

Infrastructure Failures Could Help Revive the Optical Network Industry

John S. Mazur

Infrastructure failures like July's train tunnel fire in Baltimore show the vulnerability of networks to natural disaster — but they may also point to a significant opportunity for makers of disaster recovery technologies, such as optical switching equipment.

NEWS ANALYSIS

Event

On 18 July 2001, a fire in a Baltimore train tunnel destroyed a major fiber-optic cable installation. The loss of the cable halted or disrupted network operations (including Internet service) for enterprises in several parts of the East Coast of the United States. These services were not fully restored for at least five days.

Analysis

The disastrous Baltimore train tunnel fire highlights the vulnerabilities of communication networks to catastrophic infrastructure failures (see *Gartner FirstTake* "A Catastrophe Like Baltimore's Train Fire Could Disrupt Your Communications"). However, it also points to a potential increase in demand for technologies that can enable networks to recover rapidly from such failure — an increase in demand that could potentially help revive the moribund optical networking industry. The industry as a whole has declined largely because of the recent economic downturn and excess capacity. Demand has been slow for third-generation optical networking products, but the Baltimore disaster shows that certain types of these products — notably optical switches that can rapidly route communications traffic around problem areas — can solve serious real-world problems.

The total recovery effort in Baltimore took at least five days, but optical switching systems have become available that can help solve these problems almost instantly by switching traffic to different paths. Carriers deploying optical switches for these functions may actually come back into service before their customers know that a failure has occurred. Disaster recovery is more critical for carriers than for enterprises. Carriers' networks cross huge distances. The Federal Communications Commission also regulates them, and they may offer service-level agreements (SLAs), often promising "five-nines" (i.e., 99.999 percent) reliability. These factors leave the carriers little margin for error, so they need to mechanize their disaster recovery processes by using optical technology with stored program logic and control to avoid network meltdowns.

Enterprises, too, should prepare for catastrophic network failures. They should also ask their carriers what level of redundancy the carrier supports — ideally, a combination of equipment redundancy and route or path diversity — to ensure reliable service. Enterprises should also check their SLAs to determine whether they are entitled to refunds in the event of a network outage.

Analytical Source: John Mazur, Public Network Infrastructure

Written by Terry Allan Hicks, gartner.com

REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Level 7, 40 Miller Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Latin America Headquarters
Av. das Nações Unidas 12.551
9 andar—WTC
04578-903 São Paulo SP
BRAZIL
+55 11 3443 1509