Observations from Rakesh Bharania
A Tactical Operations Support Engineer
For a Major Telecommunications Company

Lessons Learned
Information Sharing
LLIS.gov

NOTES FROM THE FIELD

Learning from Hurricane Sandy and the Waldo Canyon Fire: Considerations for Emergency Wi-Fi Networks

INTRODUCTION

In the 1980s, MIT Professor Nicholas Negroponte proposed an idea that became known as the "Negroponte Switch," the idea that technologies that were then wired (such as telephone service) would become wireless, and that technologies that were then wireless (such as television) would become wired. The growth in subsequent decades of mobile phone service and cable television both are examples of how this switch has been realized. Similarly in disaster response, we've seen a tremendous uptake in technology – PCs, tablets, and smartphones. When I first started seeing computers used in disaster response in the early part of the 2000s, wired Ethernet connections were the rule, as 802.11 wireless networks were then in their infancy.

Today, of course, wireless networks tend to predominate the mobile, always-connected world we now live in. Smartphones, tablets, and most computers have on-board wireless networking, and the disadvantage of reduced speeds of modern wireless networks compared to their wired counterparts is often more than made up for in user mobility and ease of moves, adds and changes as new stations come online. Because of its ease of use and support for most devices, Wi-Fi (802.11 a/b/g/n/ac) networks are considered an integral part of the Hastily Formed Network (HFN) architecture.

In the rush of governments and NGOs alike to deploy emergency Wi-Fi networks after a disaster, recent emergencies have shown that there are going to be increasingly significant challenges for disaster responders to get the kind of quality of service they require. Solving this may require us to reverse the Negroponte Switch (just a little bit) in order to accommodate the Bring Your Own Device (BYOD) world.

CHALLENGES

Spectrum

The most common frequency space for 802.11 wireless networks is in the unlicensed 2.4 GHz space. Without going too deeply into frequency management, understand that there are 14 channels designated within that space between 2.4 and 2.5 GHz. Now understand that since it's unlicensed spectrum, any number of other devices may also occupy that same space, blasting away with their radiofrequency (RF) noise, including cordless telephones and microwave ovens.

During the Waldo Canyon Fire in Colorado in 2012, for example, our equipment detected more than 40 access points operating in the immediate area around the Incident Command Post. Some of these belonged to the local school, others to local residences, and still others were portable "Mi-Fi" hotspots brought in

Waldo Canyon Fire
Starting on June, 23rd 2012, the Waldo Canyon Fire burned 18,247 acres and destroyed 345 homes over a 19 day period. For more information, read the Initial After-Action Report.

by responders themselves. Every responding agency seemed intent on bringing in their own Wi-Fi network. When you put them all close together, you can easily see how those limited numbers of channels suddenly had a lot of contention on them. Forty doesn't divide into fourteen so well…

From a wireless network standpoint, there was so much contention that most of these networks were stomping on one another, jamming their users' ability to get useful connectivity. Technology exists to overcome such contention, but the equipment tends to be pretty expensive enterprise-class stuff, not the consumer-level equipment often used by smaller departments and most NGOs. In effect, it becomes a silent arms race between wireless access points.

During Hurricane Sandy, the problems were different. The power was knocked out in the Rockaways, so many of the otherwise competing access points we ought to have seen were simply disabled by the emergency itself. The problem then became that many of the emergency services buildings we were asked to connect were of a type of construction that significantly degraded wireless network signals.

More Notes from the Field from Hurricane Sandy
Read more about Rakesh's Hurricane Sandy experiences in Hurricane Sandy and Disaster Networks: Key Observations, Good Practices, and Challenges

Education

In the United States, many incidents will have Communications Unit Leaders (COMLs) and Communications Unit Technicians (COMTs) or individuals with similar skills managing frequency allocation for the Land Mobile Radio (LMR) service that is supporting the emergency. However, my experience to date has been that most communications staff do not recognize how important data is to any successful emergency response, are not aware of the contention and quality issues of Wi-Fi networking, and even in situations where they are aware, they often lack the equipment and training (and perhaps even mandate) to effectively deal with the issue.

RECOMMENDATIONS

Reversing the Negroponte Switch is OK

While most techs today think about how to deploy Wi-Fi networks in the early hours of an emergency, I am recommending that network engineers, technology NGOs, and other organizations deploying emergency networks should consider how to solve their connectivity needs through wired networks first, and only then consider where Wi-Fi may be appropriate. There is a cost to this: you need switches, spools of Ethernet cables, and staff equipped to crimp cables in the field. But for mission critical connectivity, I would argue that the benefits of avoiding contention in the Wi-Fi space, and the better quality of network connectivity offered by wired networks is worth it.

Even in a situation with a lot of tablet use, community Wi-Fi hotspots, or other locations where wired connections are not going to be practical, technical staff should consider having a few wired computers available for use just in case the contention at the location becomes too great.

Technology Teams Need to be Prepared to Deploy Wired Networks Early

Many technology NGO and government response teams in the early days of a response will travel lightly, with a few devices and a Wi-Fi hotspot or two. Experience has told us that while this maximizes portability, on-scene connectivity may not be anywhere near as good as you'd hoped when you set out. Assume every other mutual aid responder coming to your emergency is bringing similar kit. Anticipate the need for early wired networks.

If You Must Use Wireless, Consider How to Move Off 2.4Gz

The worst of the contention problem occurs in the 2.4 GHz space. Can you move to the 5 GHz (802.a/n/ac) space, where there are more channels? Some clients don't support 5 GHz connections, so you need to consider compatibility issues. Public safety agencies who are eligible for 4.9 GHz licenses should consider use of 802.11y networks.

Educate Emergency Communicators About the Challenges of Wireless Data Networks

Many emergency communicators are still unaware of the challenges of non-LMR RF spectrum management. These teams need to be trained, equipped and empowered to de-conflict and manage all spectrum related issues related to the incident. This is obviously non-trivial, but it needs to happen.

CONCLUSION

The popularity of Wi-Fi networks is not going to decrease in the foreseeable future. Most modern communications technologies assume a wireless network connection – just try finding the Ethernet jack on an iPad! – but this popularity also creates significant challenges for disaster communicators, even as it opens up huge productivity benefits for disaster responders themselves. While spectrum management equipment and process languishes, the simplest tool that emergency communicators have today is the basic, boring wired Ethernet connection. Communications teams need to be prepared to deploy wired Ethernet early during the response, perhaps alongside of their wireless networks, in order to ensure that mission critical communications is not disrupted or delayed due to spectrum congestion, building attenuation or other radio challenges. Reversing the Negroponte Switch (just a little bit) can go a long way to ensuring that communications stays up and available in the middle of a tech-heavy disaster response.

DISCLAIMER

The views expressed in this document are those of the author and do not necessarily reflect those of *Lessons Learned Information Sharing*.

Lessons Learned Information Sharing (*LLIS.gov)* is the Department of Homeland Security/Federal Emergency Management Agency's national online network of lessons learned, best practices, and innovative ideas for the emergency management and homeland security communities. The Web site and its contents are provided for informational purposes only, without warranty or guarantee of any kind, and do not represent the official positions of the Department of Homeland Security. For more information on *LLIS.gov*, please email feedback@llis.dhs.gov or visit www.llis.gov.