

## From Disasters to Bankruptcy: New WAN Threats

*and How to Economically Protect Your Network*

### **Executive Overview**

*Wide area networks (WANs) are key elements of enterprise infrastructures because they provide connectivity to remote offices, backup data centers, business partners, and customers. The cost of WAN outages, which can range into the millions of dollars per hour, drives enterprises to invest in backup facilities to bypass WAN outages when they occur.*

*Recently, the level of threats to WAN availability has increased significantly causing more network managers to consider beefing up their WAN backup capabilities. Threats of cyberterrorism and the well-publicized problems of WorldCom and other telecoms have brought this about. Enterprises must consider the possibility that the performance of entire service provider networks might be severely degraded and some networks might even be shut down.*

*This white paper analyzes the potential impact of these new business threats and how they differ from traditional WAN outages. It also shows how Expand Networks ACCELERATORs can reduce the cost of WAN backup in this new environment.*

### **WAN Threats: Old and New**

Network managers have always had to deal with the possibility of WAN outages because the cost of downtime can have a severe impact of revenues, employee productivity, and customer satisfaction. Backup strategies have traditionally focused on bypassing problems caused by:

- Hardware/software problems
- Power failures
- Natural disasters
- Human error

These types of problems typically cause outages within isolated geographic areas and they impact a limited number of network routes. The outages also tend to be of short duration because the service provider can usually bypass or repair the problem quickly.

But what happens when an entire service provider network becomes unavailable or is severely degraded? Actually, this is not an entirely new problem. Network-wide outages in large service provider networks have been few and far between, but there have been some well-publicized examples including:

In 1998 the AT&T frame relay network went down because its backbone switches started sending erroneous routing messages to one another. This outage lasted two days and impacted some high-visibility customers, including a nation-wide ATM network.

In 1999, MCI WorldCom's frame relay network experienced widespread outages and performance problems over a ten-day period. The problems occurred during the

consolidation of MCI and WorldCom networks as MCI customers were migrated to the WorldCom network.

In 2001 AT&T's ATM network was severely degraded by a firestorm of network management messages sent by one of the network's backbone switches. The problem was corrected in less than one day.

Unfortunately, these types of network-wide outages are likely to become more common for several reasons. First, the economic problems in the telecom market have resulted in dramatic reductions in support staffs. It is estimated that over 300,000 telecom jobs were lost in 2001 and that trend has continued. Not only does this mean that there are fewer people to resolve problems, it also means that lead times to provision new services, including backup facilities, will be stretched out. Network managers will have to plan and provision their backup facilities well in advance

Another problem is that service providers have delayed capital expenditures to upgrade their networks. This could lead to more frequent outages due to aging equipment. In addition, the network consolidation that is likely to occur as a result of mergers and acquisitions may lead to more of the types of network-wide outages that were experienced by MCI and WorldCom customers in 1999.

And finally, the worst-case scenarios involve service provider bankruptcies that result in sudden service termination. An example of this possibility is the European KPNQuest network, which was abruptly shut down in 2002.

The bottom line is that both localized and network-wide outages may become more common and whether they are caused by technical, legal, or business factors, the impact on the enterprise is the same – lost productivity, lost revenue, and lost customers. Network managers have to build effective WAN backup into their infrastructures and they have to do it within severe budget constraints.

### *Two Backup Approaches: Route Diversity and Vendor Diversity*

The key to designing high availability networks is redundancy. When networks are configured with redundant resources, the workload of failed resources can be taken over by alternate resources, enabling network operations to continue.

Diverse routing is the traditional way of taking advantage of redundancy for users of connection-oriented WAN services such as frame relay, ATM, and private lines. These services can be provisioned with multiple diverse routes between Point A and Point B. Diverse routes are configured to use disjoint sets of resources including:

- Routers and switches
- Backbone links
- Central offices
- Access links
- Access nodes
- CSUs/DSUs

In addition, these resources are geographically separated whenever possible to avoid environmental problems that would otherwise affect resources on both routes. When an outage occurs on a primary route, the traffic is rerouted to a diverse backup route, ensuring that the failed resource is bypassed. Route diversity provides adequate protection when one or a small number of resources within a service provider network fail, but it does not provide protection from network-wide outages.

The AT&T frame relay outage in 1998 provides a good example of the limitations of route diversity within a single service provider network. At the time of the outage, AT&T offered several optional backup services that provided diverse routing. The problem was that all of the backup options provided rerouting through the same failed network and as a result they offered no protection from this outage.

The bottom line is that traditional route diversity does not provide adequate protection from network-wide outages. Protection from these outages requires vendor diversity, not just route diversity. Vendor diversity goes an additional step by employing diverse routes across two or more different service provider networks. This ensures that traffic will continue to flow even when an entire service provider network goes down.

Despite its advantages, vendor diversity has not been widely used as a backup strategy for several reasons. One is cost. When customers split their communications budgets across multiple service providers they lose some of the high-volume discounts that are typically associated with doing a single large deal for services. The second drawback of vendor diversity is the administrative overhead of dealing with multiple service providers. Today's lean networking staffs are already stretched thin.

Despite the cost and overhead, Gen2 Ventures believes that the current state of the telecom market will increase the probability of network-wide outages and enterprises should consider making vendor diversity part of their network backup strategy, at least for their most critical traffic.

## *Changing the Economics of WAN Backup*

There are no two ways about it, WAN backup is expensive because it requires redundant communications facilities. But it is possible to reduce the cost of network bandwidth, including backup facilities, by using Expand Networks ACCELERATORS to increase the effective bandwidth of WAN facilities. By enabling WAN links to carry an average of 100% to 400% of the normal amount of traffic with peaks of up to 1,000%, ACCELERATORS allow enterprises to reduce costs by provisioning less bandwidth on both primary and backup routes.

ACCELERATORS also provide a variety of benefits that ensure the performance and integrity of critical applications during normal network operations as well as in backup mode:

- Reduced packet loss and retransmissions
- Monitoring facilities provide application traffic visibility
- Delivers QoS by prioritizing critical traffic
- Works with all network protocols, not just IP
- Requires no changes to normal or backup network configurations

ACCELERATORS fit into virtually any enterprise network backup scenario.

### **Switched Backup**

Switched backup, or dial-around, is commonly used to backup private line, frame relay, or ATM WANs. When an outage occurs on a primary communication facility, a WAN router can automatically initiate a backup dial-up connection using any of the following switched facilities:

- Basic rate ISDN (128 kbps)
- Primary rate ISDN (T1)
- Switched 56 services (56 kbps)
- Analog (56 kbps))

These backup facilities are relatively inexpensive because their pricing is based on usage, which would only occur during outages on the primary network. Another benefit of switched backup is that enterprises may be able to purchase switched backup facilities from their primary network service provider and still be protected when network-wide outages occur in the primary network. This is because separate circuit-switched networks are usually used to deliver the switched services.

Expand's ACCELERATORS can be used to overcome the key drawback of switched backup, the fact that the speeds of low-cost switched services are limited to 56 – 128 kbps. When these services are used to backup higher speed primary links, users can experience very degraded performance. ACCELERATORS enable these backup links (as well as the primary links) to carry an average of 100% to 400% more capacity and provide faster backup service while taking advantage of the low-cost switched services. The ACCELERATORS can also prioritize critical traffic to ensure adequate performance over the backup links.

### ***Frame Relay Backup***

Frame relay customers often use redundant PVCs with diverse routing to provide backup services. Diverse routing within a provider network can effectively bypass most localized outages, but to ensure continued service during network-wide outages, the backup PVCs should be purchased from a different service provider.

The other frame relay network components that must be backed up are the local access links that provide connections to service provider PoPs. Like the PVCs within the frame relay “cloud”, diverse routing is also required for redundant access links.

The key problem with frame relay backup is its added cost. This includes the cost of additional PVCs, additional access links, and additional frame relay port charges. By using ACCELERATORS to increase the effective bandwidth of all of these elements, frame relay customers can reduce the CIRs of both their primary and backup PVCs. Similarly, they can reduce port speeds and the speeds of their local access links. The resulting cost reductions can help to offset the cost of backing up a frame relay network.

## ***Summary and Conclusions***

WAN backup facilities are an expensive but increasingly important part of enterprise networks. When Expand Networks ACCELERATORS are installed in enterprise networks they increase the effective bandwidth of both the primary and backup communications facilities. The combined cost savings can help to offset the cost of adding backup facilities to a network and make high availability networking available to a wider range of users and applications.

### **About Gen2 Ventures**

Gen2 Ventures, led by industry veteran Donald Czubek, is a leading analyst firm specializing in emerging technologies that accelerate and manage the performance of networked applications. Focus areas include network acceleration and QoS management, and Web server acceleration. Gen2 Ventures provides research reports, consulting services, and training to vendors, service providers, and enterprise IT clients.