NSF/OECD Workshop on the "Social and Economic Factors Shaping the Future of the Internet"

Geoff Huston
January 2007

Question 1: ***Addressing (as reflected in routing protocols, etc) is a fundamental part of the Internet. How can addressing be improved so as to improve efficiency of inter-networking and so as to face the challenges of addressing new devices and objects?***

Addresses in the context of the Internet's architecture fulfill a number of roles. Addresses uniquely identity network "endpoints", providing a means of identifying the parties to a communication transaction. AS well as this end-to-end identification role, addresses also used by the network itself to undertake transfer of data, where the address is used as a means of identifying the location of the identified endpoint, relative to the topology of the network. Addresses are also used within the switching elements of the network as lookup key to perform a switching decision. In other words addresses in the IP architecture undertake the combination of "who", "where" and "how" roles in the network's architecture.

Addresses have a number of properties are all essential in the context of the integrity of the network:

- Uniqueness: Addresses should be uniquely deployed (considerations of anycast deployments notwithstanding). Uniqueness is not an intrinsic property of an addressing scheme per se, but is a derived property of the associated distribution and deployment framework. And addressing scheme in this context should preserve this attribute.

- Consistency: Addresses should be drawn from a consistent identifier space. Using multiple identifier spaces causes the potential of misinterpretation of the address.

- Persistence: The address value should remain constant, and gratuitous changes in the mapping from the identifier to the referenced object should be avoided. Constantly changing address-derived identities are, at the very least, very difficult to track.

- Trust: Can an address object withstand a challenge as to the validity of the address? Other parties who would like to use this address in the context of an identified endpoint would like to be reassured that they are not being deceived. 'Use' in this context is a generic term that includes actions such as resolution to the object identified by the address value, storage of the address for subsequent 'use', referral, where the address token is passed to another party for their 'use'.

- Robustness: The deployed address infrastructure should be capable of withstanding deliberate or unintentional attempts to corrupt it in various ways. A robust address system should be able to withstand efforts to subvert the integrity of the address framework as a means of undertaking identity theft or fraud.

The issues, or shortfalls, with this Internet addressing architecture start with the collection of basic roles that are undertaken by a single IP address. This combination of "who", "where" and "how" makes for highly efficient network operations that are essential in any connectionless packetized data communications system, but at the same time this semantic overload of the address is also the cause of considerable complexity in the Internet:

- Mobility remains a significant challenge in this environment, where the major attribute of any form of mobility is to preserve the notion of endpoint identity, while allowing the network location and switching decisions to change, reflecting the changing physical location of the endpoint.

- The granularity of the addressing system represents an uncomfortable compromise. An IP address is intended to identify a device's network interface, as distinct from the device itself or the device user. A device with multiple active interfaces has multiple IP addresses, and while its obvious to the device itself that it has multiple identities, no one else can tell that the multiple identities are in fact pseudonyms, and that the multiple addresses simply reflect the potential for multiple paths to reach the same endpoint.

- The granularity of the overtly network visible part of the address is not that of an application, service class, or user. This has implications in terms of the ability of the network to provide varying service responses to various packet classes, where deep packet inspection, and an associated omission of any form of application header encryption, is required for such measures.

- Also, the address does not identify a particular path, or set of paths through a network, or possibly even a sequence of forwarding landmarks, but simply the desired endpoint for the packet's delivery. This has implications in terms of application performance and robustness, and also has quite fundamental implications in terms of the design of the associated routing system.

The Internet's address architecture represents a collection of design decisions, or trade-offs, between various forms of conflicting requirements. For example, with respect to the routing system, the desire for extremely high speed and low cost switching implementations has been expressed as a strong preference for fixed size and relatively compact address formats. With respect to the role of addresses as identity tokens, the desire for low cost deployment and a high level of address permanence implies a strong desire for long term stable address deployments, which, in turn, is expressed as a string desire for low levels of address utilization efficiency in deployed systems, which for large systems implies extended address formats, potentially of variable length.

With respect to the IP architecture, these trade-offs in addressing design are now relatively long-standing, representing decisions that were made some decades ago in an entirely different context to that of today's Internet. Are these design decisions still relevant today, or are there other potential ways of undertaking these design tradeoffs that would represent a more effective outcome?

The most significant issue with addressing is the fixed length address "span". While 32 bits represents a considerable span, encompassing some 4.4 billion unique addresses, there is an inevitable level of wastage in deployment, and a completely exhausted 32 bit address space may encompass at best some 200 to 400 million uniquely addressed IP devices. Given that the population of deployed IP devices already exceeds this number by a considerable margin, and when looking forward to a world of embedded IP devices in all kinds of industrial and consumer applications, this 32 bit address space is simply inadequate. In response, we've seen the deployment of a number of technologies that deliberately set out to break any strong binding of IP address with persistent endpoint identity, and treat the IP address purely as a convenient routing and forwarding token without any of the other attributes of identity, including persistence and public association. The Dynamic Host configuration Protocol (DHCP) is a commonly used method of extending a fixed pool of IP addresses over a domain where not every device is connected to the network at any time, or when devices enter and leave a local network over time and need addresses only for the period where they are within the local network's domain. This has been used in LANs, dial-up, ADSL, WiFi service networks and a wide variety of applications. In this form of identity, the association of the device to a particular IP address is temporary, and hence there is some weakening of the identity concept, and the dynamically-assigned IP address is being used primarily for routing and forwarding. This was taken a further step with the use of Network Address Translation approaches, where a single device has a pool of public addresses to use, and maps a privately used address device to one of its public addresses when the private device initiates a session with a remote public device. The private-side device has no idea of the address that the NAT edge will use for a session, nor does the corresponding public-side device know that it is using a temporary identity association to address the private device. This approach has been further refined with the Port Address translators that also use the port address field in the TCP and UDP packet headers to achieve an even high level of effective address compression.

NATs, particularly port translating NATs, are very effective in a client-server network environment, where clients lie on the "internal" side of a NAT and all the well known servers lie on the "external side. But is an environment of peer-to-peer applications, including VOIP this concept of using raise a number of challenging questions. Each unique session is mapped to a unique port and IP address, and sessions from multiple private sources may share a common IP addresses, but differentiate themselves by having the NAT-PT unit assign port addresses such that the extended IP + port address is unique. How do you know if you are talking directly to a remote device, or talking through a NAT filter, or multiple NAT filters, or NAT-PT filters? And if you are talking through a NAT, how do you know if you are on the 'outside' or the 'inside'?

These forms of changes to the original semantics of an IP address are uncomfortable changes to the concept of identity in IP, particularly in the area of NAT. The widespread adoption continues to underline the concept that as an identity token there is a lack of persistence, and the various forms of aliasing weaken its utility as an identity system. Increasingly an IP address, in the world of IPv4, is being seen as a locality token with a very weak association with some form of identity.

Of course that doesn't stop undue assumptions being made about the uniform equivalence of identity and IP address, however specious it may be in particular situations, and various forms of IP filter lists, whether they be various forms of abuse black lists or security permission lists all are evidence of this contradictory behavior of assuming that persistent identity and IP address are uniformly equivalent.

Version 6 of IP is an attempt to restructure the address field using a larger span, and the 128 bits of address space represent a very large space in which to attempt to place structure. However in and of itself IPv6 still has not been able to make any significant changes to the address role within the Internet architecture.

If we want to consider changes to the address semantics in the Internet's architecture then it appears that simply increasing the span of the address value range presents a weak value proposition in terms of remedies to the shortfalls of the overloaded semantics of an IP address. None of the deeper and more persistent issues relating to the overloaded address semantics are reduced through this measure and the issues relating to the scaleability of routing, mobility, application level complexity, and robustness persist.

An area of investigation that presents greater levels of potential may lie in cleaving the concept of an address into distinct realms, minimally that of endpoint identity and that of network location. Such an approach could embrace a relatively unstructured identity space, whose major attribute would be persistent uniqueness, and where the identity value of an object, or part thereof, could be embedded at the time of manufacture. It would also allow the deployment of a structured location space that had the capability to describe the topology of the network in a manner that was able to guide efficient local switching decisions. The challenge here is not necessarily in the devising of the characteristics of these identity spaces, but more likely to be in the definition of mapping capabilities between the two distinct identification realms. In other words how to map, in a highly efficient ad robust manner, from an identity value to a current or useable location value, and, potentially, how to perform a reverse mapping from a location to the identity of the object that is located at that position in the network.

There is a considerable range of design choices that are exposed when the address-based binding of identity with location is removed. The most salient observation here is that if we want to consider some form of "improvement" to the current role of addresses in the Internet's architecture, then there is little, if any, practical leverage to be obtained by simply increasing the size of the address field within the protocol's data structures or altering the internal structure of the address, or even in altering the address distribution framework. Such measures are essentially meaningless in terms of making any significant impact on the semantics of the address, nor on its flexibility of utility within the IP archtecture.

If we want to create additional degrees of flexibility within the architecture of the network, then it would appear that we need to decouple aspects of current address semantics and in so doing we need to revisit the fundamental concepts of the Internet's architecture. If we want identity, location and network path determination to be expressed in such a manner that are not fate-shared then we also need to bring into

play additional concepts of dynamic mapping, binding security and integrity, and various forms of rendezvous mechanisms.

As the original question asserts, addressing is a fundamental part of the Internet. If we want to contemplate substantive changes to the address model we are in effect contemplating substantive changes to the architecture of the resultant network, as compared to today's Internet. Perhaps this is indeed a more productive area of activity than the approach taken by IPv6, where the changes have been relatively minor and the impetus for adoption by industry has, to date, proved to be insufficient to offset against the incremental costs and perceived incremental benefits.

Question 2: In designing new protocols, what lessons can be learned from the slow deployment of IPv6 to date?

There are significant differences between devising an experiment that investigates various models of communications paradigms and undertaking a major revision to a mainstream communications protocol. The major reasons for the slow deployment of IPv6 today lie in both economic and public policy considerations as much as they lie in considerations of the underlying technology.

The Internet's major positive attribute was not derived any particular aspect of its underlying architecture or characteristic of its protocols. Indeed, the Internet was in many ways essentially dormant through the 1980's, and, in terms of its architecture and protocol technology the Internet has not changed in any fundamental sense for some decades. It remains a connectionless, hop-by-hop forwarding, destination-addressed unreliable datagram delivery system with end-to-end control loop overlays to provide additional services related to resiliency, session management and performance characteristics.

The major economic and social factor of the late 1980s' and early 1990s' when the Internet was expanding rapidly included the shift away from a highly regulated data market to a regulatory framework that allowed, and in some cases even encouraged, the proliferation of private data networks that went well beyond closed user groups based on tightly constrained bounds of common use. The prevailing regulatory regime allowed all forms of resale and service provision in a highly competitive market for data services, and the economic environment was one of considerable interest in technology and communications. This was coupled with the shift in the computing market from large scale mainframe systems into the computer as an item of consumer electronics, and a change in the nature of the information industry workforce into one that relied on intense use of IT solutions and associated networks.

The attributes that the Internet bought to this emerging market was an unprecedented level of flexibility and efficiency that allowed almost any combination of underlying communications media and all forms of end devices to be amalgamated into a single cohesive IP network. The technical factors that lead to the rapid deployment of IPv4 included IPv4's flexibility and ability to bridge across multiple underlying network media in a flexibly and cost efficient way.

The economic and public policy factors included IPv4's considerably lower unit cost due to the high carriage efficiency and foundation in open standards with open reference implementations. The policy framework of deregulating the data services market and allowing various forms of resale and competition encouraged new investors who were inclined to use innovative products and services as part of their market positioning.

None of these factors are driving IPv6 deployment. IPv6 is no different to IPv4 in terms of its deployment capabilities, carriage efficiencies, security properties, or service capabilities. There is no change in the public policy regime with respect to IPv6, and no significant innovative difference in IPv6 that would provide a competitive edge to innovators in the market. An additional consideration is that IP services are now marketed in a highly contested price-sensitive market, and the revenue margins for most forms of mass-market IP services are very low. The capacity of the service industry to absorb the incremental costs associated with a dual-stack deployment of IPv6 without an associated incremental revenue stream are, to date, evidently unsupportable.

The basis of this observation is that the significant impediment to IPv6 deployment is not availability of network equipment, nor the capability of end systems to support IPv6, nor the capability to roll out IPv6 support in most service providers' IP network. The impediment for IPv6 deployment appears to be a well-grounded business case to actually do so.

The expectation with IPv6 was that the increasing scarcity of IPv4 addresses would drive service providers and their customer base to IPv6 deployment. What does not appear to be factored into this expectation is that Network Address Translators (NATs) produce a similar outcome in terms of virtually extending the IPv4 address space, and, additionally, are an externalized cost to the service provider. Service providers do not have to fund NAT deployment. For the consumer the use of embedded NATs into the edge device is a zero cost solution. The marginal incremental cost of NAT functionality in the edge device is effectively zero for the consumer. So, in general, neither the consumer nor the service provider see a higher incremental cost in the use of NATs. Even at the application level the incremental cost of NATs are not uniformly visible. For traditional client-server based applications then there is no incremental cost of NATs. Even various forms of peer-to-peer applications operate through NATs. It appears that the only application that has some significant issues with NATs are VOIP applications, where the major issue is not the presence of NATs per se, but the fact that NATs has never been standardized and different NATS can behave differently. Currently it appears that the path of least resistance for the industry appears to be that of standardizing NATs, over the option of a near term migration of the entire Internet to IPv6.

It is not enough to consult with industry players as to their perceptions of technology needs, as was the case in the design of IPv6. It is also necessary to understand how needs are actually expressed within the economics of the industry. If a technology is to be taken up by an industry, then the factors that lead to take up are variable, and are not wholly concentrated on aspects of superior performance or lower cost of deployment and operation.

Question 3: What will a new Internet with different architecture and protocols mean to IPv6 deployment?

This is a topic that lies well into the area of speculation.

The one salient observation is that infrastructure investment is a long term investment and such investments accrete strong resistance to further change. It is unlikely that the development of further communications technologies, whether terms "Internet" or otherwise, would have any particular impact on the prospects of IPv6 deployment, positive or negative, assuming that the incremental benefits of this "new" technology were relatively marginal in nature.

Any viable "new" communications technology would once again have to demonstrate further gains in efficiency of at least one order of magnitude, or potentially two or three orders of magnitude over those achieves by existing Internet networks, and make substantive gains in the areas of support for mobility, configurability, security and performance in order to represent a serious increment in the value proposition that would induce industry deployment. Of course if a new technology were capable of offering such significant improvement in benefits, then there would be little sense in further deployment of either IPv4 or IPv6.

So the most appropriate response to the question is that "it depends". If such a "new" Internet with a different architecture and different protocol were in a position to offer clearly demonstrable significant improvements in the cost and benefit proposition, then the impetus for deployment would be relatively assured. On the other hand if the case for improvements in the cost and benefit were more marginal in nature then the case for deployment would be highly dubious.