MESH NETWORKS

JUNE 2004 EJEMS

BY WILLIAM E. OTT

This month I wanted to share some information with you on a rapidly developing technology, wireless mesh networks. Mesh networks are data and voice networks built primarily from off the shelf wireless computer networking equipment. The idea goes back to research started in the mid 1990s that was funded by the Defense Advanced Research Projects Agency (DARPA) for the Department of Defense to allow for faster, more reliable, and better coverage for voice and data communications on the battlefield.

I had the opportunity to attend the Homeland First Response Conference in late March/early April on my home turf of Cary North Carolina. Dr. Dave Warner from UCSD and Mindtel (www.mindtel.com) presented some information on some of the really neat things his group is involved with utilizing mesh networks. There were a number of good discussions from various people around the country on the applicability and usefulness of this technology in the public safety arena.

There are a number of deployed mesh networks now in the United States, mainly on college campuses, but some small to medium size cities have also deployed mesh networks. Most are designed for public or student access to the Internet or to make voice over Internet Protocol (VOIP) phone call. In Medford Oregon, they

have deployed a public safety mesh network to handle daily voice and data traffic of the emergency services and public works.

This is really very exciting and affordable technology. My company has been experimenting with small scale, less than 2 square mile ad-hoc wireless mesh networks as a communications overlay to be used in disasters where normal phone, radio, and data systems no longer work. That disaster could be a hurricane, tornado, wildfire, ice storm, or terror event. The mesh network concept actually is very scalable and could be quickly deployed to cover entire towns if required.

Let me explain the mesh concept so you can better visualize how this technology could fit into future operations and disaster communications plans. Mesh networks can be built from common of the shelf (COTS) wireless computer network gear from companies such as Linksys, Netgear, Cisco, D-Link, etc… that operates in the IEEE 802.11 wi-fi protocol for ad-hoc disaster type use. For permanent day to day installations like Medford Oregon has, there is a newly emerged IEEE standard 802.15.4 also known as 'Zigbee' (www.zigbee.org for more info) that offers more flexibility and robustness than the 802.11 gear but at increased cost.

The goal of a mesh network is to provide a path for voice and data traffic within the mesh as well as to the outside world. Think of the mesh as a spider web, each transceiver and access point is self discovering on the network so no switches are needed. Any number of units can be added to the mesh to cover as

large an area as needed. The edge units of the mesh are typically connected to broadband Internet connections via cable, DSL, satellite, or direct connection to the Internet backbone. Because every unit also acts as a repeater of the signals, the system has incredible redundancy and reliability. In areas of dense concrete or steel, many access points can be placed in close proximity to each other as they are placed deeper and deeper into such facilities. Utilizing the 11 available frequencies in the 802.11 protocol in the United States, a complex system can be quickly deployed allowing data and voice to flow unimpeded and without interfering with each other. If any one device fails, all of the other radios of the mesh simply adjust and recompute the path to send the packets of data and voice.

Those of you involved in your local Terrorism Task Forces, Joint Terrorism Task Forces, Emergency Operations programs, and other disaster preparedness groups; mesh network technology has real and immediate benefits. For just a few thousand dollars, maybe less with some luck on e-Bay, you can field a mesh network of your own to cover a one square mile area and deploy it in less than an hour. This would give you the ability to communicate in an otherwise communications dead area. To build the mesh network, a few 802.11 access points are raised a couple hundred feet in the air with small helium balloons like the weather service use. Each access point is powered by a deep cycle marine battery which will run the access point approximately 48 hours. During the daytime you can power the access points with small solar cells which can also charge the batteries. The balloons with the access point are anchored with the

Ethernet cable that also provides the path for the power from the battery to the access point. One or more of the access points will be tied into either a satellite Internet system or preplan arrangements could be made with local businesses and homeowners to be able to access and tie into their broadband circuits in an emergency. Using VOIP phones or radios, wireless equipped notebook PCs, wireless PocketPC and the like you can talk, pass data, and pass webcam video around the scene and to the outside would.

With this simple technology, ambulances, fire trucks, helicopters from other areas can plug right into the mesh and interoperate with the existing units as they arrive at a large event. With some simple software, the commanders can ‘see’ and identify every unit on scene on a PocketPC because each radio identifies itself and what it belongs to.

On the consumer side of things, we will likely start to see mesh type networks starting to cover many downtown areas of the country, as well as highways and Interstates. Many consumer electronics companies are planning personal area mesh networks in the next generation of TVs, stereos, light switches, PCs, etc... All of these devices will be able to communicate with each other within your house.

The possibilities that mesh networking present for emergency communications is really quite amazing. You will start to hear and read a lot more about mesh networks in the weeks ahead. I believe this is going to be a very positive technology for emergency public safety communications needs.

I welcome your comments, criticisms, feedback, and ideas. You may contact me at ejems@cpcstech.com

William Ott is president and chief consultant of CPCS Technologies, a NC-based technology consultancy providing services to the public safety and defense communities. He's been involved in EMS since 1981, in field, education and administrative capacities

William E. Ott

Digitally signed by William E. Ott
DN: CN = William E. Ott, O = VeriSign, Inc., OU = VeriSign Trust Network
Reason: I am the author of this document
Location: Cary, North Carolina
Date: 2004.06.01 20:41:40 -04'00'