GUEST EDITORIAL

NETWORK DISASTER RECOVERY

Chi-Ming Chen

Anil Macwan

Jason Rupe

Telecommunication networks are known for high reliability. This is true for normal operations and outages due to failures in the network associated with hardware, software, and so on. However, unexpected disasters (e.g., earthquakes, hurricanes, and terrorist attacks) do happen, and can have catastrophic impacts without excellent network contingency planning. This feature topic will address the various approaches to plan for and manage recovery following disasters, so that all concerned can mitigate these events effectively.

Network disaster recovery (NDR) has become timelier in the last few years, with catastrophic natural disasters occurring in different parts of the world due to various causes, with different responses necessary. There is no telling when and where the next disaster will occur, but disasters will occur. This topic will continue to gain attention until properly mitigated. Communications is critical to survival and safety, as well as to the health and security of the world. With growing penetration of the Internet from residential use, combined with commercial and otherwise significant traffic being carried over backbone networks, impacts from service interruptions continue to be critical to many segments of society. Most technical articles in this area cover emerging technologies, standards, protocols, and networking solutions; but address less in terms of what to do when they fail, especially when such failures are numerous and catastrophic, and how to maintain critical communications.

This feature topic of *IEEE Communications Magazine* aims to provide a comprehensive overview of the state of the art in technology, regulation, and standardization for NDR, and to present a view of research and industry challenges and opportunities in this area.

NDR is mainly about recovering communications after a disaster, supporting communications during disaster recovery operations, and rapidly bringing life back to normal for customers of the network. At times, you need to work toward all three at once! And because triggering events can happen without notice and in unpredictable ways, with unpredictable results, we must plan accordingly. Furthermore, the rarity of these events makes it difficult to obtain resources and assess risk.[1]

Network recovery requires mobile replacements within short times, including rapid power backup and fast restoration of service. Network operators need to be prepared to rebuild any part of their networks extremely rapidly. In addition to communications networks, disasters will most likely damage other infrastructures and systems, and render them dysfunctional. Repair of the other infrastructures requires coordination, which requires effective communications. This need makes network recovery a high priority.

Disasters can cause severe disruption to peoples' lives. Communications with relatives and assistance resources outside the scope of the disaster is critical to recovery and human security. The importance of effective communications is clear, but equally clear is the vastness of the causes of disasters. Both natural and manmade disasters should be considered. It is important to plan for what you cannot prevent; strengthen your mitigation capabilities, and plan for the massive impacts of the worst case. Because disasters can not be predicted well, it is crucial to plan creatively, robustly, but without concrete information or known risks.

Network disaster recovery is insurance paid for through preparation, supplemental to an insurance policy, so that networks, and the businesses and end users the networks serve, can survive through and after a catastrophe.

Among the five articles of this NDR feature topic, two are on the best practices of major operators; one on the lessons learned from the China earthquake in 2008; one is from a large product manufacturer on key actions necessary to properly prepare for an emergency; and one is from academia on how to deliver messages from and to a disaster area.

In "Rapidly Recovering from the Catastrophic Loss of a Major Telecommunications Office," Kelly Morrison describes the mobile response components and processes for service restoration of a failed network office. With the fast evolution of communications technology and various environmental conditions, a key step to the success of a

[1] *That is why network disaster recovery is such an important issue, and why we present these articles for your reference.*

recovery is exercise so that the recovery team is trained and ready. This article also shares the recovery experiences from real disasters.

In "Disasters Will Happen — Are You Ready?" Chris Oberg *et al.* explain in great detail the planning necessary for a solid network disaster recovery plan, the pitfalls to avoid, and the many elements of the plan that you may not have considered. They suggest several elements of a good plan, and provide some guidelines and tools you can apply to your own disaster planning. Furthermore, they cover key elements to include in a plan, and even how to work with the government to coordinate successful recovery of network services, as well as how to support recovery efforts. By sharing their real world experience at Verizon, these disaster recovery and communication network veterans share their 99 combined years of experience on network disaster recovery.

Considering many lessons learned, Yang Ran provides "Considerations and Suggestions on Improvement of Communication Network Disaster Countermeasures after the Wenchuan Earthquake." In this article she analyzes what worked and did not work well in the recovery efforts of the Wenchuan earthquake, and in related events such as Katrina, the 2005 London bombings, and the 9/11 attacks. From this analysis, the author provides several improvements: priority service functions in the public switched telephone network (PSTN), strengthening wireless communications capabilities, and leveraging technologies to handle emergency high-volume traffic. In addition, Yang Ran provides suggestions for future research to enhance network disaster recovery capabilities.

Rick Krock, in "Lack of Emergency Recovery Planning Is a Disaster Waiting to Happen," highlights the need for emergency preparedness and discusses several key actions necessary to properly prepare for an emergency. He cites a 2006 study, "Availability and Robustness of Electronic Communications Infrastructures" (ARECI), which focused on reliability and security of networks in addition to emergency preparedness. He discusses specific recommendations that are applicable to disaster recovery. This article also cites a recent example of industry's efforts to anticipate and prepare for an emergency situation, related to the 2009 worldwide flu pandemic associated with the H1N1 virus strain. Cooperation among government and industry, including network operators, vendors, and other parties, as well as among countries, should continue and get stronger for better recovery planning in the future.

An important need for end users of networks is the ability to communicate during the post-disaster phase while they are in shelters. Kenichi Mase presents a novel communication system and service to accomplish this end in the article "How to Deliver Your Message from/to a Disaster Area." The system, called the Shelter Communication System (SCS), connects to the Internet, and accounts for the fact that networks may be severely damaged and traffic overload may occur. The SCS is designed to provide message communication service between shelters, as well as between shelters and points outside the disaster area. Evaluation of a prototype of the SCS and other message services, cellular phone mail, and facsimile is presented. According to the author, the SCS can help maximize the role of the Internet as the social infrastructure to contribute to rapid disaster recovery.

BIOGRAPHIES

CHI-MING CHEN [SM] (chimingchen@ieee.org) has been working in the R&D departments of major telecommunications service providers since 1985. He joined AT&T in 1995. His current responsibility is the operations support system (OSS) architecture of process automation, traffic management, incident management, change management, and network disaster recovery. He supports the architecture planning for the AT&T Global Network Operations Center (GNOC), which monitors and controls AT&T's worldwide network. Prior to joining AT&T, he was with Bell Communications Research (currently Telcordia) from 1985 to 1995. His responsibilities included specification of quality and reliability requirements for various networks and network elements, and supplier product testing and analyses. From 1975 to 1979 he was a faculty member at Tsing Hua University, Taiwan. He received his Ph.D. in computer and information science from the University of Pennsylvania; his M.S. in computer science from Pennsylvania State University; and his M.S. and B.S. in physics from Tsing Hua University, Taiwan. For 2010–2011 he is serving as the Advisory Board Chair of the IEEE Communications Society Technical Committee on Communications Quality & Reliability. He was/is the Business Forums Chair of IEEE GLOBECOM 2009 and 2010 and ICC 2011. He has also served as Technical Program Co-Chair of the IEEE Symposium on Computers and Communications (ISCC) 2006 and 2010. He is a senior member of ACM.

ANIL P. MACWAN [M'98] (anil.macwan@alcatel-lucent.com) has been working on reliability analysis, methods, and methodology in communication and other industries since 1992. He started his career in communications with Lucent Technologies in 1996. His responsibilities include root cause analysis, hardware and procedural reliability, quality improvement, modeling and analysis, data analysis, migration to next-generation networks, and IP transformation. He has participated in the Network Reliability and Interoperability Council and the QuEST Forum. Prior to joining the communications industry, he worked on reliability projects for various industries such as power, chemical, manufacturing, aviation and space, marine transportation, and public safety. He led risk and reliability analysis projects at Delft University of Technology, The Netherlands. He received his Ph.D. in reliability engineering from the University of Maryland, his M.S. from Iowa State University, his M.Tech. from the Indian Institute of Technology, and his B.E. from M.S. University, India. He is currently serving as the Chair-Elect of the IEEE Communications Society Technical Committee on Communications Quality & Reliability.

JASON W. RUPE [SM] (jrupe@ieee.org) wants to make the world more reliable. He received his B.S. (1989), and M.S. (1991) degrees in industrial engineering from Iowa State University, and his Ph.D. (1995) form Texas A&M University. He worked on research contracts at Iowa State University for CECOM on the Command & Control Communication and Information Network Analysis Tool, and conducted research on large-scale systems and network modeling for Reliability, Availability, Maintainability, and Survivability (RAMS) at Texas A&M University. He has taught quality and reliability at these universities, published several papers in respected technical journals, reviewed books, and refereed publications and conference proceedings. He is a Senior Member of IIE. He has served as Associate Editor for *IEEE Transactions on Reliability*, and currently is its Managing Editor. He has served as Vice-Chair of RAMS, on the program committee for DRCN, on the advisory board for *IIE Solutions* magazine, and as an officer for IIE, QCRE division. He has worked at USWEST Advanced Technologies, and has held various titles at Qwest Communications Intl., Inc, most recently as director of the Technology Modeling Team, Qwest's Network Modeling and Operations Research group for the CTO. He has always been those companies' reliability lead. Currently, he is an adjunct professor at Metro State College of Denver, Colorado, and director of operational engineering at Polar Star Consulting, where he helps government and private industry to plan and build reliable network services. He holds two patents.