The ISP Column
A column on things Internet

November 2023
Geoff Huston

Call the Routing Police!

There was a somewhat unfortunate outage for a major communications service provider in Australia, Optus, in mid-November. It appears that one of their peer BGP networks mistakenly advertised a very large route collection to the Optus BGP network which caused the routers to malfunction in some manner. The problem was compounded by the fact that the engineering response required to rectify the situation was also using the same underlying platform which had just stopped functioning, so they evidently found themselves locked out of parts of their network. It's a big service provider in Australia, with a portfolio of mobile and fixes services in the retail, commercial and public sector, so this outage was big. Some 10M users found themselves without communications services for hours, and in some cases days. In terms of BGP-induced network outages it was a big one.

The forensic examination of why this occurred continues, within the company without doubt, but also in the public space. You can't have a disruption of public services to such a large set of consumers without some need to provide a public airing of the causes of the outage. If this were a bank heist the site would no doubt be saturated with investigators from the police force. But this was a routing heist. The routing system effectively seized control of the operator's network and put it out of action. So where are the routing police to investigate the incident? How can we understand the exact nature of the triggers for this outage and identify if there was some level of contributory negligence from the network operator or their suppliers that amplified a minor issue of a route leak into a major that impacted millions of consumers? We need to call the Routing Police! But who are the Routing Police? And where may be find them?

The Architecture of Routing on the Internet

Much of the Internet's architecture is decoupled, or loosely coupled at best. For example, the routing function is decoupled from forwarding, so each network can determine what internal routing protocol to use within their network without impacting on the stateless hop-by-hop destination-based packet forwarding process used across the entire Internet. Similarly, the IP protocol is decoupled from the underlying transmission media. IP can be used across a variety media, where each new media type needs to define a packet framing format and how to map an address acquisition profile, such as ARP or SLAAC, into the context of this particular network medium. This loosely coupled network architecture extends into the organisational structure of the Internet. No single entity is in control, and there is no single entity whose role is to orchestrate all the individual functions within the networked environment into the cohesive whole of a collection of networked services.

This loosely coupled model has served the Internet well in many ways. No permission is required to field a new service or a new technology or extend the capabilities of existing protocols or services. As long as the outcomes of such innovative exercises are able to safely interoperate with the installed technology base of the internet, then there is no additional authority or permission that is needed from anyone else.

If there is an arbiter of interoperation on the Internet then I guess it's the collection of Internet Standards, that define protocol behaviours that are intended to create interoperable outcomes.

But when it comes to aspects of operational stability and security and the associated topics of authenticity and verification, this open and generally permissive networked environment can run into some difficult problems. Who is to judge what fragments of routing information are genuine and being circulated with good intent? How are any such attestations of authenticity communicated across the network? And if we would like to remove false, fraudulent or accidentally included material from the network, then who has the appropriate authority to enforce such behaviour?

We've responded in various was to this challenge in various activity forums. We created a cabal called the CAB Forum who lay claim to be a universally trusted set of certificate issuers for domain name certificates used by browser vendors. We've created hierarchies of delegation of roles, such as the DNS name hierarchy, and then invested significant trust in the trustee of the single root domain at the apex of this hierarchy, in the form of the ICANN community.

In the distributed routing environment, who is in control? Who says what is acceptable and what is unacceptable in terms of routing behaviours? If there is abuse, or when two or more parties are in dispute, then who is there to sort out the routing issues, or adjudicate any disputes in the routing space? In short, who are the Routing Police for the Internet and where might we find them?

The Regional Internet Registries?

One possible response to this question is that this routing policing function is part of the role of the Regional Internet Registries (RIRs).

There have been conversations in the past about minimum address block sizes in individual address allocations, and the relation between address allocation policies in the RIR space and various transit ISPs' minimum prefix size routing policies. While the RIRs did not try to alter such routing practices, there was an effort in the RIR communities to harmonise their address allocation practices to prevailing routing policies. In IPv4 the conventional minimum allocated address block is a /24 (assuming you can receive an IPv4 address allocation these days!) and the minimum address prefix accepted by most transit providers is the same size.

Does this administrative role or performing address allocations and operating a collection of IP address registries to record these allocations cast the RIRs in the role of the Internet's Routing Police? For many years the RIRs had a consistent response to the question of enforcing various forms of routing policies: "We are the stewards of the Internet's address pool. We are not the routing police."

But even if the RIRs disclaim this role, are they they the de facto Routing Police in any case?

Some of the RIRs operate Internet Routing Registries (IRRs) which many network operators use as an input to their local routing configuration systems. These registries consist of a collection of databases where network operators publish their routing policies and intended routing announcements. Other network operators can use this information to populate route filters which can be used to reject routing information under certain cases if it does not match information in a route registry. In hosting a routing registry does this infer that the registry operator takes on the role of an active party in a routing policing role?

This seems to be a long stretch of logic to me. A registry is intended to be a common neutral asset for all of its clients and is intended to ease the burden of communication between a collection of network operators by hosting a venue where anything that is posted to the registry is visible to all the registry's clients. The registry is not there to editorialise and indicate a level of relative preference for individual registry entries. Its supposedly a more passive publication vehicle to allow a network's intentions in the routing environment to be seen by, and potentially used in the configurations of, other networks.

In more recent years, the RIRs have introduced the use of public/private keys and public key certificates as a commentary about the address registry (the so-called "Resource Public Key Infrastructure', or

RPKI). The objectives of this exercise were, at least initially, somewhat modest. The address registry describes an address holder, listing their name, address and contact details, and associating this information with the address blocks that have been allocated to this entity. Testing the validity of an asserting that "this is my address block" would require the testing agent to look up the registry and then match the details provided by the entity with the details listed in the registry. The tester may use the email contacts to send a message to validate the claim. But these are weak tests and have been abused in many ways. The RPKI framework asks of the Address Registry operator to request that the address holding entity generate a public private key pair and pass the public key to the registry in the form of a certificate request. The registry can generate and public their own certificate attesting to the fact that the holder of the matching private key is the same entity that is listed in the address registry as the holder of the addresses. Testing the validity of an entity's claim to hold an address block can now be simplified to obtaining a signed object that has been signed with the entity's private key and matching this signed object with the public key that has been published in the registry operator's certificate. This is more susceptible to rapid validation in a fully automated manner.

This may be used in the routing context to convey explicit authorities or permissions. If this address holder signs an authority to permit a network to advertise this address prefix into the routing system, then the authority can be tested for validity against the RPKI certificate set in a fully automated manner, and this lies at the core of the transformation of the RPKI from a commentary about the entities who are described in the address registry to a routing tool used by the BGP routing protocol to convey the validity of route objects being promulgated across the routing system.

The RPKI has reopened aspects of this same conversation about the role of the RIRs as Routing Police, but the answer to the implicit question, namely "Who sets the Internet's routing policies?" remains unanswered, at least from where I sit. It is certainly the case that the positioning of the RIRs at the apex of the RPKI hierarchy provides these RIRs with the wherewithal to deny the ability of a prefix to be routed within those parts of the Internet that respect the RPKI construct of Route Origination Validation. If the ability to deny an action is considered to be synonymous with the ability to control that action, then to some extent the RIRs have assumed the role of routing police, to put it informally. However, the RIR's role in the RPKI is not as the proxy operator of these private keys and the associated instruments of routing policy. The RIRs cannot alter information that has been signed with the entity's private key, nor generate new information in the name of the entity.

In terms of assuming the role of an enforcement agency in routing practices this makes the RIRs pretty poor contenders for the role of Routing Police. Their powers in the administration of the certification function for parts of the RPKI and acting as a publication agency for these signed objects certainly makes them an active entity in this space, but their limited set of abilities, and their self-admitted clear lack of intent does not make them an ideal candidate for the role of Routing Police force. The community of stakeholders in the role of address stewardship are the wrong community for such a role. The RIRs' open policy fora do not necessarily include a detailed consideration of routing capabilities in the deployed Internet, the capabilities of deployed equipment, protocol capabilities, and policy objectives of the routing system. As they say, routing is just not their point of focus, not their area of expertise and engagement and not their responsibility. They are not the Routing Police.

The IETF?

If the RIRs are not the Routing Police, then maybe the IETF is undertaking that role. After all the IETF was the venue where the technical standards for the distributed routing protocols were developed and where they are maintained. The intent of these technical standards is to increase the level of assurance that an implementation of the technology (in this case the BGP routing protocol) that adhered to the technical specification would interoperate with any other standards-conforming implementation.

However, while standards promote interoperation between the individual elements of a distributed environment, they do not necessarily constrain the actions of operators of routing infrastructure. The IETF uses a form of meta-classification to label some of their documents as "Best Current Practice".

BCPs document guidelines, processes, methods, and parameter value selection that are intended to support the stable operation of a standard protocol or service. They are intended to be more flexible than a standard specification, since such operational techniques and tools are continually evolving in the light of experience with operational deployment. There are a number of BCP documents that relate to the operation of the routing space, but it's not the role of the IETF to determine whether individual operators follow these BCPs or not.

Like most standards bodies, the IETF can define what constitutes appropriate and responsible behaviours, but they have no ability to enforce alignment to a particular set of operational practices. They cannot assume the role of the Routing Police either.

NOGs?

What about the various forums where network operators convene and exchange experiences and ideas? There are many such groups that operate at local, national and regional levels (over on Wikipedia there is a list of such groups: https://en.wikipedia.org/wiki/Internet_network_operators%27_group). Such groups are as effective as the commitment of the community they serve to the support of a local NOG. They can be highly effective in promulgating operational practices that manage stabled and efficient service delivery, and help network operators to stay abreast of developments in operating practices.

But once again, there is no enforcement capability in any NOG. They can't direct any service provider to undertake any specific action. They lack the wherewithal to do so, even if they were so motivated. About the best they can manage is a certain level of peer pressure and not much else.

Codes of Practice – MANRS?

An extension of the IETF's BCP concept is the MANRS program. MANRS, or Mutually Agreed Norms for Routing Security (MANRS) is a global initiative, supported by the Internet Society, that provides advice in the form of operational practices that are intended to reduce exposure to the most common routing threats. Again, there is not ability to check if any operator is adhering to these practices, nor any recourse to enforcement actions if they are failing to do so.

MANRS has been effective over the years in promoting the case that routing is not a "set and forget" activity for network operators. It is an activity that does require careful attention and continual monitoring, and the material, tools and data sets provided through MANRS are helpful to the task. However, MANRS is not an enforceable code. It's is more of a set of aspirational objectives for network operators in the provision of stable services.

National and Regional Public Communications Regulators?

The Internet has always represented a challenging set of issues for regulators. In this era of deregulation of communications there has been a general public stance of trying to encourage the participation of the private sector in investing in communications infrastructure and providing services to commercial and retail consumers, and the regulator has often attempted to avoid being overly prescriptive as to how these services should operate. But at the same time there is the emerging issue of public safety, and the increasing latent hostility of the digital space is a deep concern in the realm of public policy and the associated public regulatory environment.

If there is any sector that has the acknowledged legitimacy to establish a body to enforce certain operation practice in the routing space, then logically it would appear to be these national public sectors. But this is a space that is somewhat fraught with uncertainties and unclear scope. Routing is a network-wide activity, and adoption of certain operational practices in one segment of the network does not necessarily insulate that segment from the side effects of operational anomalies generated in other parts of the network. The underlying intent of the BGP routing protocol is to efficiently flood routing information to all parts of the network. BGP cannot readily discriminate "good" from "bad" information in the routing space. What that implies is that any form of routing policing undertaken at a national level does not necessarily infer that that segment of the network will always operate in a safe and secure manner.

Such a national segment of the network will still be liable to admission of anomalous routing information from other parts of the network.

The Internet as a Public Service

Nevertheless, there is perhaps a more substantive part of a role here in the public sector bodies that is missing from the other entities surveyed up to this point. The issue is less about have a regulatory body attempting to provide strictly specified guidelines about how to operate a network's routing system and an associated enforcement mechanism to obtain compliance, but more about acknowledging that each component network of the public network operates a part of the public communications domain, and as such is accountable to its users about the way in which each network operator has discharged this public duty.

We need to respond to outages and related incidents in the Internet in a way that does not immediately attempt to sweep it under the closest rug and deny that anything untoward ever happened at all! The airline industry is a case in point where the object of an investigation is not necessarily to apportion blame, but to unearth the root causes and potentially propose measures that aeroplane operators can adopt that would prevent a recurrence of the mishap.

The Internet could learn a valuable lesson from this approach, and the first step is to own up to public accountability when anomalous events occur (see https://www.potaroo.net/ispcol/2021-07/outage.html and https://www.potaroo.net/ispcol/2021-10/nofacebook.html for a closer examination of what public accountability means when responding to service outages). If the regulatory role was able to encourage such detailed and dispassionate investigation of interruptions to the public communications service, then for me it would be the most valuable role any such public regulatory body could perform.

In the world of public corporations, we've generally accepted that if you want your customers, your investors, your regulators, and the broader community to have confidence in you and have some assurance that you are doing are doing an effective job, then you need to be open and honest about what you are doing and why. The entire structure of public corporate entities was intended to reinforce that assurance by insisting on full and frank public disclosure of the corporate's actions.

So perhaps it's not a case of invoking the Routing Police to improve the Internet's routing platform. What would sharpen our attention to improving the resiliency of the routing platform is to adopt a more constructive attitude to how we response to outages and routing incidents.

It would be good if all service providers in the public Internet spent the time and effort post rectification of operational problems to produce detailed and thorough outage reports as a matter of standard operating procedure. It's not about apportioning blame or admitting liability. It's all about positioning these services as the essential foundation our of public digital environment and stressing the benefit of adopting a common culture of open disclosure and constant improvement as a way of improving the robustness of these services. It's about appreciating that these days these services are very much within the sphere of public safety and their operation should be managed in the same way.

Disclaimer

The above views do not necessarily represent the views of the Asia Pacific Network Information Centre.

Author

Geoff Huston AM, B.Sc., M.Sc., is the Chief Scientist at APNIC, the Regional Internet Registry serving the Asia Pacific region.

www.potaroo.net