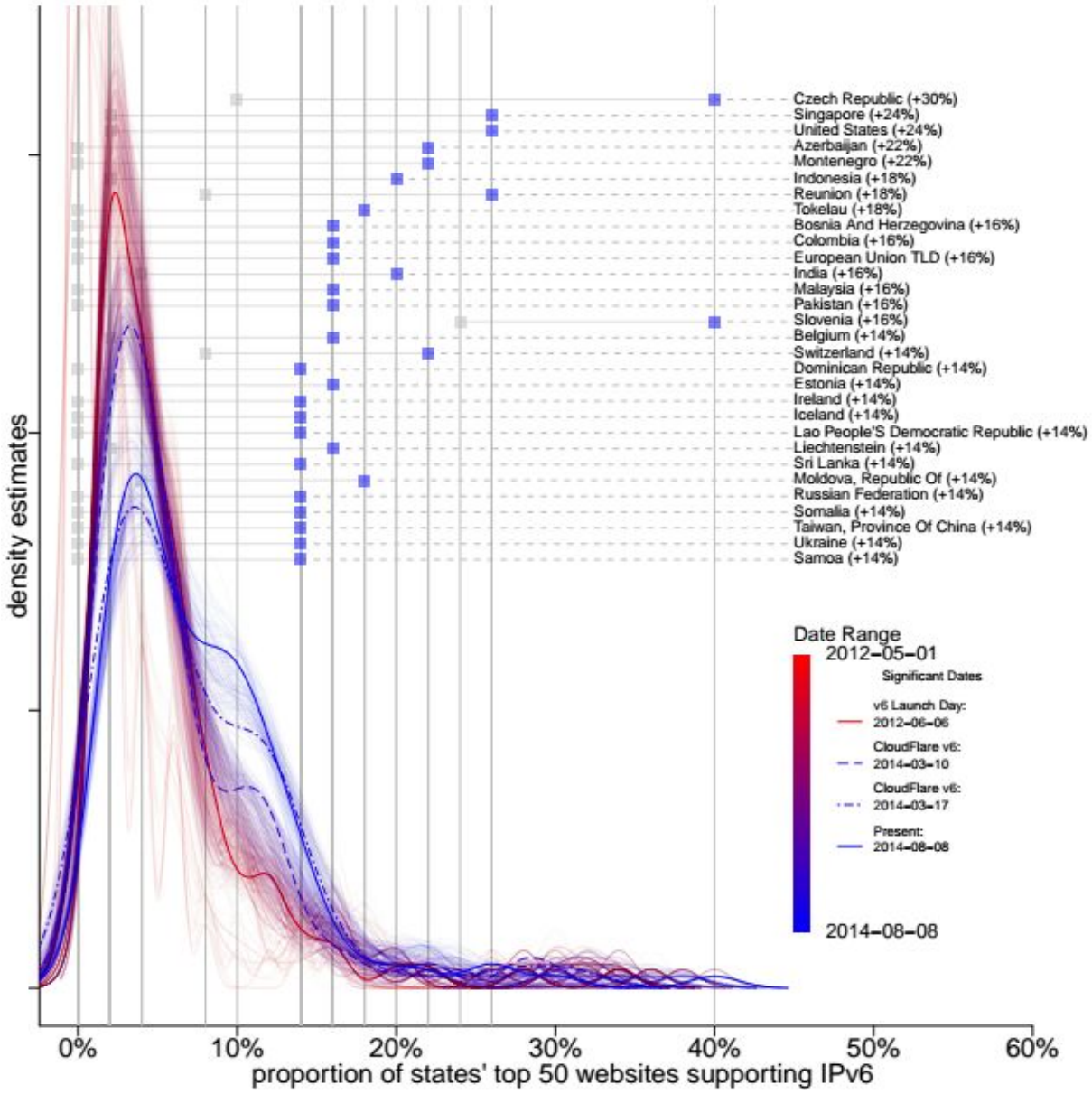


Figure 3 shows the concentration of states for which some proportion of the Alexa top 50 websites for a given country are available over IPv6. The red lines represent mid- to late-2012. Interpreting the graph above, a large concentration of countries fall under the primary peak of the red curves. The x-axis range means that, amongst those concentrated there, approximately 2.5% to 7.5% of the top 50 websites for those countries were IPv6 capable. These density estimates depict over what ranges of *proportion* of IPv6 capable websites countries are concentrated in. The greater the area under the curve for a given range, the more countries in

that range.

The curves in the figure above depict these estimates over time.[3] The color ramp from red to blue is used to depict the shift in concentration over time. In general, there is a shift to the right, indicating the average percentage of popular sites per country available over IPv6 is gradually increasing. That said, density estimates are used to given insights into concentrations in that shift, such as the primary mode and the shoulder that has emerged on the right. Along the primary modes, notice there are coarsely three clusters of lines most distinguishable near the left peaks of the of the density estimates. The red cluster will be referred to as cluster 1, the middle purplish group cluster 2, and the lower, albeit dim, bluish group cluster 3. These appear to represent distinct changes in IPv6 support amongst popular sites.

A number of countries have seen significant growth in the number of sites listed by Alexa for their country that support IPv6. The top thirty with the most significant change are listed in Figure 3. The line beside each country shows the minimum proportion of popular sites that supported IPv6 (the dim grey squares on the left) in this date range and the maximum proportion that supported IPv6 (the blue square) in this date range. The total change is listed in parens to the right of the country name. Note that those with the most growth are not necessarily those with the current greatest proportion of popular sites supporting IPv6. For instance, the Czech Republic jumped 30% to catch up with Slovenia at 40% but the 16% jump for Malaysia moved it far in the rankings, but it is still behind a number of the fast growing states and early movers.

The jumps in the clusters correspond to a few significant IPv6 related incentives and changes. The significant dates in the figure were contributed to by Eric Vyncke at Cisco and Martin Levy at CloudFlare. The first significant date is World IPv6 Launch Day, 6 June 2012, depicted with a solid red curve. The downward shift to the bottom of the red cluster provides some evidence of a shift of concentration to the right as actors turned up IPv6 for IPv6 Launch Day in the weeks beforehand. Another shift corresponds to CloudFlare pushing out IPv6 to its web hosting clients, making IPv6 support the default rather than an option that needs to be activated. The transition occurred between 10 March 2014 and 17 March 2014,[4] signified by the dotted lines in the figure.

Note the dotted lines representing CloudFlare's deployment dates account for a proportion of the shoulder on the right side, but not all of it. The solid blue line shows additional concentration

[3] Note the y-axis has tick marks to illustrate relative distance, but not numbers. The numbers in density estimates have no real meaning aside from providing a check that the area under the curve is approximately 1, i.e., it has the character and interpretation of an analytic probability density function. Following the discussion in the body, the objective is to focus on relative trends in *concentration* via inspection of the area under the curve, not a comparison of the maxima potentially implied by labeling the y-axis with real numbers.

[4] See http://blog.cloudflare.com/i-joined-cloudflare-on-monday-along-with-5-000-others for discussion.

beyond the partial evidence of CloudFlare's contribution.[5] Overall there appears to be a concentration of states around 10% to 14% range, a very visible shift in concentration to the right. Note the current proportion of IPv6 for the top 30 ranked by growth corresponds to this visible right shift. In terms of the catalysts discussed in this work, no single type of incentive can be attributed with this shift. The jump in March corresponding to the CloudFlare deployment may be illustrative of the effects of a single hosting provider and an IPv6 advocate (Levy). Singapore is an instance of effective government policy. Narratives from both Slovenia and Belgium relate instances of private policy entrepreneurs facilitated by regulators lending legitimacy to convene and facilitate IPv6 deployment working groups.

The changing shape of the density estimates further drives home the value of coordinated IPv6 transition. Although a seemingly minor bump now, the distinguished right shoulder above may portend either an intermediate step in a coordinated shift or fragmentation into an potentially increasing bimodal distribution of capabilities in states. Ideally, transition would see a single mode moving from right to left as more websites support IPv6. The ideal outcome is a tight concentration in the high 90% range. The distinguished right shift could portend fragmentation. Rather than "pulling" a tight peak to the right, the emergence of a bimodal distribution would indicate some groups are moving forward while others lag behind. A bimodal or multimodal distribution does not necessarily signal failure, but it will require actors in the IPv6 institutions discussed in the next sections carefully consider which regions or organizations remain concentrated in the leftmost nodes, potentially adjusting their strategies to fit those groups' transition needs, identifying what is necessary to move those actors to the right, and whether those incentives are best leveraged by the state or the private institutions.

Expertise, Capability, and Change

Resource scarcity and demand for IPv6 are key foundations for understanding IPv6 deployment, but deployment also requires an active agent of change. Agents of change may serve as catalysts, conveners of experts, or may be those with the operational capability and knowledge to affect change. The notion of an epistemic community and prestige within those communities helps explain the role of those with operational capability and technical knowledge. As per Haas (p. 3, 1992):

> An epistemic community is a network of professionals with recognized expertise and competence in a particular domain and an authoritative claim to policy-relevant knowledge within that domain or issue-area.

Here, that network of professionals is the community of network operators that deploy and manage layer 2 (IP) infrastructure. Following Sowell's dissertation work, these are referred to

[5] Other views of the data verify the correlation between CloudFlare's deployment time frame and a distinct shift. This *does not* imply CloudFlare is the the sole cause. The authors are digging further into the data set and exploring complementary data to validate the degree of contribution by CloudFlare or whether, albeit unlikely, this is an uncanny coincidence driven by other factors.

as *operational* epistemic communities to distinguish them from the term's frequent reference to scientific communities.[6] The modifier *operational* highlights that knowledge is derived from experience deploying infrastructure and differentiates these communities from protocol design communities such as the IETF and transnational issue-areas catalyzed by the Internet such as those frequently discussed in fora such as ICANN and the IGF. In operational epistemic community writ large and the cases below, recognized expertise and competence is a function of participation in the community, contributions to problem solving efforts at the interstices of shared IP infrastructure, and the willingness to make that knowledge available to others. In this paper, the subset of network actors that have developed IPv6 knowledge in the field will be referred to as the IPv6 (operational epistemic) community.

Historically, much of the effort at managing IP interconnection has gone on "underneath the hood." As Internet communication continues to proliferate as an essential element of global economic and social relations, state regulators have turned their attention to how it is managed and the integrity of that system. A key premise of Haas' work, as a foundation for the explanations of cases of IPv6 development here, is the examination of

> the role that networks of knowledge-based experts---epistemic communities---play in articulating the cause-and-effect relationships of complex problems, helping states identify their interests, framing the issues of collective debate, proposing specific policies, and identifying salient points of negotiation. (p. 2, 1992)

Simply put, epistemic communities can serve as effective state advisors on complex issues such as IPv6 transition. Most notably in the cases below, the IPv6 community has helped elucidate the costs of potential critical paths from IPv4 to IPv6 deployment (a form of cause-and-effect relationship) and they have helped states understand the benefits of deployment (identifying interests). In return, in a number of the cases below, states have lent their legitimacy and credibility as catalysts to IPv6 development in their local economy and legitimizing conveners facilitating the promulgation if IPv6 development knowledge.

Participants in operational epistemic communities should *not be* construed as purely altruistic contributors to a knowledge commons. Knowledge derived from the community contributes to both day-to-day operations of the Internet infrastructure industry and the routing mechanics that bind private networks together into a commonly managed *Inter*net. Within the operational epistemic community, prestige is bestowed on those that make consistent, valuable, and reusable contributions to the knowledge base, frequently referred to as best practices. Prestige is also at play outside the operational epistemic community. Haas (1989) argues that actors contributing to policy and regulatory efforts garner prestige within the policy arena. These participants are a form a policy entrepreneur; in this work, these are IPv6 policy entrepreneurs. Such recognition sends a credible signal to other actors both *outside and within* the operational

[6] This last clause paraphrase's Haas' longer distinction in Footnote 4 of Haas (p. 3, 1992). See Chapter 3 of Sowell's forthcoming dissertation for elaboration of this concept in relation to managing the integrity of commonly provisioned resources in the Internet's layer 2 infrastructure.

epistemic community that these policy entrepreneurs are valuable experts in their domain. Collateral benefits include both political power and benefits for the expert authority of policy entrepreneurs' employers.

In the cases discussed below, in particular coordination between government agents and the IPv6 community, the role of expertise and authority are discussed in terms of the operational epistemic community, its authority derived from expert knowledge, and how that authority is complementary to states public policy objectives. Based on the cases discussed, the mix of government agency and epistemic community capability varies with the context. These concepts are revisited and elaborated in the Section entitled Explaining Incentive Structures.

IPv6 Deployment Incentives

Three institutional configurations for incenting IPv6 have been identified: government public policy efforts; hybrid incentives developed through coordination between government actors and IPv6 policy entrepreneurs; private deployment driven by charismatic IPv6 policy entrepreneurs within the firm. Government public policy efforts are exclusively the product of regulatory and policy incentives intended to exogenously stimulate IPv6 deployment. Hybrid incentives combine government capabilities as a potential legitimizing catalyst and/or convener to facilitate the IPv6 community's efforts at disseminating IPv6 deployment and development knowledge. In these scenarios, IPv6 policy entrepreneurs are often enlisted to engage with and share IPv6 development knowledge with other members of the operational epistemic community and their executive counterparts in the firms that employ them as a means to promote the implications of IPv4 depletion and the need of IPv6 deployment. The final configuration is the charismatic IPv6 policy entrepreneur---this class of actor is a member of the IPv6 community and drives IPv6 deployment endogenously.

Before further elaborating these configuration in the following sections, an interlude with what will be referred to as the simple market solution is warranted. The oft invoked market solution presumes the market will select IPv6 over IPv4 when firms' burden becomes greater than the cost of transition. As alluded to in early discussions, actors may reach this threshold at very different times. There is no doubt that the pressure forcing transition will eventually materialize, but, depending on which actors reach that threshold first, how well prepared for that transition they are (or not), and how effectively they can respond will all contribute to how turbulent the transition may be. Strong proponents of the simple market solution can easily claim this is Schumpeterian creative destruction at work: less fit firms that cannot keep pace, those inadequately prepared for the transition, are winnowed out.

While there are merits to creative destruction, the public is much less tolerant of these turbulent transitions when they affect the quality of industries such as the Internet infrastructure industry and the downstream public, private, and social goods provisioned atop that infrastructure. Moreover, governments and private stewards of these infrastructures face potential audience costs when creative destruction, albeit temporarily, damages both consumer welfare and these institutions constituents' perception of the management abilities. The result is that both governments and private stewards have incentives to smooth the transition---in other words, they have both political and economic incentives to facilitate a more coordinated transition.

Public policy efforts by government is the first class of incentives discussed. Under this model, governments create policy, such as the US mandate for government agencies to support IPv6, to incent IPv6 deployment. Among those in our sample, those efforts correlate to web deployment, but not to consumer access. Hybrid, public-private incentive structures were also observed. These are best characterized in terms of who instigated IPv6 deployment efforts, who played the role of convener, and who sustained those efforts. Finally, the third instance is the charismatic policy entrepreneur inside the firm, driving deployment initiatives. As noted in

the Introduction, none of these are considered universal solutions. Rather, they are contingent on the context, in particular the capabilities, of actors engaged. Contexts, existing resource deployment, and capabilities are discussed in the following sections.

Landscape: Selected IPv6 Public Policy Incentives

The first step to understanding the success of IPv6 deployment efforts was to develop a summary of selected policy initiatives that could be used as a first pass to understanding the IPv6 development landscape. Table 1 provides a 10,000 foot view. As of 20 August 2014, the countries with the most active IPv6 users, and the countries with the most IPv6-capable web sites in their Alexa Top 50, were as listed in Table 1. Note that for top content, we only included countries where 50 sites were surveyed, thus excluding Vanuatu, Central African Republic, and Maldives, as being too small to provide significant insight.This table is based on data collected by Eric Vyncke.

Table 1: Relative Ranking of Countries by IPv6 Users and Web Sites

Country	User Rank	Pct Users IPv6	Content Rank	Pct Web IPv6
United States	5	9.39	4	22
Singapore	11	3.81	5	20
Czech Republic	8	5.69	1	40
Switzerland	2	11.86	7	18
Belgium	1	28.25	32	10
Slovenia	13	3.22	3	26
Germany	3	10.77	20	12
Japan	10	4.52	13	14
Luxembourg	4	10.64	35	10
Brazil	59	0.05	2	28
China	23	0.56	101	2

(data from [Vyncke] using [goog] data as of 20 August 2014)

We observed three kinds of government policies:

1. Requiring IPv6-supporting actions from government agencies;
2. Requiring private industry to support IPv6;

3. Funding some of the effort by private industry to support IPv6. These are classified as government actions because they are edicts from governments to industry--they do not have the character of collaborative hybrid models.

As an example of the first kind of action, some government IPv6 policies relate to what they can directly achieve. For instance, the United States, Brazil, and Belgium have policies requiring government agencies to plan to support IPv6, and for all new purchases to support IPv6. In November 2013, CZ.NIC reported on support within European government agencies (at national, regional, and local levels) [GEN6-RIPE] with the specific intent to report on progress on compliance with Action 89 of the European Union's Digital Agenda for Europe. The report found mixed results but did not look for causes or influences on deployment. The Gen6 project, for "Governments Enabled with IPv6" [GEN6] has made an effort to pilot several approaches to enabling IPv6 for government services, with unclear results. Finally, NIST provides a similar scorecard for U.S. government agencies (http://usgv6-deploymon.antd.nist.gov/cgi-bin/generate-gov), showing about 50% of sites supporting IPv6.

China, Singapore and Belgium have policies implementing the second kind of action, requiring industry to support IPv6. China required certain numbers of consumers to be connected from each of the three largest providers, with very uneven achievement. Singapore does not have any enforcement mechanism in place yet. Belgium only required IPv6 indirectly, by limiting the allowed network address translation.

For the third kind of action, only China and Singapore have funded some of the effort by private industry; China provided some funding for the ISPs, and Singapore supported early web deployment. In several countries, free IPv6 training has been provided; in Singapore, by the government, and in other locations, by the RIR.

A comparison of countries with the greatest web and household deployment provides some evidence that government policy is not necessarily the primary driver of IPv6 adoption.

Table 2: IPv6 Development among Countries with Highest Consumer Adoption

	Policy Type	Small Group	Single Company	ISP%	ISP Rank
Belgium		y		21	1
Switzerland			y	10.8	2
Germany				8.8	3
United States	1	y		8.4	4
Luxembourg			y	8.1	5

Romania			y	5.5	6
France			y	5.1	8
Czech Republic	1			4.1	9
Japan				3.7	10
Slovenia		y		3.9	11
Singapore	1,2,3			3.5	12

Table 3: IPv6 Development among Countries with Highest Web Adoption

	Policy Type	Small Group	Single Company	Web%	Web Rank
Czech Republic	1			38	1
Brazil	1	y		26	2
Slovenia		y		32	3
United States	1	y		22	4
Singapore	1			20	5
Switzerland			y	20	7
Japan				12	10

Careful study of the tables shows:

- The four countries with policies requiring government services to be available over IPv6 (the Czech Republic, Brazil, the U.S., and Singapore) are ranked first, second, fourth, and fifth in the world for web. There is a correlation between government web services requiring IPv6 and top web sites supporting IPv6.
- Countries requiring ISPs to deploy of IPv6 (Singapore, China) are ranked 11th and 23rd in deployment, and notably, China has no web deployment. Direct regulation requiring IPv6 has a negative correlation with ISP deployment. However, the sample is small, regulations are still relatively new, and Belgium indirectly motivated IPv6 of its ISPs (see detail below), and has the highest deployment.
- Countries with the highest deployment among ISPs (Switzerland, Germany, the U.S., Luxembourg, Romania) are those where one large ISP deployed IPv6, with no government coordination. In some cases, this was followed closely by other ISPs. In the U.S., deployment was led by Comcast, followed by AT&T, Time Warner Cable, and Verizon Wireless. Although there was some communication around World IPv6 Launch, it appears that each company had already independently begun deployment, so the

case is essentially similar to others, where a single company deployed.

An examination of the factors leading to IPv6 deployment among the leaders in both web deployment and ISP deployment reveals the essential role of the individual. Among ISPs, a single company generally led deployment, generally championed by a single internal entrepreneur. Among countries where the government convenes private firms, there is generally a policy entrepreneur driving the process. The characteristics and motivations of these entrepreneurs are fundamental to their success.

Trends are observed in the commonalities among countries with highest IPv6 deployment:

- Government public policy efforts that leverage the role of government in leading by example, reducing risk and developing capability
- Government public policy efforts that leverage purchasing power to incent production of IPv6 capable equipment early on;
- Coordination between an IPv6 policy entrepreneur and government (or other legitimating convening entity) promoting IPv6 amongst private firms;
- The role of the charismatic policy entrepreneur internal to the firm who pushes her company to deploy IPv6.

Policy Configurations

The tables above depict gross trends in government policy activities and rough correlation with web and ISP support for IPv6. Following a mixed-methods approach to case study analysis, the following sections describe the the policy configurations observed, highlighting nuance elicited from interviews and case studies. Government policy efforts are presented first. The next section, Government as a Legitimating Convener, describes the role of government serving as a legitimating convener and/or exogeneously catalyzing effort within the IPv6 community. The key distinction in these configurations is the rule of government legitimizing based on public policy interests but, following the general notion of government engagement with epistemic communities, relying on the IPv6 community as the authoritative source of knowledge and operational capacity. The last section discusses private actors as conveners and catalysts. Discussions of RIR efforts highlight their role in promoting IPv6, their efforts at bridging the gaps between C-level executives and engineers regarding IPv6 deployment, and the role of governments as legitimizing agents. The different configurations offered here are not a strict taxonomy. Rather, they are a typology of strategies that are often mixed-and-matched (for instance RIR convener, government catalyst, IPv6 community/industry implements) depending on the particularistic context.

Government Public Policy Efforts

The **United States** has had a formal government transition plan in place since 2007 [OMB]. This plan required U.S. government agencies to meet IPv6 support milestones at various deadlines. This plan has had some success at pushing government agencies [NIST]. Although government policy made no mention of private industry, it was among the earliest organizations to require IPv6 from network equipment manufacturers and web hosting providers. Even where such support was unreliable, it may have made it easier for industry to deploy IPv6, since they could file bug reports rather than feature requests.

The **Czech Republic** issued "Government Resolution #727" in 2009 [Průša], requiring ministries to support IPv6 and to make online services available dual-stack by end of 2010. Government Resolution #7272 met with some success: government web sites have about the same proportion of support for IPv6 as those in the Alexa Top 50.[7] Private industry web deployment started about the same time, with significant deployment by World IPv6 Day in June 2011.

In 2010, the **European Union** published its Digital Agenda for Europe, which included:

> *Action 89: Member States to make eGovernment services fully interoperable*
> Member States should make eGovernment services fully interoperable overcoming organisational, technical or semantic barriers and supporting IPv6.

This action is part of a broader plan for 2011-2015, but such EU plans are essentially advisory to member states.

The **Singapore** Infocomm Development Authority (IDA) has a formal policy is called the "Internet Protocol 'No Islanding' Principle for Internet Access Service Providers," [IDA] requiring residential ISPs ensure that systems, equipment, and networks within their control and operation are capable of allowing access to content on the public Internet, regardless of whether the end-user is on IPv4 or IPv6. IDA's activities in support of this principle have included:

- training more than 300 industry professionals and 6,000 students from the Institute of Higher Learning (iHLs);
- providing financial support for some major websites in Singapore to enable IPv6;
- helping one of the leading local banks to adopt IPv6, demonstrating capability and enabling e-commerce for other sites.

As a result, more than 70% of the Government e-services are IPv6 ready.

---

[7] As of 16 April 2014, https://devpub.labs.nic.cz/ipv6-smt-new/country/cz/ reported 83/250, 33.2%, compared to 36/50 of the Alexa Top 50 per https://www.vyncke.org/ipv6status/detailed.php?country=cz

The government of **Brazil** publishes an interoperability guideline called "e-ping" [http://www.governoeletronico.gov.br/acoes-e-projetos/e-ping-padroes-de-interoperabilidade] . The 2013 version added text:

> Due to exhaustion of public IPv4 addresses, the APF agencies should plan your future migration to IPv6. New contracts and interoperable network upgrades required to implement both IPv4 and IPv6 protocols.

This appears to require IPv6 only for new federal government activities, not for work in place, and does not have a deadline. New contracts with ISPs or telcos for buying IP transit have started to require IPv6. This may have provided some momentum, but appears to be responsive, not leading, to the efforts of NIC.br.

In each of these cases, the government is the actor leveraging the incentive. Incentive structures are largely linked to governments sphere of purchasing and contracting influence, with the exception of Singapore's funding of IPv6 development. As an incentive, this seems to have had positive effects and may have encouraged the development of IPv6 operations capabilities and strategic planning by government contractors. While that is a productive start, a large swath of other network actors fall outside of the scope of this mechanism. Despite these limitations, governments can and do have other means to influence and contribute to IPv6 deployment, in particular as a legitimate convener discussed in the next section.

Government as Legitimating Convener

In many nations, the government, or another agent, has leveraged its position of authority to convene formal or informal groups promoting IPv6 adoption. In many of these scenarios, an IPv6 policy entrepreneur is the catalyst. That said, not all policy entrepreneurs have sufficient influence to act as a convener. In these situations, government is ostensibly the convener, but the *agenda* of the forum is driven by the operational epistemic community.

Consider the the case of **Slovenia.** Jan Zorz identified the need for IPv6 in 2008 and founded the Go6 Institute. Zorz met with the government agency responsible for communications, convincing them to participate in the community of operators. A critical element of this mode of engagement is that Zorz convinced the agency to participate *without* driving an agenda. The government sent invitations to major content companies to participate in an IPv6 Summit. Since the invitations came from government, they were routed to C-level executives, who had to ask their engineers for information and advice about IPv6. C-level executives wished to participate and look informed. Go6 held semi-annual or annual meetings, at which each participant would describe their IPv6 status. Firms with nothing to report lost prestige. To garner prestige, participants would attempt to have something positive to report.

In **Belgium,** a couple of engineers from Cisco, Éric Vyncke and Gunter van der Velde, had concerns about Belgium's IPv6 deployment progress. These IPv6 policy entrepreneurs took it

upon themselves to discuss IPv6 and CGN with cable companies and Belgacom. Vyncke and van der Velde also met with the communications regulator, the economic ministry, and the federal police. They made the argument that CGN was an inferior solution to IPv6, because:

1. Competition is unfair with CGN; new entrants have no IPv4, and must do CGN, which has the documented costs and failings.
2. CGN is a security issue. Many users sharing an address makes law enforcement harder. An investigation into actions from a single IPv4 address atop CGN may point to many individuals, only one or a few of which may be the actual target of the investigation. Further compounding the problem, most sites do not log the source port, which would be the disambiguating identifier.

The regulator, economic authority, and law enforcement conferred with ISPs, and agreed to a limit of 16 users per address behind CGN. This had to be an informal agreement, since their understanding of European law regarding personally identifiable information (PII) is that address sharing is forbidden.[8] The enforcement of the 16:1 agreement is simply that if an organization exceeds that limit, the policy will apply the strict legal interpretation that no address sharing is acceptable.

The 16:1 limit gave C-level executives at ISPs and mobile carriers an incentive to deploy IPv6. The limit highlighted scalability and growth thresholds in CGN. In addition, Vyncke and/or van der Velde would point out each ISP's success to others, bestowing prestige and fostering competition. As a small country, the operational epistemic community at play was a textbook instance of informal norms amongst a close-knit, yet loosely organized set of actors with a common interest in IPv6 development.

Private Actors Catalyzing Deployment

In the **United States,** a couple of engineers determined that no major web site would enable IPv6, out of fear that disruption might drive users to alternate sites, until major sites worked together to share the risk on the same day. They encouraged the Internet Society (ISOC) to coordinate efforts to enable IPv6 among major sites, including Google, Facebook, Yahoo!, Akamai, and Limelight, which became World IPv6 Day in 2011.

The web companies then turned to large ISPs Comcast, AT&T, Verizon Wireless, and Time Warner Cable, who were all already planning IPv6. The ISPs agreed to turn up 1% of their users, as measured by the web companies, for the 2012 World IPv6 Launch. World IPv6 Launch day is highlighted as a significant date in Figure X's description of popular websites supporting IPv6. The red cluster above the solid red line is interpreted as an indicator of World IPv6 Launch day preparation efforts. World IPv6 Launch Day was coordinated by ISOC. Participating engineers gained a certain degree of prestige among their peers.

[8] They seem to be the only ones with this interpretation, and could not cite a document supporting that interpretation. It may derive from the classification of an IP address as Personally Identifiable Information (PII) combined with a requirement to log IP address assignments and a requirement not to maintain PII.

Brazil's NIC.br is the national Internet registry (NIR) for Brazil, as well as being the country's ccTLD operator. As the NIR, they provided free IPv6 training for network operators (they trained about 4,000 professionals between 2009 and 2013), and hosted meetings with the major players (vendors, operators, associations, the telecom regulator, government, and others) to coordinate efforts. NIC.br helped organize Regional IPv6 Week, in February 2012 [http://www.ipv6week.org/] since major web sites had found that they did not have time to offer dual-stack service in time for World IPv6 Day, and that they could not get IPv6 transit from ISPs.

Of the five RIRs, three, APNIC, LACNIC, and AFRINIC, comprise a significant complement of developing states. In addition to these RIRs' core function as a numbers registry, Internet development with its respective region is within the RIR's remit. For instance, consider the mission of the APNIC:[9]

- Function as the RIR for the Asia Pacific, in the service of the community of Members and others
- Provide Internet registry services to the highest possible standards of trust, neutrality, and accuracy
- **Provide information, training, and supporting services to assist the community in building and managing the Internet**
- **Support critical Internet infrastructure to assist in creating and maintaining a robust Internet environment**
- Provide leadership and advocacy in support of its vision and the community
- **Facilitate regional Internet development as needed throughout the APNIC community**

Note the highlighted goals. All of the RIRs provide training on how to use the registry systems those RIRs provision. In contrast, APNIC, LACNIC, and AFRINIC offer additional training on network operations, including IPv6 deployment. This remit is tied to the fourth bullet, "[s]upport[ing] critical Internet infrastructure." Part of this support is a coordinated transition to IPv6. Finally, unpacking the last point, "[f]acilitat[ing] regional Internet development as needed," is manifest in APNIC policies reducing the barriers to participation in RIR fora by the least developed countries (LDCs) in its region. Amongst resources invested in development by these RIRs are training sessions coordinated with NOGs such as LACNOG, Apricot, and AFNOG. Both APNIC and LACNIC have done remote training sessions as well as providing online training courses via interactive web conferencing.

The membership of the RIRs are firms, but *participants* primarily comprise engineers in these firms, the operational epistemic community discussed in the Section Explaining Incentive Structures. This is also the case, if not more so, for the corresponding NOGs. With limited exceptions of CTOs that have climbed the ranks from operations technician to C-level management and, through that experience recognize the value of knowledge developed in

[9] As per https://www.apnic.net/publications/news/2013/apnics-new-vision-and-mission-for-the-future. Emphasis added for discussion in this work.

these fora, RIR and NOG participants are largely engineers. The result is that while these engineers understand IPv4 runout and the operational processes necessary, the tactical and strategic implications of IPv4 depletion and coordinated transition may not be communicated to firm decision makers.

APNIC and LACNIC staff have recognized this disconnect. In both cases staff indicate that participants have engaged in IPv6 training, but in many cases have not be able to gain traction within their parent firm. This is not a reflection on the participants, but rather internal firm politics and organization that may limit access to C-level decision makers. Returning the framing in the Introduction, these different contexts give rise to differentiated strategies.[10] In both regions C-level staff have mobilized to engage C-level decision makers in their member firms. In some cases, these RIRs have been able to engage in bilateral discussions on a member-by-member basis. In other cases, RIRs have coordinated with government agencies and agents of governments, such as the ITU-D in the Asia Pacific (AP) region as conveners. Adding further nuance to the distinctions amongst conveners, in some cases government agencies acted as legitimating conveners. In others, in particular the case of APNIC and the ITU-D, the ITU-D invited APNIC because of its existing, well-developed IPv6 training program and materials. In this latter case, the ITU-D and APNIC leveraged complementary knowledge bases (development and IPv6 operations) to facilitate training in the AP region.

Consider brief discussions of cases in the LACNIC and APNIC regions. In both cases, LACNIC and APNIC have existing, ongoing IPv6 promotion programs in place. As such, in these cases, like the previous section, governments or IGOs may lend political legitimacy, but the RIRs lend technical and operational capability and legitimacy that serves as the operating catalyst for development. Moreover, in contrast to governments as convener in the previous section, the RIRs here already have IPv6 programs, the government is not convening entrepreneurs that then develop additional materials and outreach programs. In this sense, the government and IGO's legitimacy complements existing programs rather than jump-starting them or driving them forward.

In LACNIC, staff related a narrative on IPv6 development in Bolivia. Initially, the meeting was focused on the development of an Internet eXchange (IX). At the time, Bolivia's infrastructure market was fragmented, there were a number of local and regional providers that could benefit from local interconnection. It was also perceived that there was a dearth of IPv6 knowledge in the region. In convening the meeting, LACNIC and the local regulator combined the two, first presenting IPv6, then IX development strategies. Like previous scenarios, while LACNIC staff believed the meeting would go ahead regardless, the regulator acted as a convening agent, leveraging its authority to incent larger ISPs to participate. Ultimately the meeting comprised the regulator as a neutral convener, high ranking engineers and finance staff from ISPs, and

[10] While the discussion of particularistic political and organizational barriers within particular firms is outside of the scope of this work, the outcomes, namely whether RIR and NOG participants have sufficient access and influence is sufficient to differentiate the two scenarios as contexts that inform contingent strategies and hypotheses.

RIR staff. This mix bridges the gap between RIR participants with operational knowledge and decision makers that can influence longer term, strategic decisions. The outcome was considered positive, Bolivia has since begun experimenting with IPv6 deployment. LACNIC staff relate a similar story for Costa Rica. In that case, the convening agent was both the local regulator and a longstanding participant in the local ISOC chapter. The local university was used as the neutral convening location.

In addition to collaboration with the ITU-D as a convener, APNIC has also engaged in a strategy of member-by-member (bilateral) engagement. APNIC staff have identified similar trends amongst their participants as LACNIC: enthusiasm amongst engineers but mixed access to decision makers. APNIC staff have made concerted efforts to bridge the gap by engaging C-level decision makers at member firms. These visits were largely informative: IPv4 depletion is a reality; addresses are a necessary asset into network operations; a variety of options are available, IPv6 being the long term solution; and high-level strategies for deploying IPv6 in the firm. One conversation with APNIC staff related the story of Bangladesh. APNIC staff visited one of the major backbone providers in the country, describing the need for IPv6. The backbone provider consulted with its engineers and found that it was actually quite IPv6 ready and that it would enable IPv6 in its backbone immediately. A couple of weeks later, that provider supported IPv6.

Within the operator community, IPv6 deployment is a “cause celebre,” invoking both impassioned support because “it is good for the Internet” and business case rationales. Some RIR leadership have lamented a surfeit of the former and dearth of the latter. While promotional campaigns are valuable, the message from this subset of the leadership is that ultimately decision makers will respond to arguments regarding how IPv6 will affect the bottom line, not whether lots of engineers have IPv6 stickers on the back of their laptop. Along this line of reasoning, a common theme in both LACNIC and APNIC was a pragmatic focus on IPv6 rather than a largely ideological appeal. For instance, both highlight the costs of CGN technologies. Both also speak to the effect of IPv4 depletion and IPv6 deployment on the firm’s value proposition. In the case of LACNIC, staff indicated that IPv6 (as well as RPKI and DNSSEC) were framed in terms of how they supported existing products and revenue streams. These actors were, in effect, promoting by demonstrating collateral benefits for existing value streams as a mean to offset deployment costs and rationalize long term strategies.[11] In the case of APNIC, members’ experience deploying first in the backbone, then data centers, then finally the costly effort of replacing end-user equipment, was developed into an IPv6 deployment strategy. Both LACNIC and APNIC attempt to assuage fears of large upfront costs by highlighting incremental critical paths that follow existing upgrade cycles rather than introducing new process from whole cloth. Again, this strategy attempts to identify a critical path rooted in

[11] These actors did not claim to have precise cost information for every firm they engaged with. Moreover, arguments were based on community knowledge reported by actors that had deployed IPv6, their experience, and general cost relations. Future work will attempt to contact firms, both those that have successfully deployed IPv6 and those considering deployment to develop a cost model that provides a road map individual firms can parameterize with their specific costs.

collateral benefits that build on existing resource deployments and planned deployments, both defraying costs and reducing interruptions in operations. That said, this requires careful planning by credibly committed decision makers.

Aside from direct government incentives, three of the four IPv6 deployment configurations described here can be explained in terms of incenting industry collaboration and knowledge sharing. The next section provides explanations drawing from the political economy literature. In particular, it offers the notion of an operational epistemic community, and the idea of (IPv6) policy entrepreneurs as concepts that help explain empirically observed incentive structures.

Explaining Incentive Structures

Two frameworks from the political economy literature provide some explanation of these processes: (a) epistemic communities and (b) policy entrepreneurs in conjunction with private resource coordination institutions (RIRs, ISOC, IPv6 Forums, others). Epistemic communities, here refined to operational epistemic communities, describe the communities of actors that have the requisite operational knowledge necessary for a successful IPv6 deployment. Policy entrepreneurs, here IPv6 policy entrepreneurs, are a distinguished subset of the operational epistemic community that has supplemented their technical skills with management skills and strategic engagement with various external actors. Combining these two frameworks provides a useful set of concepts for explaining the motivations of private IPv6 entrepreneurs leveraging a substantive technical knowledge base and strategic engagement within hybrid collaborations and private coordination to promote IPv6 development strategies and deployment.

Operational Epistemic Communities[12] and Prestige

Most literature on epistemic communities refers to communities of academics or professionals such as physicians or lawyers. The essential component of an epistemic community is that it is the steward of a specialized body of knowledge. P.M. Haas (1992) provides definition and characteristics:

> An epistemic community is a network of *professionals with recognized expertise* and competence in a particular domain and an *authoritative claim* to policy-relevant knowledge within this domain or issue area. Although and epistemic community may consist of professionals from a variety of disciplines and backgrounds, they have (1) a shared set of normative and principled beliefs, which provide a value-based rationale for the social action of community members; (2) shared causal beliefs, which are derived from their analysis of practices leading or contributing to a central set of problems in their domain and which then serve as the basis for elucidating the multiple linkages between possible policy actions and desired outcomes; (3) shared notions of validity—that is, intersubjective, internally defined criteria for weighing and validating knowledge in the domain of their expertise; and (4) a common policy enterprise—that is, a set of common practices associated with a set of problems to which their professional competence is directed, presumably out of the conviction that human welfare will be enhanced as a consequence. (1992, p. 3, emphasis added here)

In all epistemic communities, the legitimacy of the authoritative claim and recognized expertise is extensive, specialized training. For the conventional epistemic community, this means formal training and schooling: graduate school for academics, medical school and residency for physicians, law school for legal professionals.

[12] The notion of an epistemic community has been developed by Peter Haas, as referenced in this section. The notion of an *operational* epistemic community, in particular network operators as an operational epistemic community, is based on Sowell's PhD dissertation work combining information sharing strategies of common resource managers and notions of epistemic communities developed by Haas and others.

While many network operators have formal training in computer science and maths, a common complaint in community fora and network operator groups is the lack of formal training in network operations. Much of network operator training is exclusively on-the-job through an apprentice-like structure. In effect, knowledge and legitimate authority is developed within a "close-knit yet loosely organized" community of actors that engage with one another in the regular course of ensuring network connectivity. Repeated engagement and a culture of technical information sharing in the early Internet gave rise to network operator fora such as NANOG (North American Network Operators Group), RIPE (Reseaux Internet Protocol European, the European network operator group), Apricot in Asia, as well as sub-regional and national operator forums such as UKNOF (UK Network Operators Forum) and JANOG (Japan Network Operator Group). These serve as both venues for sharing state-of-the-art in network operations as well as a common location for meetings and negotiations between firms.

A key element of these fora is the education and knowledge building components. NANOG presentations, for example, must be focused on sharing operational knowledge relevant and useful to operators---the presentation may have the logo of the presenter's employer, but it cannot be an advertisement for a product. Program Committee members charged with evaluating presentations often have to re-iterate this characteristic to new presenters. The general ethos is that NANOG presentations are actionable information or adjacent industry topics of interest to the community, in furtherance of effective infrastructure management.

This brief overview illustrates the "shared commitment to the application and production of knowledge" in the network operation domain. That said, legitimacy is not as clear cut as in conventional epistemic communities. Beyond what can be learned in tutorials and weeklong training seminars, the nuts and bolts of network operations is what is referred to in the management and political economy literature as tacit knowledge. Tacit knowledge is derived from experience performing the task. An broadly accessible analogy is that anyone can learn music theory in a semester or two, but it takes years of practice, trial and error, apprenticeship, and engagement with other knowledgeable members of the (jazz) community to become an accomplished jazz musician. As per above, while new operators may have a fantastic grounding in computer science and mathematics, providing the theory of error correction, ethernet protocols, and TCP/IP standards, deep understanding of these technologies behavior modes, failure modes, and varieties of externalities is largely tacit knowledge in the community.

Returning to the characteristics of epistemic communities, there is certainly a shared set of beliefs and values. The informational character of NANOG (and other NOG) presentations is one particular interest. Another recognizes the need for some degree of cooperation between nominal competitors. From an end-to-end perspective Internet infrastructure, both the control plane and the data plane are jointly provisioned resources. The value proposition of every network that relies on Internet connectivity depends on sustaining and maintaining these resources. In the words of one network operator, "if we didn't cooperate to a certain degree, it would be assured mutual destruction." Often, this ethos is abstracted to assertions that part of a

particular communities remit is to “serve the good of the Internet.” This is the network operator’s equivalent of claiming what a conventional governance actor would label the public interest.

Often, NOG presentations and community discussion are problem-focused. One actors sees a problem, solves it, reports their solution to the community in a presentation or on an e-mail list. Well known problems in the community are prefix disaggregation, route flap, prefix hijacking, equipment failure modes, upgrade paths, deployment experience reports, reports on new technologies, interconnection trends and failure modes, and others. Much of this reporting has the style of a case study. This is the mode of exploring a “a central set of problems.” The case study style is an exercise in pragmatism: causal beliefs start and end with empirical evidence reported by credible actors in the community. There is little tolerance for untested or speculative theory. These characteristics of the operator community satisfy the first portion of point (2) in the characteristics of epistemic communities. The second half of (2), linking policy and outcomes, is taken up in the discussion of the distinguished set of policy entrepreneurs emerging from this community.

The pragmatic character of the community also speaks to shared norms of validity. The Internet is a network of networks, there is no single point of objective observation. Absent a formalized knowledge base, community vernacular describing routing phenomena (viz. route flap) has evolved as the base of “internal criteria.” Part of validating criteria is, like other epistemic communities, reproducibility. Taken together with different vantage points, do actors with similar vantage points see the same failure of behavior mode? At what point, at what difference in vantage points, do reports of behavior modes differ? As a close-knit community, actors that consistently make sense of this information, that provide useful and actionable generalizations, garner reputations as valid. While there is no single universally objective observer, there are sufficient actors from sufficiently similar vantage points that incredible reports are often challenged.

The common policy enterprise is where operational epistemic communities have, on the surface, contradictory outcomes. In terms of operational practices and number delegation, i.e. IP address delegation in the RIRs, operators have a well-developed set of common policy norms and formal collective choice processes. The latter, in particular in the RIRs, is rooted in a consensus process similar to that of the IETF. These processes contribute to operational resource policy---they do not necessarily address issues of public interest or those bearing directly on consumer interest, such as IPv6 deployment. In the case of IPv6 resource policy, operational rules deal largely with ensuring resources are delegated in such a way that effective deployment is possible. While some policies attempt to incentivize IPv6 development and deployment, as pragmatic rules intended for application after the decision to deploy, they do not create the full range of incentives for non-operators necessary to deploy. Incenting external actions, linking “policy decisions to outcomes” through “common practices associated with a set of problems” is a relatively new venture. It requires actors credibly committed to an activity generally outside of the network operator’s value proposition.

Studies of epistemic communities have highlighted collateral benefit of participating in external facing roles of the common policy enterprise: community and external prestige. As an illustration, consider Haas' discussion of scientists participation in a program for cleaning up pollution in the Mediterranean (the Med Plan via UNEP):

> The external support from UNEP enhanced the scientists' domestic prestige and strengthened their domestic political base. Although their work was only loosely coordinated by UNEP, the knowledge gained through collaborative efforts established or reinforced their authority in the issue-area of marine pollution control. (Haas, 1989, p. 387)

Generalizing, engagement in both information dissemination within the community and in the common policy enterprise both contribute to an actor's prestige. Recall the balance that presentations are informational, but may retain the company logo. Simply put, this sends the signal that company X employs actors at the cutting edge of industry knowledge. The common policy enterprise has a similar effect: it positions actors and, by proxy, the firms that employee them as credible sources of operational knowledge. Haas provides evidence of this in the context of the Med Plan, illustrated in the quote above. Here, evidence of prestige is depicted in cases of actors with prestige within the operator community working to convene hybrid collaborations between themselves, government agencies, and (C-level) firm leadership. Internal prestige facilitates the development of these relations, creating a productive feedback loop as these actors work to establish "linkages" between the actors shaping "policy actions". The next section refines this distinguished class as the IPv6 policy entrepreneur.

Policy Entrepreneurs

Mattli and Woods use the term "policy entrepreneur" in relation to the public interest:

> Crucially, the entrepreneur involves himself or herself to the best of his or her abilities in the process of change, offering counsel, logistics, financial and technical expertise, or otherwise empowering poorly resourced societal groups adversely affected by the regulatory status quo. The motives of the entrepreneur need not be altruistic; they can be perfectly self-interested. (2009-04-27). The Politics of Global Regulation (Kindle Locations 653-659). Princeton University Press. Kindle Edition.

The notion of a policy entrepreneur used here is consonant with both government policies, and government and non-governmental conveners, such as the epistemic communities. The description above assumes entrepreneurship in the public policy arena. As described in the Introduction, IPv6 deployment is not primarily a public policy issue, but does have implications for public, private, and social goods as downstream products of a well-managed Internet infrastructure. Rather than mobilizing *public* sentiment, IPv6 policy entrepreneurs mobilize actors in a variety of arenas: the operational epistemic community, resource policy, firm strategy, and public policy. As above, the operational epistemic community is the IPv6 policy

entrepreneur's "native habitat." In the resource policy arena, these actors develop supporting policies in the RIR system. Mobilizing broader sentiment in firm strategy and (hybrid) public policy arenas is the challenge at the heart of this work.

Within the latter arenas, operational and resource policy, the "impending crisis" is the confluence of IPv4 depletion and under-provisioning of IPv6 as a substitute. This is a costly scenario for the firm. These costly transitions will have adverse implications for consumers, exposing users to lower quality service and the costs to ultimately transition to IPv6. The objective of the IPv6 policy entrepreneur is to convey these outcomes by leveraging specialized knowledge to describe both constructive outcomes and *tractable critical paths* to those outcomes. As will be discussed in the typology of actors, the ability to describe tractable critical paths is a key difference between the evangelist and the policy entrepreneur. In general, the ideal outcome is to activate and sustain regulatory processes expected to further catalyze IPv6 deployment. Although not completely answered by the cases presented here, hybrid solutions provide hints at what the "key junctures of the regulatory process" may be. Moreover, these may not be key junctures in conventional regulatory processes but rather, as implied by the label hybrid, may be integrated public-private partnerships discussed in Section Y.

In the case of government regulations, these actors have been called upon to comment on the state of IPv6 deployment in fora such as BEREC. In these cases, the IPv6 policy entrepreneur has been invited to offer counsel, input that may be taken back to conventional regulatory arenas. Direct regulation may benefit from counsel, but does not have the character of directly engaging processes of change within firms. Hybrid and private coordination leverage the counsel of IPv6 entrepreneurs, but also convey "logistics, financial and technical expertise" to facilitate develop firm-specific critical paths. In terms of regulatory models of organizations (both firms and governments), the former pushes invokes a model that treats governments and firms as unitary actors whereas the latter invokes a model of governments and firms as collections of agents that can coordinate directly. In the former, governments and firms are black boxes that, supposedly, have their own unified public facing policies and strategies that internal mechanisms hew to.

A more realistic view is to recognize negotiations amongst actors both across boundaries within organizations and between organizations themselves. Policy entrepreneurs in the IPv6 space know how to navigate within the operational and resource policy communities. Cases of hybrid collaboration and private coordination illustrate a learning process as IPv6 policy entrepreneurs learn how to navigate and develop policy arena at the intersection of resource policy and public policy. Transorganizational engagement by specialized actors from each organization results closer coordination amongst actors that are credibly committed to IPv6 deployment.

The last component of Mattli and Woods quote speaks to both credible commitment of IPv6 policy entrepreneurs and the balance of public and private benefits. Recall from the discussion of operational epistemic communities in the previous section that prestige is a motivating factor in participation. The policy entrepreneur is not purely and altruistically driven by "empowering

poorly resourced societal groups adversely affected by the regulatory status quo." This should not be a criteria rooted . The knowledge necessary to effectively play the role of the IPv6 policy entrepreneur as laid out here requires tacit knowledge largely available only through industry experience and apprenticeship. The IPv6 policy entrepreneur derives value from both a regulatory environment that facilitates (or at least does not artificially limit) the development of IPv6 infrastructure and in which they derive prestige from their contributions. Thus, although not purely altruistic, from the IPv6 policy entrepreneurs perspective, downstream benefits are collateral benefits. Similarly, from the public policy perspective, the prestige of effective IPv6 entrepreneurship that positively contributes to the public good is collateral benefits. The key to hybrid collaboration and private coordination efforts is to align these incentives. To understand these, the next section offers a typology of actors and their incentives as the building blocks for explaining supporting cases.

Conclusions

There are a few steps governments concerned about slow adoption of IPv6 can take:

- Meet with technical representatives from industry to communicate concerns about rising costs
- Review data retention laws and their effect on CGN
- Require IPv6 support on all government agency web sites
- Require IPv6 support from all government vendors

Given the examples above, it is clear that so far, the broadest IPv6 deployment to web sites is in countries where there is a government policy requiring IPv6 for government web sites; it also helps to have a small group of companies advancing IPv6. The existence of such a policy has a smaller effect, if any, on deployment of IPv6 to end users. Among countries with a relatively high number of end users running IPv6, there is more likely to be a single large company (less often, a small group of companies), that decided to deploy IPv6 to all of its users.

Countries in or near the top ten in both categories tend to have both a public policy, and a leading operator deploying.

Government policies vary widely, but fall into a few broad categories:

1. Requiring IPv6 for government purchases. These raise visibility, and in early years may have generated a little activity among vendors, but consensus is that they have little effect on private sector deployment (and even public sector deployment is not universal).
2. Encouraging the use of IPv6, but providing no legal requirement or funding.
3. No policy.

Although there is some correlation between the existence of a government IPv6 policy and the level of IPv6 deployment in a country, it does not appear to be causal. In fact, there is some indication of an inverse relation, where the presence of influential experts on IPv6 drive both deployment and the creation of a government policy.

Directives requiring IPv6 of industry have not proven to be the most effective means of encouraging IPv6. Therefore, the most effective way to protect citizens' access to the growing capabilities of the Internet is for governments to encourage industry to act collaboratively and draw on that expertise to develop and incent tractable deployment strategies.

Appendix: Methodology

We review the government policy of the following countries, based on high user counts or high numbers of popular web sites supporting IPv6. Then we consider governments with a stated IPv6 policy position but that do not have a significant deployment of IPv6 as of this writing. Finally, we look for commonalities among successful and unsuccessful policies.

We chose to focus on the number of users capable of IPv6 and the number of top websites, because the web is the largest part of the Internet. Most applications, including e-mail, are usually accessed through web clients. The support from consumer electronics figures into the user count, since users can't access IPv6 web sites without IPv6-capable equipment.

Public measures of IPv6 vary by methodology. Some include the number of IPv6 prefixes announced, but since enabling IPv6 on a backbone network is pretty simple, and often precedes other IPv6 deployment by years, it is not a reliable indicator of readiness. The number of important web sites running IPv6 is an important indicator of how close IPv6 is to being a substitute for IPv6; as it approaches 100%, the web experience becomes indistinguishable for the consumer. The number of consumers capable of using IPv6 is another essential indicator, showing how broad the reach of IPv6 is. The degree of difficulty in enabling IPv6 varies by web site, though many can simply request their content delivery network to enable it, with little to no further work required. By contrast, ISPs must update provisioning and monitoring systems, and must wait for older consumer edge equipment to age out before they will see significant uptake. In addition, retail home routers lag the industry in IPv6 support; consumers do not make buying decisions based on IPv6, so a significant number of home gateways do not support IPv6.

Appendix: Case Studies

We interviewed people with direct knowledge of the IPv6 deployment and policies in each country.

Switzerland does not have a formal IPv6 public policy. One company, Swisscom, independently determined that IPv6 was economically or operationally important. They build their own CPE software, and found the argument for 6rd compelling, so they rolled it out to their users, 30% of whom now use IPv6 [labs.apnic]. The Swiss educational network also has a fair deployment, and there is movement at two other much smaller companies (out of twenty). Éric Vyncke argues that companies in Switzerland and other German-speaking countries are run the the chief engineer Herr Doktor, so engineering considerations are given higher priority than at companies in English-speaking countries where the CTO has a finance background.

The **United States** has had a formal government transition plan in place since 2007.[OMB] This plan provided deadlines for U.S. government agencies to provide various levels of IPv6 support at various deadlines. This plan has had some success at pushing government agencies [NIST]. Although government policy made no mention of private industry, it may be that its requirement encouraged vendor support, which made it easier for industry to deploy. Large ISPs Comcast, AT&T, Verizon Wireless, and Time Warner Cable independently determined that IPv6 was economically or operationally important to them, and rolled it out to their users. These companies worked with major content providers and The Internet Society on World IPv6 Day and World IPv6 Launch.

The **Singapore** Infocomm Development Authority (IDA) is a statutory board of Singapore government which has a formal and active IPv6 program. The formal policy is called the "Internet Protocol "No Islanding" Principle for Internet Access Service Providers," [IDA] requiring residential ISPs to ensure that systems, equipment and networks within their control and operation are capable of allowing access to content on the public Internet, regardless whether the end-user is on IPv4 or IPv6. IDA's activities in support of this principle have included:

- IDA convened the Singapore IPv6 Task Force. [IDAFAQ]
- Business and technical conferences (often partnered with other organizations)
- Training
    - They have a mobile training lab, designed to show that ignoring IPv6 creates vulnerabilities in the enterprise, and showing how to secure IPv6 networks.
    - They have trained more than 300 industry professionals and 6000 students from the Institute of Higher Learning (iHLs). IDA co-funded the training / certification costs from the IPv6 Forum, and sponsors IPv6 training programmes from NICF (National Infocomm Competency Framework). As a result, Singapore more certified IPv6 professionals than any other nation.
- Provided financial support for some majore websites in Singapore to enable IPv6.
- Helped one of the leading local banks to adopt IPv6. This both demonstrated capability,

and enabled e-commerce for other sites.
- More than 70% of the Government e-services are IPv6 ready.

The **Czech Republic** issued "Government Resolution #727" in 2009 [Průša] requiring ministries to support IPv6 and to make online services available dual-stack by end of 2010. Government sites have about the same support for IPv6 as those in the Alexa Top 50.[13] Web deployment is very high due to the efforts of a small group, including Seznam.cz and Centrum.cz, and hosting providers Active24 and Wedos.cz. All of these companies implemented IPv6 for World IPv6 Day, and the hosting providers turned it on automatically for all new customers from then on. With large content having added support already, other engineers may find it less risky. Internet access is progressing, led almost exclusively by Telefonica. However, the Czech access market is highly fragmented, with many small ISPs competing aggressively, so any other individual provider's support will not have a significant effect on deployment.

Romania does not have a public IPv6 policy. One company, RCS/RDS, which is a major ISP there, independently determined that IPv6 was economically or operationally important, and rolled it out to their users.

Luxembourg
Gen6 report shows that many government name servers support IPv6, but no web sites.

In terms of private sector deployment, [labs.apnic] shows the incumbent (Entreprise des Postes et Telecommunications) having 23% IPv6 support, relatively speaking a very high number, followed by Luxembourg Online at more than 9%. This suggests that one person at the incumbent decided to deploy IPv6 (a gradual increase since 2012), and one of the two competitors followed (in January 2014). Luxembourg is another small country, which both means that individuals in the industry are likely to know each other, and that sample sizes are small.

France does not have a formal IPv6 public policy. One company, Free, determined that it could enable IPv6 quickly using 6rd (IPv6 Rapid Deployment), and famously deployed to 10% of the population of France in only six weeks. OVH followed with a significant IPv6 deployment, along with several others in the single digits.

Germany
Governments and universities made IPv6 a requirement, but the real deployment story is from Kabel Deutschland, which determined that it would soon run out of IPv4 addresses based on its

[13] As of 16 April 2014, https://devpub.labs.nic.cz/ipv6-smt-new/country/cz/ reported 83/250, 33.2%, compared to 36/50 of the Alexa Top 50 per https://www.vyncke.org/ipv6status/detailed.php?country=cz

growth. They deployed Dual-stack Lite, a transition technology that tunnels IPv4 (with CGN) over IPv6. Deutsche Telekom has similar

Slovenia has a small, socially connected network of Internet companies. Jan Zorz identified the need for IPv6 in 2008, and founded the Go6 Institute. He met with the government agency responsible for communications, and convinced them to participate. The government sent invitations to major content companies to participate in an IPv6 Summit, which led CEOs (as recipients of the invitations) to ask their engineers for information and advice about IPv6. Go6 held semi-annual or annual meetings, at which each participant would describe their IPv6 status. Because of the need to report, people worked to have something good to report. With about 4% of users running IPv6, ISPs have only recently started deployment.

Brazil
The NIC.br organization is an unusually centralized non-governmental authority for Internet coordinatation in Brazil. It is the national Internet registry (NIR) for Brazil, as well as being the country's ccTLD (operator. As the NIR, they acknowledged the shortage of IPv4 addresses early, and began initiatives, including free IPv6 training for network operators (they trained about 4000 professionals between 2009 and 2013). They also host meetings with the major players (vendors, operators, associations, the local telecom regulator, government, and others) in the Internet market in Brazil, trying to coordinate efforts. They also offer free IPv6 transit in the main IXP.

NIC.br helped organize Regional IPv6 Week, in February 2012 [http://www.ipv6week.org/]. Major web sites found that they did not have time to offer dual-stack service in time for World IPv6 Day, and that they could not get IPv6 transit from ISPs; this event followed eight months later. Some of the participants just left the IPv6 enabled after the IPv6 Week.

The Brazilian government publishes an interoperability guideline called "e-ping" [http://www.governoeletronico.gov.br/acoes-e-projetos/e-ping-padroes-de-interoperabilidade] . The 2013 version added text:

> Due to exhaustion of public IPv4 addresses, the APF agencies should plan your future migration to IPv6. New contracts and interoperable network upgrades required to implement both IPv4 and IPv6 protocols.

This appears to require IPv6 only for new federal government activities, not for work in place, and does not have a deadline. New contracts with ISPs or telcos for buying IP transit have started to require IPv6.

Belgium
In June 2012, after the second World IPv6 event, the Belgian federal government published a circulaire to govt agencies, advising them they need to require IPv6 in their tenders. [http://economie.fgov.be/fr/binaries/Plan_national_pour_implementation_IPV6_Belgique_tcm32

6-208123.pdf] The plan did not include detailed requirements, and included no budget or enforcement.

A couple of engineers from Cisco, Éric Vyncke and Gunter van der Velde, had concerns about Belgium's IPv6 deployment progress, and talked with the cable companies and Belgacom about IPv6 and CGN. They also met with the communications regulator, the economic ministry, and the federal police, and made the argument that CGN was an inferior solution to IPv6, because:

3. Competition is unfair with CGN; new entrants have no IPv4, and must do CGN, which has the documented costs and failings.
4. CGN is a security issue. They explain to the federal police how many users sharing an address makes law enforcement harder, since an investigation into actions from an IPv4 address may point to many individuals (and most sites don't log the source port, which would be the disambiguating identifier).

Went to the providers and did education, IPv6 isn't that complex. Then among those constituencies, the regulator, police, economy, ISP association, they agreed to a limit of 16 users per address behind CGN. This had to be an informal agreement, since their understanding of European law regarding personally identifiable information (PII) is that address sharing is forbidden.[14] The enforcement of the 16:1 agreement is simply that if an organization exceeds that limit, the policy will apply the strict legal interpretation that no address sharing is acceptable.

The 16:1 limit gave ISPs and mobile carriers an incentive to deploy IPv6, since they could see the limit on scalability and growth in CGN, and compare to their expected IPv4 address market prices. In addition, an element of competitive pride existed: when one ISP did something, Vyncke or van der Velde would point it out to others, who would want to catch up. As a small country, everyone knows each other, which makes such competitions personal.

Belgium does not have the same level of success with content providers, which Vyncke says is due to the fact that he doesn't know the content providers.

Malaysia

In March 2005, the Malaysian government recognized the NGN group as a pioneer in the area of IPv6 expertise in the country by awarding the NGN group the *"National Advanced IPv6 Centre of Excellence" (NAv6)* status. [http://www.nav6.org/About%20Us/visionmission.php] NAv6 has an org chart featuring at least 17 people, and Malaysia's research network has shown good progress [labs.apnic], along with three other networks. The incumbent has enormous market share, and has a moderate 3% deployment, all achieved since October 2013. Only five of the top 50 web sites have IPv6.

[14] They seem to be the only ones with this interpretation, and we could not find a document supporting that interpretation. It may derive from the classification of an IP address as Personally Identifiable Information (PII) combined with a requirement to log IP address assignments and a requirement not to maintain PII.

China has a formal IPv6 public policy. The Chinese government has provided financial support for the three largest Internet providers, China Telecom, China Mobile, and China Unicom, to facilitate their IPv6 migration. The government set a specific goal for each of those companies to enable IPv6 to 3 million users by the end of 2013 (9 million total). It is difficult to verify from outside China how effectively these goals are being met; [goog] shows China oscillating wildly between 0.05% and over 1% within weeks.

Works Cited

[Bonus] “Performance Bonus of IPv6” panel at NANOG, convened by Lee Howard, February 2014.
https://www.nanog.org/sites/default/files/11-feb-2014.webcast.howard.ipv6-performance-bonus.mp4

[FB]http://www.internetsociety.org/deploy360/wp-content/uploads/2014/04/WorldIPv6Congress-IPv6_LH-v2.pdf

[GEN6] http://www.gen6.eu/docs/deliverables/GEN6_PU_D6_1_v1_3.pdf and https://devpub.labs.nic.cz/ipv6-smt-new/country/

[GEN6-RIPE] “IPv6 Readiness & Public Administration in Europe” presentation at RIPE meeting in October 2013, retrieved on 16 April 2014 from http://www.ipv6observatory.eu/wp-content/uploads/2013/09/06-GEN6_ZD_Athens_2013.pdf

[goog] http://www.google.com/intl/en/ipv6/statistics/

[Huston] Geoff Huston, “Launch+365” Presented at RIPE67 16 October 2013.
https://ripe67.ripe.net/presentations/115-2013-10-16-ipv6-launch-365.pdf

[IDA] Internet Protocol “No Islanding” Principle for Internet Access Service Providers, 1 June 2013,
https://www.ida.gov.sg/~/media/Files/PCDG/Consultations/20110620_NoIslandingPrinciple/IntProNoIslPrinciple.pdf

[IDAFAQ] From Idacomm IPv6 FAQs, accessed on 11 April 2014 at
http://www.ifaq.gov.sg/iDA/apps/fcd_faqmain.aspx?qst=2fN7e274RAp%2bbUzLdEL%2fmCxs7iwcgv8gv2atNDOvsLC0Cx6jOAw1Z58ChwPxurxYiJDVkHCsS%2f44%2f4VvIEMuMWXDpF8J%2fh7Yyjh5hpl5zFTwbOoVYZf8UOKxfGACAGjTR20lS9UsyntjSWfruR52pHb63EJfkC%2f5s5ZMDte%2bGjtv7j4JqMvyNZO5IeFcZtbDqev8ieQ6Rp%2bFNtuytotQjHbVagZpOv4CgT%2bMq96y3PY08K1E8RJPKg%3d%3d#FAQ_40721

[labs.apnic] http://labs.apnic.net/ipv6-measurement/Economies/LU/ provides tools to view deployment by country or by ASN/company.

[NIST] U.S. Government IPv6 statistics from NIST, accessed 17 June 2014 at
http://usgv6-deploymon.antd.nist.gov/cgi-bin/generate-gov

[NRO-survey] Number Resource Organization, “Global IPv7 Deployment Survey,” June 2013.
http://www.nro.net/wp-content/uploads/Global-IPv6-Deployment-Survey-2013-final.pdf

[OMB] Memorandum M-05-22, "Transition Planning for Internet Protocol Version 6 (IPv6)" http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2005/m05-22.pdf

[Průša] From "Policies and IPv6: Lessons Learnt from the Czech Republic" presentation by Jiří Průša to ION meeting, retrieved on 16 April 2014 from http://www.internetsociety.org/deploy360/wp-content/uploads/2012/09/Prusa-ION_Sao_Paulo.pdf

[rfc7021] Donley, C. and L. Howard, V. Kuarsingh, J. Berg, J. Doshi, "Assessing the Impact of Carrier-Grade NAT on Network Applications." http://tools.ietf.org/html/rfc7021

[supply] Howard, Lee, and Kelly Brooks, "IPv4 Supply Analysis," November 2013.

[TCO of CGN] Howard, Lee, "Internet Access Pricing in a Post-IPv4 Runout World." http://www.wleecoyote.com/documents/pricing_v1.3.docx.

[Vyncke] http://www.vyncke.org/ipv6status/