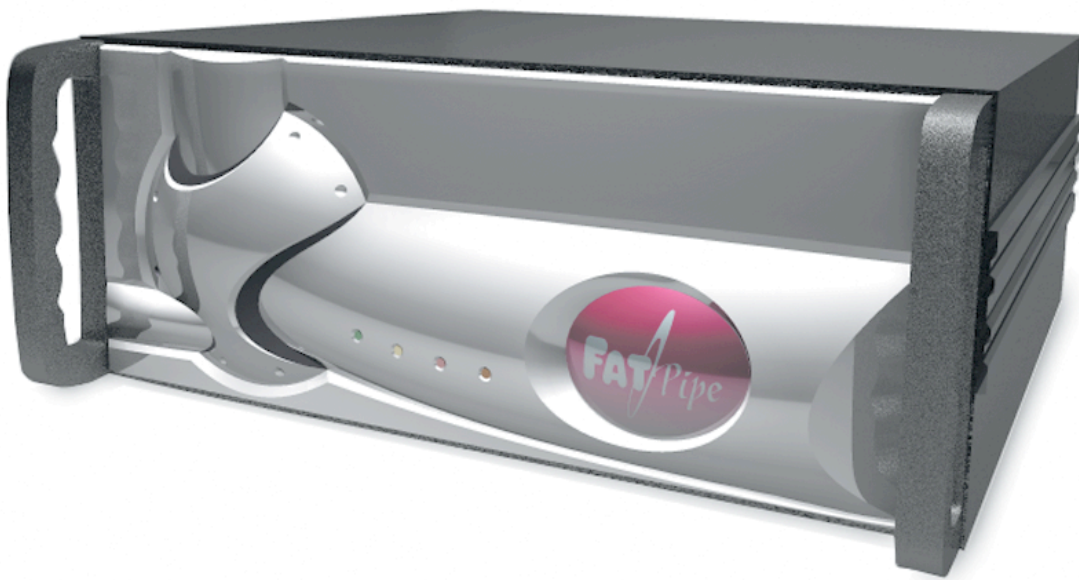




BUSINESS CONTINUITY THROUGH WAN REDUNDANCY



A FatPipe Networks White Paper

4455 SOUTH 700 EAST, SALT LAKE CITY, UT 84107
800-724-8521 • WWW.FATPIPE.COM

WIDE AREA NETWORK (WAN) REDUNDANCY: A KEYSTONE FOR BUSINESS CONTINUITY

The Internet plays a vital part in business activity in today's markets. Companies require viable Internet/Wide Area Network (WAN) connectivity in order to succeed in an increasingly competitive and global business landscape and to insure that business is not interrupted. This paper explores how companies use the Internet and other types of WANs to conduct day-to-day functions that help employees, customers, partners, suppliers and investors. The paper will also review recommendations of what companies need to implement to keep their WAN infrastructures highly available, secure and efficient.

The first part of the paper gives a general overview of how WANs are utilized in businesses today and the importance of WAN stability and accessibility within a business framework. The second half of the paper defines how FatPipe technology can greatly assist businesses by resolving their WAN bandwidth issues and eliminating WAN downtime. Customer scenarios and case studies are included to illustrate implementation for better understanding of application in business.

GROWTH TRENDS FOR WANS NEEDS

The growth of the Internet has spawned a variety of new business that is based around a cyber model rather than the traditional brick and mortar fixed location model. This is very pronounced in the retail sector where cyber stores have mushroomed and taken significant market share from traditional stores. Traditional stores have fought back by moving to a hybrid model that has both the traditional and the cyber model. The cyber model is considered as another sales outlet and in most cases the two are kept separate on the front end, but share many of the backend systems such as payroll, supplier payments, order placing, Enterprise Resource Planning (ERP), etc.

Medium to large size businesses have improved communications and increased productivity by implementing web-based applications that streamline day-to-day

business activities, improve customer service using online customer service tools, and strengthened their relations with partners and remote office locations using ERP that integrates processes and data into a more unified systems. These systems require robust and secure WAN infrastructure that is of a high availability nature. To attain this, companies need to create and execute WAN Redundancy planning as part of their overall business strategy, ensuring a stable means to communicate via the Internet. WAN Redundancy is essential if a business is to stay in a Business Continuity mode.

BUSINESS CONTINUITY AND THE IMPORTANCE OF WAN REDUNDANCY

Back in late '90's and early 2000's, the implementation of WAN Redundancy and Disaster Recovery plans were far and few between. They were reserved for only the largest corporations who had the cash on-hand. They were viewed as luxury strategies for most small and medium sized companies. It was not until on one of the worst days in American history, September 11, 2001, that importance of WAN Redundancy and Disaster Recovery was brought to the forefront and quickly viewed as practices that in the near future should be universally applied to business. These related issues were discussed frequently at that time because many businesses that were headquartered in New York City were not only devastated by the impact of a terrorist attack, but also paralyzed by downed data and voice services for days, weeks and sometimes more than a month.

The WTC housed one of the largest Telco switching centers in the United States - a major Point of Presence (POP) - in its basement. When the buildings were destroyed, several of the centers went out immediately while some continued functioning for a few more hours on battery power. Businesses that had single data lines and no WAN redundancy had their WANs compromised and unavailable immediately, proving to be detrimental to their ability to conduct business. Business that had planned for WAN failure and incorporated WAN Redundancy into their strategy -- including utilizing more than one ISP -- had a backup line as an alternative data path.

Events such as Katrina and the Tsunami in Asia brought the need for WAN Redundancy back to the front position of business discussions, and IT organizations started organizing workshops and conferences around WAN Redundancy.

Although most people will not directly experience a terrorist attack or a horrific natural disaster, it was these large and devastating events that helped open the discussion and analysis of the importance of Disaster Recovery and Business Continuity. It is essential that businesses plan for such large scale disasters. However, these in most instances, are once-in-lifetime events. The most common disruption to business activity in this context is WAN failure. Addressing the issue of WAN Redundancy is crucial to companies that run mission critical, web-based applications for business and at the same time mitigate a common cause of failure.

In the early 2000's, the cost of data lines was high, and WAN Redundancy, while desirable, was not affordable. Hence many -- especially SMBs -- forwent the induction of WAN Redundancy and took risks that in some cases led to the demise of businesses and for others proved to be a costly experience. Over time, WAN Redundancy has gained prominence in IT infrastructure planning and has taken its place among the top considerations when planning IT infrastructure and strategies.

NEED FOR HIGH AVAILABILITY WAN INFRASTRUCTURE

The global economy has led to a flattening of the business world and geographic boundaries have fallen to a great extent. No longer does a country's physical boundary pose an insurmountable barrier to entry as it did in the decades following WWII through the early 90s. The driving forces for this were the IT revolution and the signing of many bilateral and multilateral free trade agreements among nations. These have suppressed boundaries as barriers and the availability of information, and the ability to distribute data over the web has hastened these trends. Thus, businesses have to ensure they are constantly creating value for customers by driving costs from their operations. This takes several forms such as relocating manufacturing to low cost, high efficiency parts of the world, outsourcing non-core operations (e.g.: payroll, programming), etc. The ability to do this is tied to the health of businesses' WANs, creating the information highway

that connects various business operations together and also cements the relationship between customer and business.

Lack of a Business Continuity Plan is fraught with the danger of having a business vulnerable to various interruptions. From a data perspective, businesses that plan for disasters improve their chances of recovering very quickly, while those that do not have a plan scramble in panic. Those that are unprepared lose money and customers and oftentimes suffer irreparable harm to their reputations. A few key Business Continuity concerns are listed below.

- Bandwidth Management *
- Server Accessibility *
- Cyber Criminals
- Pandemics
- Terrorist Strikes
- Transportation stoppage
- Bandwidth Reliability *
- Network Recovery *
- Network Security *
- Staffing
- Natural Disasters *
- Data Storage *

A Business Continuity Plan, from a protecting data planning perspective, calls for Data Mirroring, Off-Site Data Storage, and WAN Redundancy. Data Mirroring and Off-Site Data Storage are required to handle emergencies such as 9/11, Katrina, Tsunami, and other rare but catastrophic events.

Of the three mentioned above, WAN Redundancy is the most critical because it happens most frequently. Intermittent WAN failures and disruptions happen often enough they have to be taken into account when developing a Business Continuity Plan. It is estimated that WAN Redundancy will take care of 35% of all Business Continuity concerns. Thus a small effort in the area of WAN Redundancy has a big payback.

ESTIMATING THE COSTS OF WAN DOWNTIME

Estimating the cost of WAN downtime and the extent of the investment needed for WAN Redundancy to offset this is not always straightforward, but several studies have been done to gauge the effect of WAN downtime. An Infonetics study in 2004 estimated that large companies

on the average have their WAN down 500 hours per year at an estimated cost of approximately \$4 million annually. Another estimate put out by Gardner research indicates the hour cost of downtime to be \$42,000 with companies averaging approximately 87 hours of downtime per year. This puts the estimated revenue loss at \$3.6 million.

A study conducted by Beacon Technology Partners published that about two-thirds of executives from fortune 1000 companies feel their companies do not have sufficient WAN redundancy plans, even though there is widespread acknowledgement of the importance of ensuring uninterrupted service.

Other research studies point to different numbers, but the bottom line indicates that in today's global economy, WAN downtime results in significant loss of revenue, productivity and opportunities, making WAN Redundancy an imperative.

There are a couple of ways to look at the cost of WAN downtime can be calculated in Productivity Losses and actual Business Losses, or loss of revenue.

Lost Productivity

To calculate productivity losses due to WAN downtime, the average hourly cost of wages including overhead must be calculated. This can be determined by dividing the total annual payroll divided by the number of working hours per year (typically about 2000 hours). This number is the average hourly cost of labor at a site.

Example Company:

- 1000 employees
- \$50 million annual wage bill
- 2000 working hours per year
- Annual company profit \$100,000,000
- Average hourly labor cost = $50,000,000/2000 = \$25000$
- Assume 100 hours of WAN downtime and 50% of labor are negatively affected

Average productivity loss = $100 \times 25000 \times 0.5 = 1,250,000$ per year

Business Losses Due to WAN Downtime

To determine the business losses due to WAN downtime, the following must be calculated (using the same company data as in the previous example):

Average profit per employee – this is determined by taking the total company profit and dividing this by the total number of employees. To calculate this, divide this by 2000 to get average hourly profit per employee. Determine the number of employees affected by the downtime and the percentage of their work affected during the downtime.

To calculate the business losses:

- Average hourly profit per employee = $\$100,000,000/1000/2000 = \50
- Loss for 100 hours of WAN downtime = $100 \times 1000 \times 0.5 \times 50 = \$2,500,000$

Total loss due to WAN downtime = \$1,250,000 + \$2,500,000 = \$3,750,000 per year

This does not take into account opportunities lost, loss of customer goodwill, etc., which adds an invisible tab to this amount. The point is that the numbers associated with WAN downtime is significant and investment in WAN Redundancy pays back in a relatively short time. Some other numbers estimated for various industries by several research organizations indicate the following losses by industry per hour of WAN downtime:

- E commerce \$600,000
- Customer service = \$222,000
- ATM/POS = \$210,000

These are very large numbers that easily justify investments in WAN Redundancy.

CAUSES OF WAN DOWNTIME

WAN downtime is a serious problem that affects most business immediately because it is unexpected. The frequency of occurrence is hard to predict but several problems associated with a variety of causes can be eliminated or prevented by introducing WAN Redundancy into the Business Continuity strategy. The following is a list of common causes for WAN downtime.

Many others -- with varying degrees of effect on WAN availability -- are not listed, but it should be noted they do exist.

ISP or Telco Failure – problems in ISP and Telco networks can cause WAN downtime and oftentimes are the common blame point for non-availability of WANs. However, over the years, this has taken a catchall meaning and any un-attributable WAN downtimes are lumped in this category. WAN Redundancy, through the use of multiple carriers at any facility will resolve this problem satisfactorily (see WAN Redundancy technology).

Hardware Failure – failure of hardware such as routers, switches, etc., can result in WAN downtime. Regular maintenance can reduce the number of failures and having “hot” spares on hand can reduce downtime to minimal levels.

Natural Disasters – this is an area that can have potentially very serious effects on Business Continuity. Major natural disasters like Katrina or the Tsunami can not only wipe out the Wide Area Network, but also can wipe out the entire office. WAN Redundancy may not work if all lines go down or if there is a total blackout. In this case, a site-to-site failover solution would be applicable. Site-to-site failover provides failover to a different location if the main site is incapacitated.

Human Error – WAN downtime can be caused by human error. Many times the error is in the setup stage itself. To ensure WAN Redundancy, all settings of different equipment should be checked thoroughly and tested under simulated conditions.

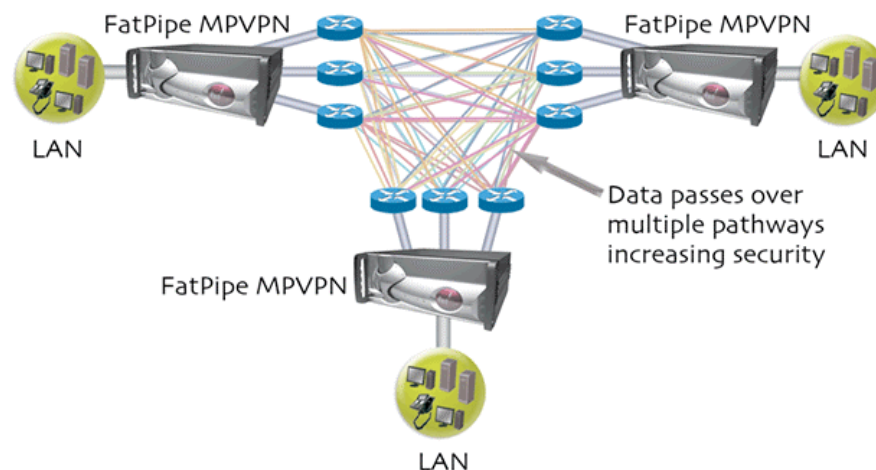
Terrorism, employee sabotage, corporate sabotage, etc., – this is very hard to prevent, but WAN Redundancy via off-site data storage and DR sites can mitigate the effects of this.

SECURITY

As the volumes of data moving across WANs continue to increase, security of data is a growing concern. There is a strong recognition that this aspect of network infrastructure is vital to any business' health and well being.

Data security has many facets. The most obvious is to ensure that data is not stolen when it moves across the public Internet. The problem of securely moving data over the Internet was solved using Virtual Private Network (VPN) technology. This technology establishes secure tunnels between senders and receivers and encrypts data packets.

Breaking the encrypted dataflow is very difficult but determined hackers have done it. Technology is available that enhances security and also provides WAN Redundancy. For example, FatPipe Networks markets a device designed for existing VPN infrastructures called MPVPN, which aggregates multiple data connections to achieve high levels of reliability, redundancy, security and data transmission speed. Its patented technology, MPSEc, adds an additional layer of security above encryption, by breaking down encrypted data to the packet level, randomly sending the packets over the multiple connections, where they are reassembled on the other side with virtually no latency. A hacker would have to get hold of all data lines, trap the data, put it in the correct sequence and then break the encryption, an almost impossible task.



Other areas of security involve employees keeping a post open on a network, thus allowing intruders access to the network. Stolen laptops, data disks, etc., have also played a significant part in the breakdown of security. Even if the WAN is secure, such actions by employees can trigger a massive breach of security with sensitive data being lost. A corporate procedure that minimizes these possibilities is very desirable. Password protected laptops and well guarded data storage devices all have to form a part of the security regime in place.

The most insidious form of breach of WAN security is that caused by malevolent actions of past and present employees. This is oftentimes very hard to prevent but careful scrutiny of employee online actions, background checks and constant monitoring can minimize this. In some business, data security is of such concern that all LAN devices have disabled copying capabilities and in some cases employees are not allowed to take writing materials of any sort into secure rooms. Special clothing without pockets is also a technique used by some firms to enhance data security and it is within the gamete of WAN security.

WAN REDUNDANCY TECHNOLOGY

WAN Redundancy is a cornerstone of strategic imperatives that govern Business Continuity decisions. While Business Continuity concerns tend to place a heavy emphasis on the large-scale disasters, these occur very rarely but nonetheless need to be taken into account. However, a much more frequent occurrence that affects Business Continuity is WAN downtime. As we mentioned before, it is estimated that introducing WAN Redundancy to networks eliminates as much as 35% of Business Continuity concerns.

There are several paths to WAN Redundancy. The most basic form is to have a shadow or dark line to be used in case of failure of the primary line. However, while this may save on some initial costs, it is inefficient and requires manual handling. If no technically competent person is on hand, the resulting WAN downtime could be exorbitantly costly for a business due to the delay of failover. Other choices include are Border Gateway Protocol and Router Clustering, which are explained below.

Routing Protocols

BGP is one of the main routing protocols used in the Internet, but other routing protocols are also used to achieve WAN redundancy, including EIGRP and OSPF. They utilize complex sets of routing tables of IP networks, which maintain network connectivity between WAN networks.

In particular, BGP's use of routing protocols makes it a very difficult to deploy technology for WAN Redundancy. The programmable router used to attain WAN Redundancy has to have sufficient memory and processing power to hold the ever expanding list of routing tables that are necessary for proper operation. Additionally, routing protocols are very complex and require

people with specialized expertise to set it up. Since most companies do not have routing experts on staff, outside consultants have to be relied upon and thus increased the expense of deployment.

Routing protocols are traditionally not applied to DSL or cable. (Note: BGP is not supported on DSL or cable lines). and most wireless providers will not support routing protocols. Furthermore, unlike FatPipe, when implementing a failover solution using routing protocols between two or more ISPs using BGP, providers must have a peering agreement. ISPs can refuse to work with (peer with) a competitor and they can refuse to peer, creating a single point of failure.

While BGP does provide for WAN Redundancy, some of the concerns are:

- Implementations needs expert BGP programmers
- Require routers to be upgraded to programmable ones with maximum memory
- Can “weight” traffic, but there is no dynamic load balancing
- Needs ISP and Telco cooperation, especially when using one or more ISPs to achieve WAN reliability and redundancy
- Needs high level programming
- Changes to the network need more programming

WAN Redundancy Technology – Router Clustering

Router Clustering is a relatively simple solution to automate WAN Redundancy. It is based on the principle of combining multiple Internet connections from multiple ISPs or Telcos through a router clustering device that sits on the edge of the LAN.

Router clustering technology will combine multiple data lines from multiple providers without the need of their cooperation or permission. No setup is required at the ISP, either. The technology is agnostic to type of data line or WAN, and also towards the ISP or Telco providing the service. Thus, this technology can combine any combination of lines whether the same or disparate data lines such DSL, ISDN, T1, DS3, E1, Cable Modem, Wireless, etc. In fact, router clustering devices can handle any type of data line that terminates in a router and has an Ethernet handoff or is Ethernet itself. Since this technology is not dependent on the providers doing anything on their networks, it is very versatile and can be used in a variety of WAN configurations.

A natural extension to this router clustering technology is to extend it to other WAN connectivity types such as VPN, Frame Relay, ATM, IPVPN, and Private Point to Point Networks. Thus, router clustering technology provides WAN Redundancy for simple Direct Internet Access (DIA) connections and to sophisticated networks such as VPN, Managed Services, Private Networks, and can also combine private and public networks, as well.

The main advantages of Router Clustering Devices are:

- Easy to deploy
- Dynamic and intelligent load balancing
- Does not need ISP or Telco cooperation or permission
- Works with multiple types of data lines and WAN connections
- Simple GUI interface
- No command-line programming
- No change to Router Based protocols, including BGP, HSRP, VRRP, EIGRP, and OSPF
- Additional policy routing tools
- Additional security tools

FATPIPE ROUTER CLUSTERING PRODUCTS

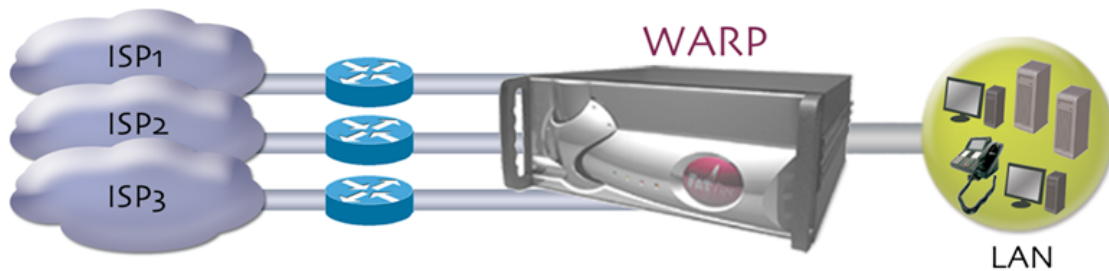
FatPipe offers different and flexible solutions for all types of WAN infrastructures. All products come with core benefits, including reliability, redundancy and speed for outbound IP traffic, policy routing tools for efficient data flow, and remote monitoring capabilities. Advanced features include redundancy and high availability for inbound traffic such as email, redundancy of Voice traffic using Voice over IP, QoS, compression, and additional security of all data traffic.

FatPipe WARP is a router-clustering device that combines multiple WAN connections of any kind over multiple backbones and ISPs (or the same ISP with different POPs), to provide the world's highest level of reliability and redundancy for inbound and outbound IP traffic. Businesses can host servers internally with the highest degree of availability.

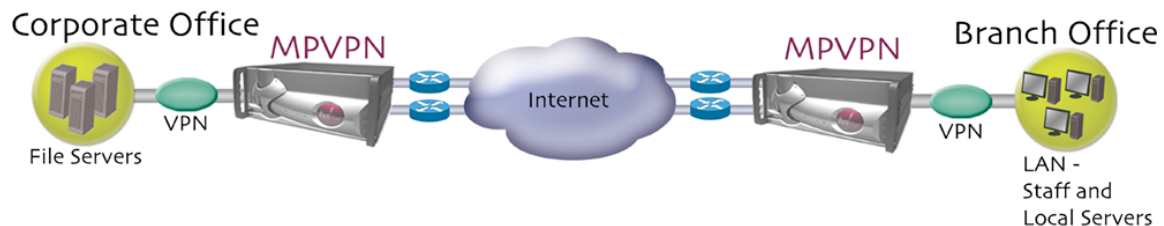
FatPipe WARP technology significantly enhances the ability to maintain the integrity of Wide Area Networks (WANs). Basic product features such as dynamic load balancing and intelligent, automatic failover capabilities substantially increase the efficiency of WANs.

Advanced product features include SmartDNS and Policy Routing. SmartDNS is a patent pending technology from FatPipe that efficiently balances inbound load over multiple lines and will intelligently sense when a line is down and reroute IP packets to available lines when a failure occurs. The failover is automatic.

Policy routing gives IT Administrators more control over their networks, allowing them to define how they would like data to be transmitted over their networks based on protocol, source and destination IP address, and/or source, destination port and time of day.

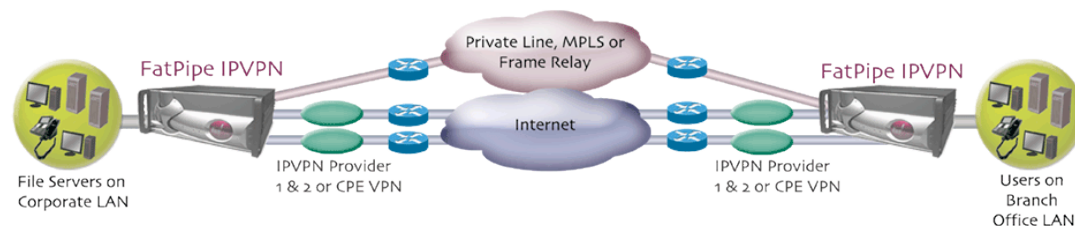


FatPipe MPVPN® enables IT Administrators' VPNs to stay "up" at all times by transcending the failures of any WAN line, ISP, router or other individual hardware components. Security of data transmission is also increased up to 900% with FatPipe's patented MPSec™, which breaks each data stream down to the packet level, randomly sends the packets over multiple connections, and reassembles the packets at the receiving end. As businesses transmit more data over Internet connections, security of that data is a growing concern. MPSec makes it virtually impossible for hackers or intruders to trap data and decrypt confidential information.



FatPipe IPVPN works with new and existing networks, creating a flexible system that balances load among multiple managed and Customer Premise Equipment (CPE) based VPNs as well as dedicated private networks. Businesses can deploy VPNs anywhere and still get the highest level of WAN availability and uptime with FatPipe IPVPN.

FatPipe IPVPN can also provide an easy, low-cost migration path from Frame Relay to VPN. Businesses can aggregate multiple private and public networks without BGP or additional equipment at the provider's site. FatPipe IPVPN gives the administrator the option of using a VPN at the customer premise or with a managed VPN service as a backup to a frame relay or private line.



FatPipe provides the highest level of redundancy, security and speed, guaranteeing more efficient and secure delivery of data. If any connection fails at any site, FatPipe automatically and seamlessly reroutes data to available lines. FatPipe also gives clients route control tools, multiple load balancing methods, and line speed charts and meters viewed in a GUI for easy installation and management.

Business Continuity through WAN Redundancy - Case Studies

The following case studies illustrate the application of FatPipe technology in strengthening business continuity.

CASE STUDY: MAJOR U.S. FURNITURE MANUFACTURE

A Major U.S. Furniture Manufacture Uses FatPipe MPVPN to Ensure Business Continuity

Major U.S. furniture manufacture, one of America's top 100 furniture retailers, operates 26 furniture stores, with three warehouse distribution centers. Processing orders and general office communications are supported by a site-to-site VPN infrastructure directly connected to its headquarters. "Computer automation is a key element to our overall business process," said their network engineer. A stable VPN is essential to the company's ability to conduct business.

They realized how mission critical its VPN was when communications to one of its warehouses was cut off for one whole business day due to a downed line. The line was physically cut, accidentally, on account of construction in the area. The data stream was stopped and productivity was significantly affected. They experienced delays in putting through orders because they had to revert to manual processes. Their inventory control was difficult to maintain and had to be reconciled from paper records once the data line was available again.

SOLUTION OVERVIEW

SITUATION

This major furniture manufacture required reliability and redundancy for its VPN infrastructure. After experiencing a business disruption of a downed data line connection, the manufacturer looked at BGP and FatPipe as possible solutions.

SOLUTION

They went with FatPipe over BGP to achieve business continuity. FatPipe was chosen for its vastly superior cost benefits and management capabilities.

BENEFITS

The company benefits from the highest levels of WAN reliability and redundancy utilizing a combination of DSL, T1, wireless, and Metro-Ethernet connections at all of their sites. It also takes advantage of the added benefit of FatPipe's security feature, MPsec. Its business continuity from a WAN perspective is assured.

"Our entire business process for that location was affected when our VPN went down," said its network engineer. Other applications, including email, accounting, inventory software, and warehouse management software all run over the VPN. "We hit the point where downtime is unacceptable," said the network engineer.

He and his team researched ways to mitigate the effects of WAN downtime. They first considered BGP. According to their network engineer, it was a hassle. "We started the ball rolling on implementing BGP and the more we got into it, the more difficult it was becoming, so we looked for an easier solution that was just as effective, but less expensive and time consuming. We chose FatPipe MPVPN."

Not only can MPVPN conduct line failover automatically, it is dynamic and works with their diverse combination of data lines including DSL – something BGP simply cannot do. The company uses FatPipe to aggregate a mixed breed of DSL, T1, wireless, and Metro-Ethernet ring at the various sites. Data is automatically failed over to available lines if a connection, component, or service fails.

The company also enjoys the added benefit of FatPipe's patented security technology, MPsec, which provides an additional layer of security.

The IT team is planning to implement other mission critical applications, including VoIP, over the company's VPN, where IP data route control and QoS will come into play. These features are available on the MPVPN.

CASE STUDY: ALLSECTOR

FatPipe WARP Provides Redundancy for the WECARE Initiative Run by FECS, the Largest Not-For-Profit Health and Human Services Organization in the US

ALLSector Technology Group is an information technology consulting company that provides not-for-profit and for-profit businesses options for outsourcing and project management of its MIS and IT services. In particular, ALLSector works in close partnership with the Federation Employment and Guidance Service (FECS), the largest and most diversified private, not-for-profit health related and human services organization in the US.

SOLUTION OVERVIEW

SITUATION

ALLSector required fault tolerance for its mission critical WAN applications run from a centralized location. The main application is accessed by other agencies using Internet connections. ALLSector wanted to create a disaster recovery plan to avoid WAN downtime.

SOLUTION

ALLSector integrated three FatPipe WARPs into its WAN. Two are setup in failover mode at one location, and a remote failover unit at a separate office for disaster recovery. ALLSector bonds a 6 mbps connection with a T1 from two ISPs at the main location, with one connection to the disaster recovery site.

BENEFITS

ALLSector achieved total WAN fault tolerance, and was successful in having control over its DNS records for true inbound IP traffic redundancy. WARP's automatic failover and easy management tools give ALLSector piece of mind that its WAN will stay up and running, even when they experience ISP failure.

One of FECS' newest applications, run by ALLSector, is a case management system called WECARE (Wellness, comprehensive Assessment, Rehabilitation and Employment), which bridge together a diverse range of home, healthcare, psychology, and housing agencies to create an efficient "welfare to work" program.

The case management system resides at one location, and is regularly accessed via the Internet by multiple agencies on a consistent basis. Online availability to the WECARE program is an essential tool for the agencies to use to help the recipients of the program. Disruptions in services due to WAN failures put a stop to the important and intricate support system for the women and men who benefit from this program simply because the hospitals and agencies that are part of the program cannot access it.

ALLSector experienced unpredictable ISP failure, and looked for a way to have disaster recovery between ISPs and two different office locations. They did not want to use BGP.

"BGP is simply too complicated and hard to maintain. We were especially concerned with inbound traffic redundancy because many agencies access the program from the outside," said Joe Baskin, Director of ALLSector's Network Operations. "We went with FatPipe WARP. It's SmartDNS feature allows us to have the automatic inbound failover we're looking for, which is faster and more predicable than failover with BGP announcements."

Using WARP's easy GUI interface, ALLSector was able to define settings with the SmartDNS and use other tools, such as Policy Routing, where they can set priorities based on application type. "Instillation went great and the support is excellent," said Baskin.

"ALLSector experienced ISP drops, but the failover was seamless. It's good to know that it's working, and that we will not experience WAN failures," concluded Baskin.

CASE STUDY: JENNER & BLOCK LLP

Jenner & Block Uses FatPipe IPVPN to Achieve Reliability and Redundancy for its VPN and VoIP Applications by Aggregating MPLS and 100 Meg Connections at Three Locations

Jenner & Block LLP is a national law firm with offices in Chicago, Dallas, New York and Washington, DC. The Firm's over 450 lawyers specialize in litigation and corporate transactions supporting multinational corporations. It is also well known for its public service and pro bono advocacy.

As an integral part of its communications system, Jenner & Block deploys a wide variety of services and applications over its Wide Area Network (WAN). The firm utilized MPLS circuits to support its primary WAN needs, and was looking for a way to increase bandwidth and WAN reliability, but did not want to incur the exorbitant costs of additional MPLS circuits. Through extensive research on how to accomplish its objective, Jenner & Block chose FatPipe IPVPN.

SOLUTION OVERVIEW “We decided to go with FatPipe IPVPN because we were looking to increase bandwidth, balance load, and have a failover solution using MPLS and Internet connections. FatPipe IPVPN gave us the flexibility we were looking for, using both private and public lines,” said Amiras Savani, Senior Networking Engineer at Jenner & Block.

SITUATION

Jenner & Block wanted to increase bandwidth and obtain WAN fault tolerance by integrating MPLS circuits and 100 mbps Internet connections to support its heavy WAN traffic.

The firm combines MPLS circuits and 100 mbps connections using FatPipe IPVPNs at its New York and Washington DC sites, along with two IPVPNs setup in automatic unit failover mode at its headquarters located in Chicago. It runs many of its applications originating from the corporate office in Chicago, including payroll, accounting and extranets, which is why it has the failover unit cluster. Every office has its own data center and local Exchange servers to support email, and local file exchanges such as litigation support applications.

SOLUTION

Installed four FatPipe IPVPNs at three locations; two in a primary/standby configuration at the corporate office, and single units at two other office locations.

A VPN tunnel was setup between the offices as an alternative path if the MPLS goes down. Utilizing FatPipe IPVPNs policy routing tools, the firm runs VoIP and back ups on the MPLS, while the day-to-day data transfers, emails, and Intranets for clients are active on its VPN using the 100 mbps Internet connections.

BENEFITS

Successfully acquired redundancy for its complex WAN between public and private networks, and gained greater control of traffic flow by balancing IP load - based on application -- using FatPipe IPVPN's management tools.

“FatPipe has met our objectives indefinitely,” said Savani. “It works beautifully. We have experienced a few circuit failures, and none of our end-users noticed because of FatPipe IPVPN's automatic failover. Management is easy, too.”

Savani and his team also enjoy an excellent working relationship with FatPipe's technical support staff, knowing that they are available whenever they have questions.

“FatPipe IPVPN has performed above our expectations, with no failure whatsoever in three years,” he added.

CONCLUSION

In today's business environment, business continuity is an imperative. Major disasters such as terrorist attacks and natural disasters have to be planned for, but are fortunately rare. Wide Area Network failure is the most common form of business disruption. FatPipe technology is designed to overcome such failures.

FatPipe Networks Patents

Please see below for the FatPipe Patents. Go to <http://patft.uspto.gov/> to read about each patent in detail.

The patent numbers are as follows:

US Patent 6,493,341

US Patent 6,253,247

US Patent 6,295,276

US Patent 6,775,235

US Patent 7,269,143