

# Issues in Merging Internet Autonomous Systems for Emergency Communications

Selwyn Russell<sup>1,2</sup> \*

<sup>1</sup> School of Software Engineering and Data Communications  
Queensland University of Technology, Brisbane, Australia  
S.Russell@qut.edu.au

<sup>2</sup> National ICT Australia Ltd. Queensland Laboratory, Brisbane, Australia

## Extended Abstract

The Internet has certain properties which make it the first choice for communications during an emergency. Experiences during the Kobe earthquake in 1995 indicated that the Internet was more resilient than other networks [1]. Fault tolerance and fault recovery were basic DARPA requirements [2]. The lack of a central controller or base station (as used in the two way radio systems often used by emergency handling teams) eliminates a potential critical point of failure.

In a large developed area, there will be numerous TCP/IP networks installed: fiber, copper, wireless, and cable. Internet connectivity is typically provided through communications carriers which operate for profit. Over the past few decades, governments have encouraged or caused, e.g. through privatisation of a government utility, increasing numbers of suppliers of communications services. In a region, the larger utilities and enterprises provide their own networks, each individually registered with the Internet authorities as an Autonomous System (AS). These competing networks normally operate independently, with common gateway points where traffic is passed from one carrier to another. In a time of a large scale emergency in the area, these independent networks provide a basis for a fault tolerant network with good capacity and compatibility with many other networks and user devices. Even though a single network may not be fault tolerant, the diversity and duplication of links and nodes of the combined individual infrastructures are the correct components to form an adaptive network suitable for the situation. The difficulty of course is in merging the independent competing networks into a single collaborative network.

During a large scale emergency traffic behaves quite differently from normal times. The emergency recovery team needs a communication network with capabilities and configurations which have a very different profile from everyday communications networks, to avoid network overload from enquiry bursts and to favour emergency management traffic. Ideally, this temporary network would involve a merger of all commercial networks in the area which at other times

---

\* National ICT Australia is funded by the Australian Government's Backing Australia's Ability initiative, in part through the Australian Research Council

are competitive. Merging networks involves reconfiguration of significant nodes throughout the individual ASes. For large networks, care is needed to ensure inefficiencies and manual errors are not introduced, resulting in a single temporary AS which is inferior to the original arrangement.

To function as a single composite network, the routing tables of at least the gateway routers need to be modified so the networks co-operate and share the loads, and give priority to traffic to/from emergency services devices. Current router software is based on the assumption of a stable network with only small and incremental changes. During an emergency, speed and accuracy are vital, but at those times there is more chance of human error. To simplify communications management throughout a region, it is desirable to be able to describe the ideal network behaviour at that time in a high level policy style specification, and to have the relevant network components automatically reconfigured in accordance with the regional specification.

To accomplish this goal, management must be able to simply specify a complete and unambiguous high level policy for the communications network, and accomplish this act in times of stress and time pressure with a minimum of delay. An RFC on policies for routing first appeared in 1989 and languages for policy specification were used in RIPE-81 in 1993 [3]. Further work has been done, e.g. [4], relating to the control of traffic through transit networks, but we conclude they are not the type of policies or policy description languages needed during an emergency.

As well as the technical difficulties involved in merging networks, there are numerous non-technical barriers, such as commercial secrets, privacy, legal liability, and policies. If the the ASes are highly competitive, commercially sensitive information on operational details might be difficult to obtain, and there is the risk of incompatible equipment, formats, databases or support systems.

In future work we will investigate in more detail requirements for solutions and ways to meet them [5]

## References

1. Yoichi Shinoda, Tomomitsu Baba, Nobuhiko Tada, Akira Kato, and Jun Murai, "Forethought and Hindsight: Experiences from the First Internet Disaster Drill", 1996, INET 1996. Accessed 24 November 2005.
2. Internet Society, "A Brief History of the Internet and Related Networks", Tech. Rep., Internet Society, Oct. 2005.
3. T. Bates, E. Gerich, L. Joncheray, J-M. Jouanigot, D. Karrenberg, and M. Terpstra. J. Yu, "Representation of IP Routing Policies in a Routing Registry (ripe-81++)", Mar. 1995, RFC 1786 and RIPE-181.
4. C. Alaettinoglu, C. Villamizar, E. Gerich, D. Kessens, D. Meyer, T. Bates, D. Karrenberg, and M. Terpstra, "Routing Policy Specification Language (RPSL)", June 1999, RFC 2622; Obsoletes: 2280.
5. Selwyn Russell and Peter Croll, "A Project for the Synthesis of Composite TCP/IP Networks During Emergencies", in *AusCERT2006*.