Quick Eagle Networks

The White Paper Series

Safety in Numbers

Using Multiple WAN Links to Secure Your Network

Roger J. Ruby
Sr. Product Manager
August 2002

Intelligent WAN Access Solutions

Executive Summary

In the aftermath of the 9-1-1 attacks, more organizations than ever are placing preservation of their mission-critical data at the top of their IT priority list. Data security and disaster recovery are being taken more seriously today than ever before. Without building redundancy into network infrastructures, the transmission and storage of data is always going to be vulnerable.

This white paper will examine the use of multilink technology to create alternate transmission paths across the Wide Area Network (WAN) and so ensure that critical data is preserved. As a solution provider to many of the world's largest enterprises and service providers, and the world leader in multilink solutions, Quick Eagle Networks is ideally placed to look at how this can be achieved. Specifically, this white paper will discuss:

- WAN data path redundancy between remote sites and a data center
- Automatic routing of data from a primary to a back-up data center
- High availability solutions with redundant data paths and back-up data centers

WAN Path Redundancy

First, we need to understand the basic principle behind multilink technology. By taking multiple WAN links (such as T1 or E1) and treating them as a 'logical bundle', multilink is able to create a higher bandwidth connection without the need for deploying an expensive link like T3 or E3. Data is simply split ('inverse multiplexed') across the multiple links, and then reassembled at the other end of the network.

The following paragraphs discuss the primary advantages of multilink technologies such as:

- Inherent redundancy,
- Automatic link recovery,
- Diverse routing between endpoints.

Inherent Redundancy

In its simplest guise, multilink technology, also known as NxT1 or NxE1, is all about deploying multiple WAN links to a single destination and so, inherently, it provides a level of redundancy for the network. If a link fails, it is temporarily removed from the logical bundle by the multilink protocol, and the remaining links continue to carry traffic, albeit at a reduced bandwidth. The inverse multiplexer device will signal the customers' access device - usually a router - that there is reduced bandwidth available on the WAN and the router can lower its WAN port speed accordingly.

Automatic Link Recovery

In many cases, the customer may be unaware that there was a faulty link. Inverse multiplexers have the ability to continually assess the status of a failed link and automatically place that link back into the bundle once it is capable of passing data. At this point the device will signal the router to send and receive data at the higher WAN speed, equivalent to the aggregate speed of the links that are fully operational.

Diverse Routing Between Endpoints

Inverse multiplexers can be used to build a diverse routing topology solution, as an added measure of reliability. Putting the digital circuits through different cables and intermediate central offices will dramatically reduce the possibility of a catastrophic failure of the entire multilink bundle. Figure 1, below, illustrates this approach.

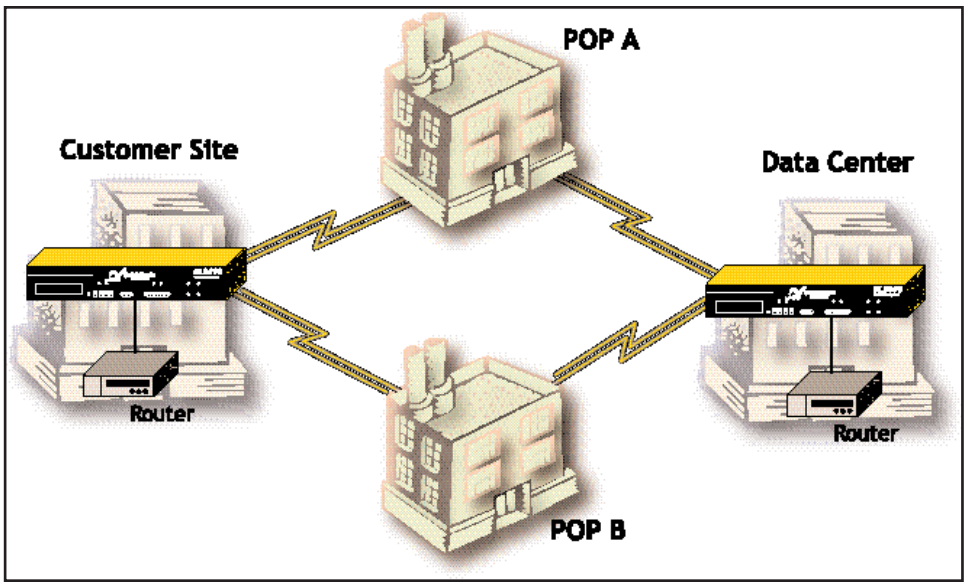

Figure 1 - Diverse Routing Topology

In this inverse multiplexed arrangement, the data is spread out over multiple links that take two different physical paths. Since no one “bundle” carries the entire payload, it makes it virtually impossible for the data flow to be totally interrupted or compromised. The primary goal of getting the data delivered, end to end, with a minimum of disruption is therefore achieved. The only trade-off in this scenario is that, should one bundle be lost, the speed of data transmission would be halved.

Alternate Routing to a Secondary Redundant Data Center

The previous discussions focused on scenarios that involve failure of a point-to-point transmission path. This section will explore a methodology that supports the re-routing of critical data to a back-up data center. Consider a bank or brokerage firm that absolutely must keep up-to-date financial transaction records on a real-time basis. The margin for error is virtually zero. Many enterprises in this market segment elect to set up redundant data centers so that, if their primary data center goes 'off-line' or suffers from a catastrophic failure, a secondary data processing facility can take over.

Single Link Standby Solution

The premise behind a single link standby solution is that, during normal operations, a remote site is connected to a primary data center but, if that data center should fail for any reason, the remote site becomes automatically linked to a backup data center. This topology is shown in Figure 2, below.

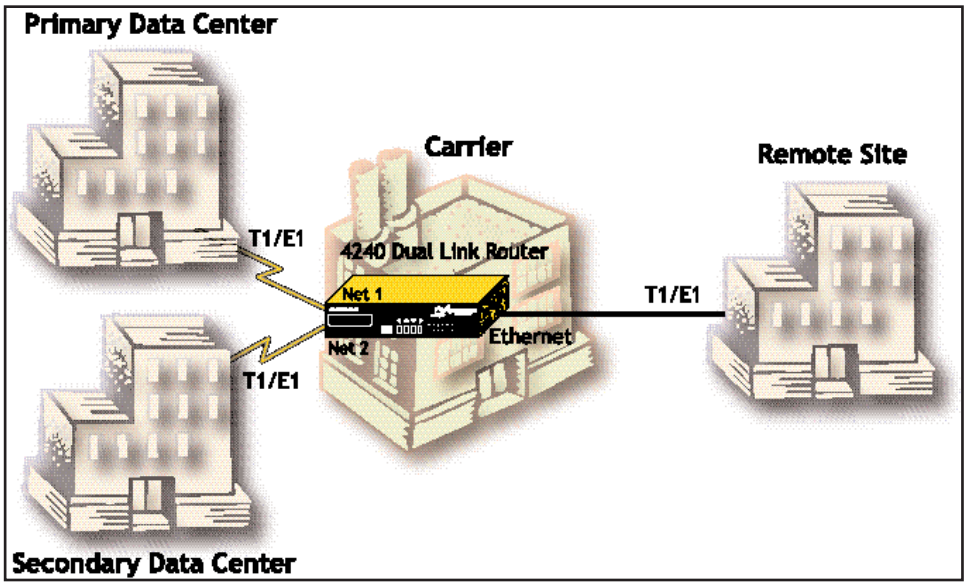

Figure 2 - Single Link Redundant Data Center Solution

In this scenario, the access device at the remote site is a 4240 Dual Link Router from Quick Eagle Networks. This device uses a unique protocol to monitor the status of the primary data center and enable cutover in an emergency situation.

Multilink / Multiple Bundle Solution

It is also possible to combine the increased bandwidth capability of a multilink solution with the link standby feature discussed in the previous section. Figure 3 depicts a multilink redundant data center scenario with NxT1 capability.

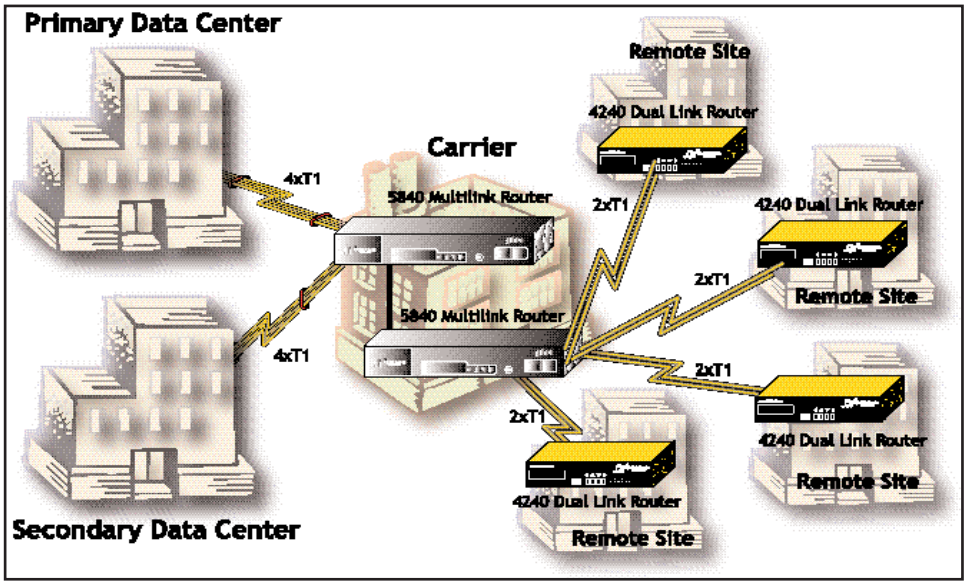

Figure 3 - Multilink / Multiple Bundle Solution

The only difference with this configuration is that instead of having a device with two WAN links at their Central Office, the carrier would opt for an NxT1/E1 device, such as the Quick Eagle Networks 5840 Multilink Router. Using multilink capability, the user can partition two or more logical bundles to reach multiple data centers. The figure above shows a topology using two logical bundles of four links each. It also shows how multilink / multiple bundle technology enables another 5840 device to be used as an 'aggregator' at the edge of the carrier's network.

High Availability with Diverse Routes and Back-Up Data Centers

A combination of the previous solutions would result in the most reliable topology for an enterprise that relies on 100% availability of data access and acquisition. Figure 4 illustrates the solution that protects the customer site from both total facility failure and from the loss of the primary data center.

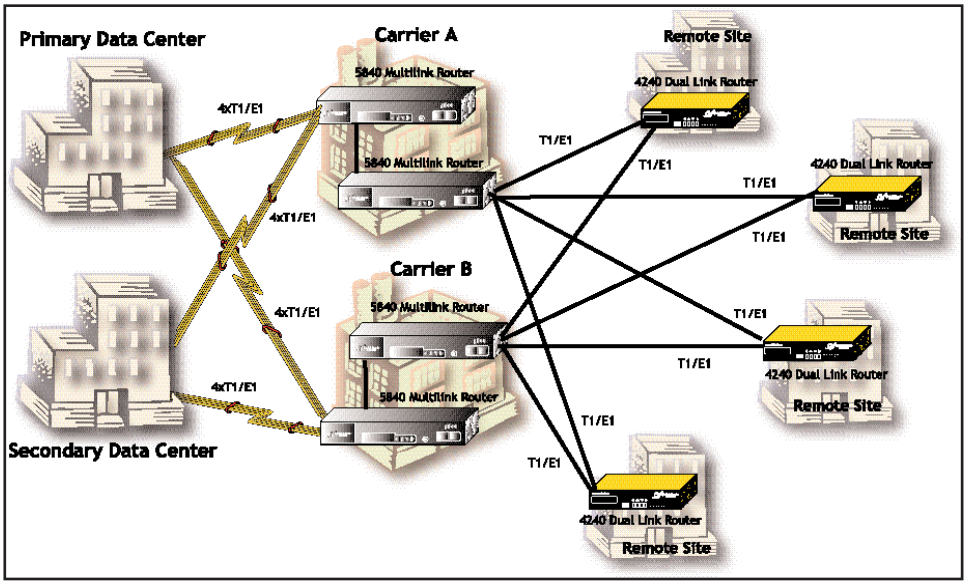

Figure 4 - Redundant Link / Redundant Data Center Solutions

This would be typical of an application that requires both a redundant path to reach multiple end points as well as full redundancy of the data for complete disaster recovery. In any of the previously described topologies - with back-up data centers - it is possible to create site mirroring by simultaneously routing to both primary and secondary end points. In this case the secondary link is not just used when the primary link becomes unavailable.

Summary

Preventing data loss and being able to recover quickly from serious outages are issues on the minds of IT Managers all over the world. Link redundancy and backup data storage facilities provide a compelling way of protecting the data networks of global organizations. Deploying a tried and trusted technology like multilink in one of these new security-oriented applications can provide you with a scalable, flexible, and cost-effective solution with which to survive the dynamics of our new world.

About Quick Eagle Networks

Quick Eagle Networks, Inc. is a provider of intelligent WAN access solutions for Frame Relay and IP networks, and the world leader in multilink access devices. The company's fully software-configurable IP access products and network management solutions provide expanded functionality for reduced cost at the LAN / WAN interface. Founded in 1985 and recognized worldwide for its Digital Link and Quick Eagle brand products, the company serves many of the world's leading enterprises and carriers including Boeing, Wells Fargo, MCI/WorldCom, Sprint, British Telecom, Bell Canada, and France Telecom. Quick Eagle Networks is an ISO-9001 certified company, with headquarters in Sunnyvale, California and sales and distribution offices worldwide.

For more information about Quick Eagle's full range of WAN access solutions visit our website at www.quickeagle.com or email info@quickeagle.com.