



BUSINESS CONTINUITY & DISASTER RECOVERY // EMERGENCY RESPONSE

ON THE CUTTING EDGE: TELECONTINUITY OFFERS SURVIVABLE COMMUNICATION SOLUTION

The announcements by the National Oceanic and Atmospheric Administration (NOAA) and the National Weather Service that the United States is facing a harsh hurricane season could not have come as good news to communication and IT managers. If the terrorist attacks of 9/11 and 7/7, Hurricane Katrina, the Mississippi River floods, and a host of other disasters are any indication, then the communication systems in the hurricane-affected areas will likely be the first to fail, complicating efforts to respond to the disasters and mitigate their consequences, confounding search and rescue operations, and hampering recovery efforts. Similar anxiety must be shared by those in charge of communication networks in Asian and Latin American countries as they brace themselves for tropical storms, volcanic eruptions, and floods.

That communication systems collapse in disaster areas, making it difficult if not impossible for people in these areas to communicate with the outside world and among themselves, should not be surprising: What with the loss of power, the collapse of relay towers and dishes, the destruction of cables and switches, the flooding of tunnels -- telephone services are discontinued, and those services which somehow manage to survive the disaster become so congested that it may not be possible to get through, certainly not in a timely fashion.

There is nothing new or startling about the description above, and yet, surprisingly, it appears that when it comes to addressing the problem of communication during disasters, most of the attention has focused on addressing the problem of communication interoperability among rescue and first response teams from different jurisdictions and agencies. Yes, interoperability is important, especially during disasters, but for communication systems to interoperate with each other they must first survive the disaster. In any event, for businesses in disaster areas the issue of survivable communication systems is more important than the problem of interagency communication interoperability.

The imbalance in addressing these two important communication issues -- interoperability problems and survivability problems -- is now being redressed. More companies and emergency services directors are thinking long and hard about how to provide for continuing communication before, during, and after a disaster hobbles business operations or wreaks havoc on a community.

Jim Kennedy, the business continuity services practice lead and a consulting member of the technical staff of Lucent Technologies, offers a good [discussion](#) which helps us understand what happens to communication networks during a disaster. Kennedy highlights the three links in the communication chain which are likely to fail during a disaster. The failure of each one of them would cause massive problems, let alone the simultaneous collapse of all three:

Local loop. The last-mile communication of service to the customer depends on copper wires or fiber optic cables extending, either above ground or below ground, from the carrier's central office to the customer's premises. This last mile connectivity between the business and its telephone provider, Internet provider, or application service provider may be severely disrupted, if not cut-off altogether, during a disaster as wires and cables are torn and underground tunnels flooded. Cell towers and the equipment mounted on them are often also destroyed during a disaster, as are the last mile circuits which connect these cell towers to the local telephone network.

Long haul. Copper wires and fiber optic cables also connect the local telephone company's central offices to other central offices in the region and to long-distance providers, cell phone carriers, and Internet and data communications service providers around the country and around the world. These inter-exchange or "long haul" circuits provide for interconnectivity and communication beyond the local area. The cables and wires used for long haul are as vulnerable to disruption as those used in the local loop -- but there is a difference: There are many more subscribers who use these long haul circuits, and these circuits carry many more calls, so carriers would typically employ "circuit diversity," that is, they would construct the system so that there are multiple paths available for voice and data on which to travel. If one path which is part of the long haul circuit is blocked, then the voice or data would automatically use another path to reach their destination. Kennedy notes that this may work well in cases of isolated disasters such as localized fires and floods, but when the level of destruction is catastrophic and wide-spread, as was the case in Hurricane Katrina, the Mississippi River floods of a decade ago, and even as a result of serious tornadoes in the Midwest section of the United States, then this circuit diversity would not be of much help because the alternative paths also fall victim to the disaster.

Power. Without power nothing will work. Some central offices and cell phone sites may have emergency power sources such as batteries and stand-alone generators which may suffice for a few hours or days of operation. In cases of harsh hurricanes and earthquakes, however, power may be interrupted for several days or even several weeks. In a major disaster it is often the case that power plants, central offices, or cell towers in the affected areas may be inaccessible for most of that time, making it impossible to change spent batteries or refuel generators.

TeleContinuity

We are intrigued by a new communication continuity solution from Rockville, Maryland-based [TeleContinuity](#). TeleContinuity's solution aims to allow a company's managers and key staff to continue to operate the company from remote locations or from their homes. By "continuing operations" TeleContinuity means that these staff members will continue to have uninterrupted access to company's records, clients, suppliers, vendors, production facilities, and other staff members. As importantly, calls made to the company would arrive at the company's regular numbers and extensions, obviating the need for secondary PBX. The TeleContinuity solution also avoids one of the major communication problems during disasters – congestion. The solution does this by routing calls around central office and PSTN outages and by reallocation bandwidth to cope with increased traffic.

TeleContinuity manages all this through a patented technology which allows calls to be moved between the PSTN and the Internet for delivery at any location over any network and on any device (landline phone, cell phone, IP phone, laptop, computer, or PDA).

There are other attractive aspects to the TeleContinuity solution. Organizations subscribe to the service on a per-user basis fee (see below) with no need to change current service plans or carrier, buy any hardware, or install any software. The service resides in the background and is always "on" -- subscribers may activate it if they suspect a disruption is about to occur, or is already underway. The service may be activated through a Web browser, e-mail, text message, or telephone call. Once the service has been activated, subscribers, regardless of where they are, may continue to make and receive calls using their regular phone numbers and extensions.

The company describes its solutions as meeting the five requirements of a reliable and robust emergency communication system: Location independence (staff must be able to make and receive calls regardless of their location); network independence (the emergency service must move call through any and all surviving operating networks – PSTN [landline, cell] or IP [softphone, VoIP, laptop, PC, PDA]); device independence (executives and staff must be able to communicate by using any device – cell phone, PDA, laptop, PC, etc.); survivable telecommunication network (the network must be self-healing and relatively immune to disaster effects); and isolation and independence from the disaster site's local loop (we said above that the first link in the chain of collapse is the local loop, so an effective emergency solution must reduce or eliminate dependence on this local loop).

How does the TeleContinuity solution work? The company does not offer too many details about its patented technology, but says that it has created a survivable network of interconnected POPS across the United States ("from Boston to San Diego") which, short of disaster which will overwhelm the entire United States, makes it impossible to shut down the network. The company's POPS are connected to every major PSTN -- and up to nine Tier 1 internet backbones – making it possible for the network to route and reroute calls around any points of failure or congestion of any carrier.

At the heart of the TeleContinuity system is what the company calls Heterogeneous Adaptive Dynamic Intelligent Routing, or HADIR. The HADIR combines distributed physical architecture with dynamic routing intelligence – the software the company developed is deployed over a network of Control Points of Presence (CPOPs) and Transport Points of Presence (TPOPs) located in co-location facilities throughout the country, and that software continuously evaluates and assesses the existing network links between POPs, from the PSTN to the POP, and from the POP to the user for those users that are on IP phones. The combination of PSTN and the Internet creates thousands of possible call paths, and during an emergency, the solution's algorithms read the real-time condition of each network and routes calls to optimize completion and quality of service.

Note that the TeleContinuity solution also addresses two potential vulnerabilities which typify today's enterprise communication universe:

- More and more business rely on VoIP for their communication. VoIP may be economical, but it is even less sturdy than more traditional communication methods, and VoIP-based network are thus even more susceptible to disruption during a disaster. TeleContinuity network addresses this vulnerability to ensure that VoIP is available during disasters.
- A second feature of today's communication world is that more and more large companies and organizations have their own central switches which control incoming and outgoing calls. Often, these central switches do not have a backup switch capable, in case of a disaster or local loop outage, of picking up the telephone traffic. The TeleContinuity solutions redirects and reroutes central switch traffic to alternate facilities -- or reroutes individual calls to the intended called party with no interruption of service.

Here are a few more things you may want to note about the solution (the first two are aimed at the more technically inclined):

- TeleContinuity does not integrate with the SS7, and all connections to all the POPS are through Q.931 signaling over Voice DS3/T1/PRI Connections.
- The meshed TeleContinuity POPS route calls are based on Application Layer 7 routing, using a modified form of SIP. The intelligence of the network is thus performed in an application and not in the link or interface layer (that is, Layer 3, 4 or 5). The intelligence in the network is based on the interaction of the routing engine with several data repositories on the network, and the proprietary routing engine evaluates information on PSTN/IP congestion, bandwidth utilization and availability, and user information in the process of making its routing decisions.
- It is a voice-only solution, guaranteeing the continuation of voice services, but not data transmissions. TeleContinuity is doing so for a reason. As far as we can tell, no one has addressed the problem of voice continuity in the marketplace from the perspective of survivability. This means that today TeleContinuity has no competition (as evidenced by several sole source agreements the company signed). The data marketplace, on the other hand, is saturated with competition..

- TeleContinuity does not need to sign any roaming or exchange agreement with any carrier – and the individual subscriber does not need to do anything, either. Note that if customers are willing to pay the per-minute fee, they may use TeleContinuity as a telework solution even during non-disaster times.
- Service may be purchased as an annual subscription at \$5 per line or extension per month plus setup fees (which start at \$2500). All usage is billed back to the customer in minute increments (\$.05-\$.07 per minute).
- As is the case with all other solutions: If there is no power, there is no service. For the system to work, subscribers must at least have a dial tone or the system does not operate (see our comments on power failure above).

Telecontinuity is currently in use at several U.S. government agencies and major financial services firms. The system was recently tested – and proven valuable -- in an actual service interruption at a financial services firm: The firm's telecom line had been cut, but services were restored within 90 seconds.

Telecontinuity has received more than \$9 million in funding support from NIST (ATP grant), the State of Maryland, and private investors, including, most recently, an investment by the Stevenson, Maryland-based [Nobska Ventures](#).