Grand Challenge: Critical Networking Infrastructure in a Suitcase

David Andersen
Carnegie Mellon University

The challenge: In an underserved rural area or in the days following a significant disaster, a team of five people deploy and operate for at least six months replacement network infrastructure that provides all necessary communication services to those within its coverage area. This deployment should take no more than three days to cover a small city of 20,000 people, providing equivalent services to the telephone network, cable network, and conventional Internet services. The deployment must be robust to challenging environmental conditions, unreliable power and transit infrastructures, and malicious activities such as the wide-spread looting that often occurs following significant disasters. It must support both commercial and life-critical emergency communication. The subsequent operation and upkeep of the network must require at most two people.

Many people have championed rapid network deployment, particularly via ad hoc wireless networks, but few have focused on the extended problems of keeping this infrastructure running and making it highly reliable. The research challenges involved in creating a functional, critically reliable communication system go beyond inventing a new routing protocol or adding radios to a network. These challenges span hardware, network architecture, and software; many would exist even if the physical infrastructure existed already. A primary challenge for these networks is management from the physical layers up: The replacement infrastructure must be self-managing and self-organizing to a much larger degree than today's networks. Both initial setup and ongoing maintenence and upgrades must be simple, fast, and safe.

The hardware to accomplish the deployment must be extremely portable, but also affordable enough to be widely useful. It should be low power, so that it can run for a time on battery power if necessary, and not place excess demands on an already strained power infrastructure. Disasters change communication patterns, often causing significant congestion that renders services such as the voice telephone network inoperable. Dealing with these massive changes is a challenge even for today's best-provisioned networks and services; they impose a tough hurdle for an instant infrastructure.

Finally, this infrastructure must be sufficiently reliable to support services that need "five nines" of availability, a challenge that even today's Internet is hard-pressed to meet. It must be secure and support some notion of authentication for at least a subset of its 20,000 users to support high priority emergency communication.

Achieving this challenge would have significant benefits outside disaster recovery and providing access in underserved areas. Reducing the management complexity of networks by an order of magnitude would significantly reduce the costs of providing network service in all areas. Vastly reduced management complexity would ultimately reduce the impact of the most significant cause of unavailability—human error. These same technologies would benefit consumers by ameliorating the "last mile" problem: if a service provider can easily deploy a high-bandwidth, capable network in an emergency, the same techniques will facilitate network deployment under ordinary conditions. The network architecture to support this challenge will improve availability in the face of more ordinary failures, making it easier to mask fiber cuts, failures due to power outages, and so on. The low-power networking technologies that would flourish in a post-disaster environment would have spillover benefits to today's power- and cooling-hungry data centers.