Thinking About

MPLS Network Backup Solutions

Looking back a few years, designing a secure, reliable corporate data network was a little simpler than it is today. If the average Frame Relay remote end point was 64 kilobits, analog dial modems could be deployed at all remote sites. If there was a failure of any nature, whether last mile access or anything in between, the remote sites would detect loss of "LMI" (Local Management Interface) and automatically phone home.

For better support, the concept of "dial around the cloud" could be implemented. In this scenario, a completely separate dial router "catcher" platform could be set up, and in the event of a network failure the remote sites would dial into the head end or disaster recovery vendor site modem bank on separate facilities.

The customer (or management supplier) had the ability to dial into remote routers/CSUs, and get "out-of-band management" (like the Cisco SAFE Blueprint) capability. Utilizing strong passwords and dial-back capability, the user had network reliability and full security at the same time.

According to Erik Westgard, a technical consultant with AT&T, "Modern applications, the Internet and MPLS (Multi Protocol Label Switched) networks have changed the above models. Now, networks often require bandwidth of T1 or better at remote sites. There may be a mixture of Internet traffic as well as the need for a full site mesh to support Services Oriented Architecture models, where layered application services may be located all over the enterprise. Analog dial (even ISDN in some cases) is just not enough bandwidth for a credible backup path."

Enterprises today have a richer range of applications, including voice, streaming media and web services. In spite of this new traffic, the threats and risks to networks have remained similar from a failure standpoint:

- Last mile outages are typically cable cuts, water damage or equipment failures
- Carrier access issues could include a central office power outage affecting a local or regional area
- Head end outages, whether datacenter or carrier related, such as the loss of a major node, fiber equipment or a datacenter
- Larger scale carrier outages, such as routing storms

The accepted rule of thumb has been to cover network outage risk by protecting the last mile. Analog dial was a reliable alternative, as long as the same cable was not followed or a different central office from the one providing the primary circuit is used. ISDN (Integrated Services Digital Network) was another good alternative, as it was reasonably fast, had good call setup time, and often went over diverse facilities from ILEC Frame Relay.

Erik Westgard points out that, "Organizations with regulatory pressures for true business continuity, such as large banks, have had to think 'big picture' on reliability, so they are moving beyond just last mile issues. If mandated uptime is needed over a network of T1s to 500 locations, a comprehensive plan should be developed."

There are three types of comprehensive backup solutions that enterprises can consider:

1. Carrier Options

The first type of backup solutions includes the options that carriers have provided in the past. These can include flavors of last mile access diversity, central office diversity and ranges of Point of Presence (POP) (Provider Edge Router for MPLS users) and routing node diversity. These options can provide good coverage for a number of outages. Care needs to be taken by the customer in areas like power protection and dual building cable entrances to help to ensure these options have the maximum benefit. Customers can also consider the risk mitigation from duplicated equipment at the site, such as dual routers and or CSUs. Redundant local access could include diverse types of technology back to the same carrier network, such as WiMAX.

MPLS carrier networks have one inherent feature that can make backup for site failures easier than say Frame Relay. In a fully meshed MPLS network, all sites can be part of the same address space. So if a site is

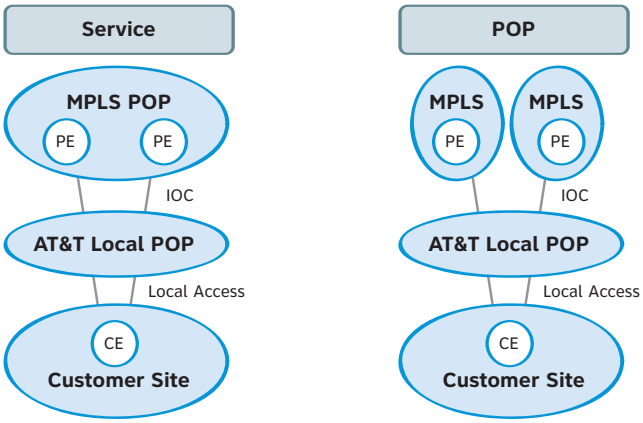
at&t

lost, businesses do not have to worry about where the Frame Relay PVCs (Permanent Virtual Circuits) are routed physically. Each site on the network has an IP address, and users can re-route easily to a secondary site. Datacenters on the same MPLS network can use IP routing to back each other up.

Figure 1 – MPLS Service Backup Options

Service Diversity – Each group of MPLS Ports provisioned to a different network switches or routers in a POP.

POP Diversity – Each group of MPLS Ports provisioned to a different POP



2. IPSec Tunneling

Another choice for backup is to bring in a second VPN technology that will provide a unique backup network to protect against local access and even network facility failures. One popular choice is the use of the Internet and IPSec (IP security) tunnels to provide network backup. A fully-managed version of this is provided by the AT&T AVTS High End Site-to-Site (S2S) Offer. If this service is selected with "3rd party/bring your own" Internet service (from a completely different carrier end to end), users can gain additional levels of separation and failure protection. Having this service managed provides defined processes and techniques to ensure the backup network is fully secure and continuously monitored. Regular testing of such a solution is also required.

The latest generation of VPN routers can provide full mesh connectivity between sites even over broadband using technology like Cisco's DMVPN (Dynamic Multipoint VPN).

One variation on using an Internet based solution is to go to a different type of network carrier for the second network. Options here include wireless carriers, who might offer services like "3G/Edge/etc" high-speed wireless, or the use of VSAT (very small aperture terminal – used in satellite communications) as a service option. Legacy networks such as private line, Frame Relay or ATM can also be used for backup. These backup options can be helpful across a wide range of failures if private line, SONET or other types of older non-layer 3 backbones are used.

Each solution has benefits and trade-offs. Wireless or VSAT solutions might be used in "fail-over" type designs, where an Internet or legacy (Frame) solution might be employed in an "active/active" model with traffic sharing across both networks.

3. Dual MPLS

A third backup choice is to implement a full dual-carrier MPLS solution. This is the highest cost, but can provide a reliable and highly secure solution. Normally, these networks are implemented as an "active/active" model, where the load is shared, but each network retains the capability to handle the entire load. One advantage of dual MPLS networks vs. using an Internet option is the ability to retain end-to-end, bi-directional QoS (quality of service) markings and support. This may be difficult or impossible to achieve across random topology. The dual MPLS backup design may be complicated, as carriers can use different QoS marking conventions.

In a dual carrier active/active network, businesses may be able to achieve shorter convergence time. In simple dial backup solutions, loss of LMI /carrier was often used to trigger the backup. In similar solutions on MPLS, the user might receive an LMI failure, or the user might have to rely on high-level routing protocols to detect loss of routes. This raises the design issue of convergence time or how long it will take for the network to detect failures, and activate the alternate path. One consideration is that this fail-over has to be carefully designed to avoid route flaps, which could also disrupt services.

Figure 2 – Using AVTS High End S2S as Backup via Internet

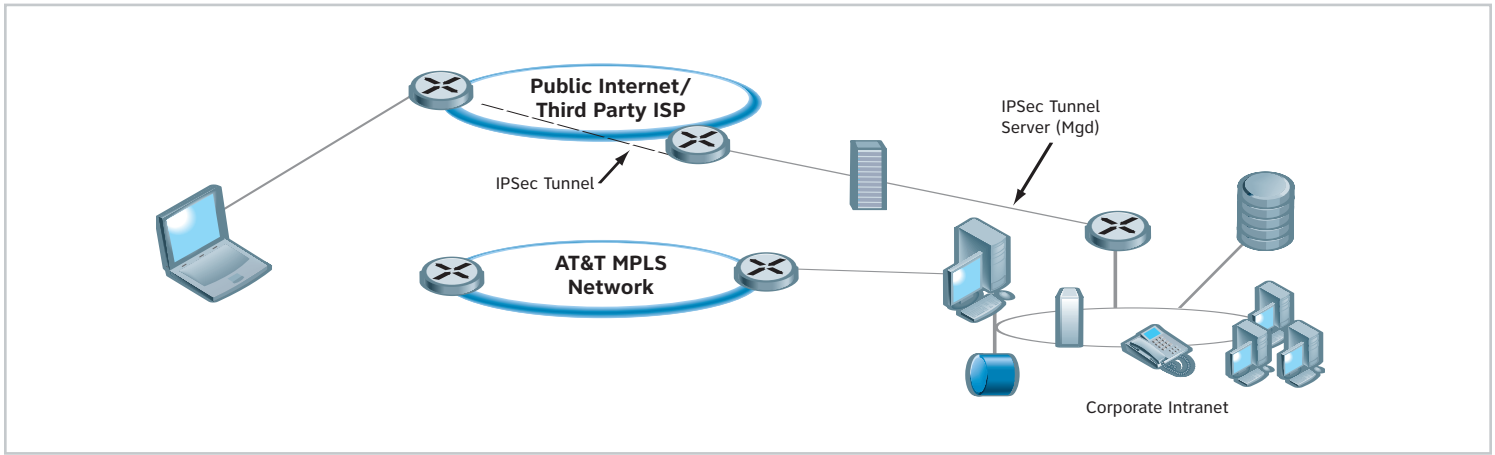
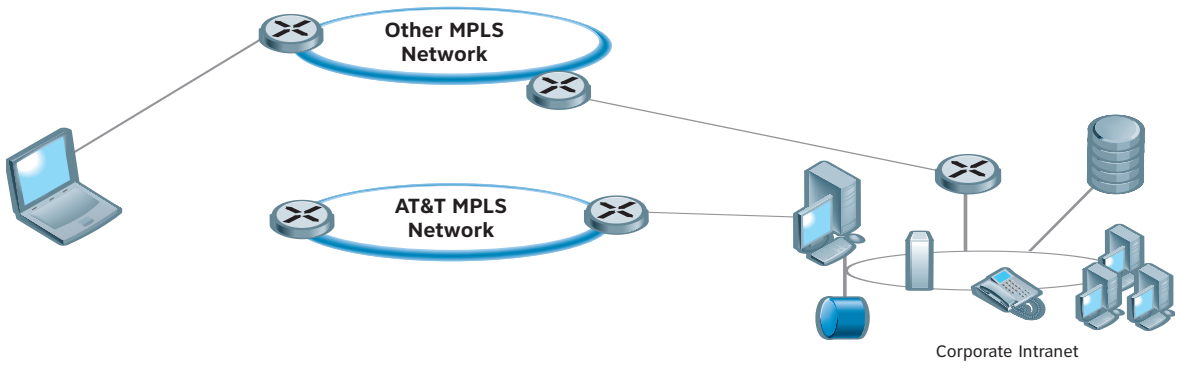


Figure 3 – Dual Carrier MPLS Solution



In a dual carrier network, users might start at a few minutes for convergence time, and be able to get this time down to under a minute or lower.

Table 1 - Backup Solutions Comparison

	Carrier Options	IPSec Tunneling	Dual MPLS
Secure	X	X	X
QoS	X		X
Last Mile	X	X	X
Full Failure		X	X
Cost	$	$$	$$$

Another advantage of a dual MPLS network is the need to support modern streaming and voice applications. Voice, in particular, has a very low tolerance for packet loss. The backup design for voice might have to include fail-over to the public switched telephone network via MPLS to take recovery time and 911 access into consideration.

Erik Westgard suggests that, "Today's enterprises need to consider redundancy and backup as part of their business plans. Both natural disasters such as Hurricane Katrina and man-made events such as 9/11 highlight the need for this type of planning."

Businesses can utilize Table 1 as a starting point for their backup plan.

Customers looking for in-depth advice on backup network designs can utilize their AT&T Technical Consultants, who can help design an optimal business continuity solution, or engage AT&T Network Integration and Professional Services to assist with the design and development of a network backup plan.

For more information contact an AT&T Representative or visit www.att.com/business.

at&t Your world. Delivered.