Are Network Designs Ready for a Pandemic?

Alan R. Mercer
Are Network Designs Ready for a Pandemic?

Trends and Issues with Today's Networks

Alan R. Mercer

University of Maryland – University College

TLMN636-9040

Summer 2006
Abstract

This paper will investigate the network planning and design considerations that would be affected by the operational impacts of an avian flu pandemic upon a typical organization. Most businesses operate their networks in an entity-centric mode based upon internal and external user and system distributions. The avian flu pandemic, if it becomes a reality will change that distribution markedly. Staffing availability, supply and demand, and numerous other factors of everyday business will change. Such changes have the potential to create considerable financial impacts upon businesses, the markets in which they operate, the communities they serve, and will probably be driven by governmental declarations of emergency. In addition, many operations rely upon third parties to provide communications facilities which will likely be under-manned and may suffer declining reliability. I propose that the conventional network design in business today is asymmetric, oriented towards normal operations and peak loads based upon common business cycles, and is ill-prepared for rapid changes in directional data flows and the changing data traffic patterns.
Are Today's Network Designs Ready for a Pandemic?

Trends and Issues with Today's Networks

The pending concerns over the current outbreaks of avian flu caused by the H5N1 virus spreading to humans and developing reports of human-to-human transmission have resulted in escalating fears of a global flu pandemic (Brown, 2006). Such concerns are highly justified due to the cyclic nature of pandemics, natural mutations of viral strains, migratory patterns of birds, and an increasingly mobile world connected by intercontinental transit. These concerns have led to preparations for such an outbreak ranging from government plans and policies to organizational pandemic planning committees. Yet such plans often focus on disease containment, prevention, and treatment and to a lesser extent how organizations that are increasingly dependent upon computer networks will operate effectively under reduced staffing and facilities closures.

Reports on current network design and studies and statistics on Internet connections used by organizations of differing sizes and locales indicate a trend of asymmetric network design. This trend provides indicators that a majority of today's networks are ill-prepared for the shift in usage patterns that would result from a global avian flu pandemic. History and current evidence lend credence to the popular view that a pandemic is inevitable and likely to occur soon. To understand the potential situation we must understand the history and effects of pandemics and a changing global economy that is increasingly reliant upon computer networks.

Our increasingly technological world has resulted in rapid adaptation of new technologies to retain competitiveness; often without consideration for the agility and adaptability necessary to respond to extreme changes in the operating environment. These factors indicate that the majority of organizational networks are designed using an entity-centric model optimized for performance under normal cyclic business flows. Such designs are unlikely to adapt easily to virtual reversals in traffic patterns that would likely result under pandemic conditions.

Recent Pandemics and Probable Effects of a Pandemic Today

In 1918, a global flu pandemic of unknown origin swept through the continents. The death toll was staggering for a 20th century disease: more than 50 million deaths worldwide were attributed to the flu (Carr, 2006). These estimates are also considered by some to be substantially understated, potentially by half as the worst hit areas were in lesser developed countries. With a global population of 1.8 billion in 1918, the flu related deaths are estimated to have killed 2.8 to 5.6 percent of the population. Estimates on infection rate vary from twenty to fifty percent of the population infected, with the majority of the most seriously affected being between the ages of 15 and 35 (Garrett, 2005).

Extrapolating that out to today's population of 6.5 billion people, an estimated 360 million people, equivalent to the entire United States population, could die from a comparable pandemic today (Osterholm, 2005). Despite improvements in medicine, the shrinking globe effect of mass and high-speed affordable transportation and a global economy has resulted in exponential growth in mobility. Pandemics will be accelerated and vastly more difficult to contain under such circumstances. The concerns of a coming pandemic are fueled by scientific research that shows that flu pandemics have been cyclic in nature, occurring every 30 to 40 years. Recent pandemics occurred in the 1850's, 1889, 1918, 1957, and 1968 (Garrett, 2005). All
but the 1918 pandemic were smaller in scale and under the theories of cyclic pandemic conditions the conditions favor a major pandemic.

Thirty-eight years have passed since the last pandemic however the threat is new and different. Human infection by the H5N1 virus was unknown until a few years ago and the first human-to-human transmission was recently reported by the World Health Organization (CBS, 2006). Like the 1918 pandemic, the most hard hit have been young adults; those that comprise approximately one-half of the work force and the future of the economy (WHO, 2006). Once the circulating strain is identified, existing facilities operating at maximum production levels could only create enough vaccine over a six-month period to immunize 14 percent of the world's population, leaving 5.6 billion people vulnerable. The 1918 flu is thought to be avian in nature and there are indications of Asian origin, but this is unknown as the flu virus was not identified until 1933 (Garrett, 2005). Similarly the 1976 Swine flu originated in Asia as did the current H5N1 avian flu (Osterholm, 2005). Remarkable parallels exist, yet our changing global economy provides an accelerated exposure vector unlike any prior history.

National and international response plans such as the U.S. National Strategy for Pandemic Influenza indicate that government may "take appropriate and lawful action to contain an outbreak within the borders of their community, province, state or nation" and "use governmental authorities to limit non-essential movement of people, goods and services into and out of areas where an outbreak occurs" (White House, 2005). This strategy continues to stipulate that government may impose social distancing measures, including quarantines and restrictions upon gatherings. Such language should alert the reader that mandatory shutdowns or restrictions upon "non-essential" services, travel, and even private business closures may be mandated.

Anticipating reduced personnel levels in the public and private sector, such plans also call for the establishment of contingency plans, particularly in the private sector to ensure continued delivery of essential goods and services. Recommendations include providing for offsite work while ill or during periods of travel restrictions. Both the public and private sectors must also consider that 32.8 percent of U.S. households are families with children, the majority of which are headed by young work-age adults (U.S. Census, 2001). In a pandemic, schools and daycare centers are likely to be considered non-essential services to be closed. Without childcare, workers may be forced to stay home to care for their children and may require leave of absence to care for ill family members including other adults. Telecommuting is prescribed as one option to address these concerns, yet lacks the acceptance in today's workplace to be a factor in network design for many organizations. Yet the potential of fifty-percent or greater absenteeism rates and localized restrictions upon travel may require far greater capacity than currently exists for remote worker access.

Current Global and U.S. Economy Dynamics

The economy today is unlike anything in prior history. Affordable mass and high-speed intercontinental transportation, megalopolises, international corporations, international trade, and increasing trends towards service based industries create an environment of interpersonal exposure spanning large regions. These factors create an infection threat vector unlike any known in history. An interconnected global economy stimulates travel and increases the needs for global communications. The travel numbers alone are staggering: for the U.S. alone, nearly 108 million people crossed U.S. borders in 2004 (ITA, 2005). This number is understated due to illegal border crossings.
Are Network Designs Ready for a Pandemic?

This level of international travel was precipitated by advances in mass, affordable international travel. Advances in communications and increased international relationships have resulted in an economy that is increasingly global in nature and susceptible to disruption from large scale regional disturbances. Most nations are no longer in a position of being economic self-sustaining entities. The United States imports more than 60 percent of its petroleum supplies (DOE, 2006). Despite U.S. leadership in electronics, computing, and communications most of the components are now manufactured overseas. International corporations now wield more influence than many nations world-wide (Anderson & Cavanaugh, 2000).

International trade and businesses have also taken advantage of the rapid growth of computing and telecommunications to conduct their business. International business operations have grown under 24 hour operations with global reach through networks attached to the Internet, affording large scale access and data transfers globally. Even small to medium sized businesses (SMB) have expanded globally by taking advantage of today's technologies. Yet most of the resources to deploy and support such networks focus upon inter-site and business-to-business communications. With few exceptions, this has resulted in networks designed to optimize performance between regional offices and business partners. SMBs are key indicators of local economies and readiness, yet are demonstrating an increasing global presence. New job growth and the trend towards contracting, outsourcing, and service oriented businesses continues to increase the role of SMBs in the economy, yet this sector of the economy is most likely to be adversely affected by a pandemic due to limited redundancy and continuity planning resources.

In the U.S. the Small Business Administration (SBA) reports that more than half of private sector employment is with small businesses and that small business comprises 99.7 percent of all employers (Wolk, 2004). While this number does not include government employees, it also excludes the self-employed, estimated at over 17 million. Small business also suffers higher failure rates than large business, indicating greater susceptibility to economic downturn and disaster response (Knaup, 2005). This sector also creates more than half of the non-farm gross domestic product annually, comprises 23 percent of federal prime contracts, and employs 41 percent of high-tech workers (SBA, nd).

Business Communications, the Internet, and Network Design

The past two decades have seen technological advances unparalleled in history. The 1980's saw the beginning of the personal computer era, the 90's the Internet, and toward the start of the 21st century, the use of the Internet as business communications vehicle. Computing and networks became ubiquitous in the past two decades as computing paradigms changed from dumb terminals and mainframes to powerful clients and servers. The economy changed rapidly as increased information flows provided new competitive advantages including remote collaboration and data sharing. New industries arose to provide these services. Businesses and consumers took advantage of this new medium to access and share information, acquire products and services, and increase communications.

In the late 80's and early 90's business adopted low cost personal computers and small PC based servers to create departmental local area networks (LAN). During the mid 90's these evolved into interconnected wide area networks (WAN), often reliant upon slow and expensive links between networks provided by local telephone carriers. By the end of the 90's a new model emerged: use of the Internet as a business tool. Internet connections for groups of users during this time often relied upon the same technologies used to interconnect WANs. Thus an
asymmetric network design model developed which provided high speed local network access with slower WAN and Internet access. Under this model, network design focused upon departmental servers servicing local area networks providing distributed systems optimized for access by local users.

By 2000, the business network design model had matured. Best practices had been developed and this structure created inflexibility. Yet the exposure to the Internet, the wealth of resources available, and an increasing reliance upon networked computing and communications strained the resources of businesses to replace slow WAN and Internet connections. The computing and telecommunications industries responded in various ways, further confusing network design. New lower cost connections to the Internet such as Digital Subscriber Lines (DSL) and Cable broadband Internet became common. Thin client technologies emerged, emulating the mainframe mode of operation. However the Internet was not controlled by any single entity or even limited number of entities. It was a shared media, reliant upon interoperability and cooperation between competing telecommunications providers. This introduced security risks to businesses. As a result Virtual Private Networks (VPN) were born to provide secure and private communications on public lines.

Yet this was not without cost: new hardware, services, software, training, and support had to be acquired. Older equipment often could not be reused in this new paradigm, further slowing adoption of the Internet as business communications tool. Businesses remain focused upon profitability and thus cost-benefit decisions focused network changes upon those that provided the greatest return to the business. For many businesses, these decisions focused upon intra-organizational and business partner communications rather than large scale capacity for individual remote access. Heeding the warnings of the Dot Com bust of 2000 through 2003, investment in technology was slowed and conservative. Cost cutting measures meant replacing or augmenting expensive dedicated circuits and hardware with asymmetric DSL and cable Internet lines. Statistics bear this out: together cable and DSL broadband connections have comprised the majority of new high-speed Internet connections. The rapid growth of DSL and cable Internet has been fueled primarily by home users and the SMB market.

Over the past few years broadband usage has increased considerably, although the cable Internet and xDSL markets have dominated the growth. U.S. Department of Commerce statistics for 2004 show that broadband usage for home users more than doubled between 2001 and 2003, with cable comprising 56.4 percent and DSL comprising 41.6 percent of broadband connections (NTIA, 2004). The U.S. exceeded 60 percent of Americans having broadband access in 2005, yet rated 20th globally in broadband penetration according to Nielsen net ratings (WebSiteOptimization, 2006). Gains were also seen among business users, where fixed broadband usage remained flat, indicating an increasing presence of xDSL and cable Internet use by business. A report in 2000 by Insight Research predicted that by 2005 over half of small businesses would have broadband access, the lion's share of the growth to be split by xDSL and cable (Insight, 2000). A similar study by the Office of National Statistics in the U.K for 2002 regarding business adoption of broadband shows that xDSL and cable Internet amongst small businesses with less than 250 employees is more than double that of other fixed broadband types (ONS, 2002).

DSL further compounds the issues of analyzing the statistics as many variants of DSL technologies exist including IDSL, ADSL, SDSL, VDSL, and HDSL. ADSL comprises nearly 95 percent of today's DSL broadband lines in the U.S. (FCC, 2005). SDSL and HDSL are
increasingly used for replacement of T1 or E1 lines, thus providing little growth in symmetric technologies. SDSL costs are frequently three to six times that of ADSL or cable Internet. The cost sensitivity of SMBs creates substantial preferences for asymmetric technologies such as ADSL and cable Internet. DSL technologies also suffer from limitations of distance: the maximum available bandwidth decreases as distance increases. Thus DSL is often not scalable when growth or traffic patterns change, causing congestion and performance issues.

Despite dramatic increases in home and business broadband adoption, telecommuting still meets resistance in business today. A U.S. Department of Transportation report in February 2005 reported that only 5.8 percent of Federal government workers participated in a telework program by the end of 2003, despite mandates that 75 percent of the federal workforce be eligible by 2003 with prior projections of more than 10 percent participation (Weiner & Stein, 2005). Despite resultant concerns of 9/11 disasters decimating large groups of valuable workers, governmental adoption of teleworker policies has been abysmal. As early as 2000, IDC reported that despite dramatic growth in remote access, mobile workers with limited access outpaced remote access worker growth by 3.5 to 1 (Kistner, 2000). In fact, ITAC and IDC estimates range from 7.9 to 8.7 million U.S. workers telecommuting at least one or more days per month in 2004, yet less than half of corporations surveyed reported telework as part of their disaster recovery or business continuity plans (Said, 2005).

Current Network Design Issues

Despite renewed interest in business continuity and disaster recovery fueled by recent events such as 9-11 and catastrophic storms such as Katrina, current business acumen held that such efforts should be focused upon known and probable events such as fire, weather, and earthquakes. Such plans assumed existing equipment and communications would be destroyed, impaired, or unavailable and thus focused upon resuming or relocating operations and equipment using a model of emulating the existing network. Little thought was given to situations where systems continued to operate, yet facilities lacked personnel due to quarantines, public closures, and transportation shutdowns thus requiring a paradigm shift from local network access to remote access by myriad users from numerous and indeterminate locations. Even an SBA news release on May 22, 2006 provides no advice to prepare for a pandemic; rather it focuses upon historically common disasters (SBA, 2006).

Typical networks today frequently demonstrate these design issues as seen in Figure 1. A typical multi-site SMB organization is likely to have a network where local network speeds are 100 Mb/S or even gigabit per second, while inter-site and internet connections are often less than five percent of the LAN throughput speeds. Local networks and inter-site connections are frequently designed using symmetric communications lines possessing equal upload and download speeds, yet many remote sites use asymmetric lines for less critical Internet access and smaller sites. This design takes the view that the most critical operational access is local to each site, with enterprise access being secondary, and Internet access being tertiary. This design optimizes local access with high-speed communications and local servers, yet constrains remote due to substantially slower communications lines. This design is frequently economic in basis as higher speed symmetric connections usually require more expensive hardware and cost more to lease due to distance and provider pricing strategies.

Why is this design flawed? A closer examination shows that this design exhibits minimal redundancy, many of the connections are asymmetric, and under heavy use between offices
throughput is constrained at several areas due to directional flows. Under this design, the majority of inter-site traffic is between remote sites and the corporate office. Normal client-server data flows are also asymmetric, with client systems retrieving more data from servers than they send to servers. The design appears well suited for normal operations as remote sites possess large download capacities for data retrieval and lesser bandwidth for upload to servers. The sum of the remote offices upload speeds is only one-half of the download speeds at the corporate offices. Similarly, the corporate offices possess only one-third the throughput of the combined remote sites download speeds. It would appear that sufficient bandwidth exists in both directions and provides reserves for growth and Internet access. Yet it also indicates that bandwidth is available which may not be usable and that any given connection between two points is limited by the slowest link, in some cases by as much as 96%.

It is these directional traffic flows that form the basis for the thesis that network designs today are ill-prepared for the changes in directional traffic flows that may result under pandemic conditions. If a pandemic were to break out in New York City the likely effect would be a near total shutdown of the city. Proposed actions include travel and gathering restrictions. Mass transit may be forced closed, effectively barring the majority of workers from their places of business. Due to family illness or school and daycare closings many workers might have to stay home. Other employees, fearing contamination and infection might refuse to work, further reducing available staffing. Many businesses could potentially lose onsite availability to 70 percent or more of their workforce. Others might be forced to close local sites completely.

In order to establish continuity, businesses would have to provide concurrent remote access capabilities for large portions of their workforce on a network designed for a large portion of the users to be located on the local network. Also consider the previous statistics on telework: only five to ten percent of workers currently participate in telework and the majority of that group only telecommutes part-time. This would equate to approximate levels of peak telecommuting usage of less than three percent of the workforce. Providing large scale remote access to displaced workers to ensure continued operations would dramatically change traffic patterns on Internet and site-to-site links. Assuming 30 percent of the workforce would be necessary and available to maintain minimum necessary operations remotely for a few weeks; this represents at least a ten-fold increase in remote access traffic.

Adding to the stress on remote access links is the fact that conventional network design focuses upon distributed data systems where data stores are located according to optimal use under normal cyclical operations. Thus users accustomed to retrieving megabytes of data across multi-megabit Ethernet connections are likely to be limited to the multi-kilobit upload speeds of asymmetric DSL or cable internet connections, at best limited bandwidth fixed speed broadband connections such as T1 or fractional T3. Upload speed limited to 128 Kb/S on some ADSL circuits will crawl under the load of numerous users accessing data remotely. Even a T1 shared by 30 users remotely and regularly accessing large files and data stores could reduce effective throughput per user to modem-like speeds. Using the estimates of 3 percent normal and 30 percent emergency remote access levels, the corporate offices would jump from approximately 6 to 60 users sharing the combined 4.5 Mb/S data lines while the Virginia office would jump from an average of less than one remote access worker to nearly five sharing a 128 Kb/S line. Nor do all inter-site communications cease if the facilities are unoccupied. Intersystem and external communications such as e-mail continue to occur, consuming even more bandwidth, thus reducing available bandwidth for remote workers.
Thus network designs are highly asymmetric due to their basis of high-speed local access with substantially lower inter-site and Internet access. This becomes even more asymmetric in nature when technologies such as cable Internet and ADSL are deployed. This asymmetric design is an underlying reason that telecommuting has not met target levels and sporadically connecting mobile worker growth has rapidly exceeded that of true remote access workers.

Case Study – Catholic Charities of Baltimore

Catholic Charities is a medium sized business located in Baltimore, Maryland with numerous offices distributed throughout central and western Maryland. The agency is the largest private provider of social services in Maryland and has 2,100 employees, 1,250 computer users, 950 PCs, 36 servers, and 38 networked locations. Remote access capabilities currently exist for 190 users however the peak concurrent remote usage is less than 20 remote users. Similar to small businesses, Catholic Charities is cost sensitive since they are a 503(c) 3 non-profit charity. Their performance is based upon the amount funding received is returned in services to the clients. Despite the number of computer systems and users, Information Technology initiatives are frequently considered administrative costs to be minimized. This has resulted in a lack of fault-tolerance and redundancy in the network design. Figure 2 provides a partial overview of the Charities network.

The main administrative site is home to the data center which houses the 12 enterprise application, mail, database, and authentication servers. This facility possesses the greatest bandwidth of all sites, with three T1 or SDSL 1.5 Mb/s Internet connections and five T1 point-to-point (PPP) WAN links. The remaining servers are distributed at the WAN and VPN sites. Of the distributed servers, three are database servers and five mail servers residing at other WAN sites. However, many WAN sites have no direct internet access and rely upon either the administrative site or other locations to provide Internet access to local WAN users and servers.

Sites not connected via PPP connections have their own Internet connections which also provide branch office VPN access to the Charities WAN. Of the 1,250 Charities network users, over 900 are on the main WAN, the remainder are located at the various VPN sites. All remote access (non-WAN) other than branch office VPNs is provided via two Citrix Presentation Servers at the main data center. Key sites on the WAN with the exception of the two administration buildings have generator power backups. The existing network design is the result of network implementations at major sites that were subsequently interconnected and smaller sites recently added using VPN technologies. The growth and evolution of the network mirrors the trends and timelines previously described as typical network design evolution.

Of the 26 VPN sites, 25 use DSL or cable Internet technologies. Unlike many small businesses, the majority of Catholic Charities VPN sites use SDSL; only nine current sites employ ADSL or cable Internet. Of the SDSL sites, due to location approximately one-third are at maximum available bandwidth. Thus over half of the VPN sites have no bandwidth scalability using existing communications technologies. Of the T1 connections used at Catholic Charities, all are full T1 lines except 2 locations, providing little to no scalability without additional hardware and communications lines. Approximately 50 percent additional growth in branch office VPNs is planned, although only minimal increases in telecommuting options are being pursued currently. Due to continuing funding constraints, a high probability currently exists that a higher ratio of asymmetric to symmetric connection technologies will be deployed at future VPN sites.
The structure of the Charities network is the result of evolution consistent with patterns of computing and telecommunications advances and cost considerations. The design is that of a hub and spoke with both WAN and VPN sites radiating outward from a central facility that houses the primary datacenter. Due to cost containment, few redundant paths exist to provide fault tolerance. At the central site, the primary purpose of the three Internet connections is dedicated load distribution and only two of the three provide automated fault-tolerance for each other.

Consistent with historical trends in disaster recovery and business continuity, much of the focus has historically been upon individual systems failure and recovery or individual site relocation. The assumptions have held that a regional disaster was not fully addressable by a small to medium sized regional business as all functions were local to the region and therefore all regional facilities were impaired. Until recently little consideration was given to business continuity scenarios where systems and facilities remained intact, but personnel were unavailable to occupy the facilities and work locally.

Thus the infrastructure requirements for large scale remote work from myriad changing locations does not exist in current plans and has not been a driving factor in network design. Instead, cost and performance optimization of branch office and local user access in relation to normal cyclical operations was the major influence upon network design. Rapid and extreme changes in directional traffic flow patterns were of extremely low importance in the design of the network.

As presented, the Catholic Charities network (Figure 2) closely resembles the network design frequently seen at SMBs (Figure 1), only on a larger scale. Many of the issues discussed related to current network design in SMBs also exist in Catholic Charities network. While well suited for normal operations, the design lacks redundancy and throughput necessary for nearly one-third of normal usage to shift to external access of internal systems. The central repository of enterprise level data is further constrained regarding remote access due to a lack of consideration of individual remote access except via Citrix. While Citrix uses a thin-client approach, the implementation of the Citrix systems places the servers behind a NAT firewall for security purposes. This further limits the bandwidth available to be used in accessing Citrix servers due to a limitation in Citrix implementations with NAT, restricting the system access to a single publicly accessible address. That address is accessible via a single T1 line despite the equivalent of three Internet T1 circuits at the location.

The dynamics of remote access requirements anticipated in a pandemic scenario would reduce local area network traffic, but place substantially higher loads upon slower external and WAN connections. While the use of Citrix mitigates this shift by keeping many activities local to the main datacenter, the increased number of external users places a substantial increase in traffic on the single internet connection. Data at other WAN sites would be retrieved via slow PPP T1 links, increasing normal bandwidth usage on these links and slowing performance. Users accustomed to high speed local retrieval of most data would now experience increased latency due to slower internet connections, increased routing hops, and slower internal WAN links.

To indicate the nature of the shift, consider Catholic Charities 1,250 users and their business. Many of the programs operated by the Charities have 24 hour residential facilities and some staff would need to remain local to provide continuing services. However many of those staff have limited or no access to the networks, thus these employees have little effect upon reducing remote access needs. Support services such as HR, Payroll, Accounting, Information Technology, Purchasing, and management however would likely shift to remote access. These
are the heavier users of the networks and would have the most effect. Even if 250 workers remained onsite at residential facilities, more than 1,000 might be displaced. Assuming our emergency continuity levels of 30 percent availability, the result is 300 users that may require regular remote access during a pandemic event. If all potential remote users required concurrent access this would allocate an average of 5 Kb/S per user on the single remote access T1 line. This average is one-third the minimum required bandwidth for reliable Citrix sessions.

Potential Corrective Actions and Issues

The problems with current network designs that are prevalent at SMBs today have been highlighted in the above explanations and case study. Constrained bandwidth, ineffective usage of bandwidth, asymmetric data lines with unbalanced data speeds, limited redundancy, and reactionary evolution of network growth are contributing factors to the issues seen. This situation is compounded by the rapid acceptance of lower cost, asymmetric Internet solutions such as ADSL and cable Internet. Noting that only 41 percent of high-tech workers are employed by SMBs that employ more than half of all workers and comprise 99.7 percent of all employers, the lack of technical capacity at SMBs becomes a major factor in network design issues. While current designs favor and work effectively with normal cyclic operations, they lack flexibility and capacity to contend with a major shift in user access dynamics from local to remote access.

Potential solutions including adding capacity, adopting symmetric communications technologies, increasing redundancy, more effective distribution or centralization of data centers, increasing use of thin-client technologies, and improved network design to increase agility. Increasing accessibility to high-tech skilled workers is also critical to improving network design. Not all solutions are applicable to all organizations, particularly SMBs. With limited resources, costs are a major consideration. Few solutions to existing design issues are without cost. Direct costs include additional monthly circuit costs, implementation costs, hardware acquisition and replacement, and maintenance costs. Nor do all issues warrant correction. Some operations may be shut down or curtailed for periods of time without long-term harm to the organization. Others are critical to the ability of the organization to continue operations and can not be allowed to shutdown or reduce operations even under emergency conditions. Failure to respond effectively could permanently harm or cause business operations to cease. Potential solutions include:

- Third party datacenter collocation - This creates a central data facility where all data stores are connected to redundant high-speed networks
- Replacement of existing lines with scalable, faster lines under metered usage agreements. This provides initial and on-demand increases in capacity.
- Automated load balancing of existing data lines - Provides load distribution across multiple communications lines to optimize usage of limited resources.
- Bonding of existing data lines - Increases data throughput by using two or more data lines as a virtual single connection.
- Redistribution/centralization of existing data stores – May optimize data access speeds and throughput due to changing conditions.
- Strategically located redundant paths. Failure of a single data line should not cause a loss of connection to key data resources and systems.
• Increased use of thin-client technologies – Reduces data traffic on WAN and Internet links by keeping most traffic on high-performance local networks.
• User work shifts for remote access during emergencies. By distributing usage over time, load on Internet connections to the WAN can reduce periodic peaks.

Most solutions provide the greatest benefit in tandem with other solutions. Nor are all solutions feasible in all areas. Rural and less economically developed areas may lack the infrastructure necessary for providers to profitably operate high-speed networks or data centers. Since many data circuits are limited by distance or their cost is based upon distance, these options are not always available or effective. Where bandwidth can not be increased, thin-client technologies may be necessary to reduce bandwidth needs. Centralization or collocation frequently require increases in high speed data access to the data stores and may necessitate the use of thin-client technologies.

Case Study – Potential Solution

In the case study of Catholic Charities the WAN was found to lack redundancy and bandwidth capacity necessary for large scale remote access. In addition, the primary data center lacks backup power capabilities; this point became painfully clear on July 28, 2006 when an area power blackout caused the data center to be shutdown for nearly 27 hours affecting operations agency wide. These conditions put Catholic Charities at risk for instability even during normal operations. The solution must provide increased reliability during normal and possibly prolonged periods of unusual conditions. Planned changes in the operations of Catholic Charities programs and the relocation of certain facilities creates an opportunity to revise the network design to provide the redundancy, bandwidth, and reliability necessary to operate under emergency conditions such as a pandemic. These changes include the relocation of the administrative offices at 2305 N. Charles including the main data center, the closing of two sites, and the consolidation of two other VPN sites into a single new facility.

One option is to collocate the data center at a third party facility with high speed connections to multiple ISPs, redundant power feeds, generator backup, and security systems. This would require substantial investment in bandwidth increases for numerous Catholic Charities sites and/or a transition to thin-client services for most network users. The thin-client option bears high initial costs due to implementation, hardware, and licensing costs. Nor does this solution address site connectivity redundancy issues, even at most larger sites on the WAN. Thus many WAN sites would be required to obtain additional bandwidth and data circuits. Many of these sites are not expected to be able to bear this added cost within the next few years.

Since Catholic Charities is a mid-size business with an experienced and highly tenured Information Technology staff, a more effective and easily implemented solution would take advantage of the closings and relocations occurring over the next nine months. Such a plan would increase bandwidth at the new facility for the data center, add necessary generator power backup, add redundancy in communications through additional data links, and optimize remote access by relocation of the Citrix remote access servers. The proposed network is presented in Figure 3 and should be compared to Figure 2.

This solution provides greater bandwidth at the main data center and creates full load balancing and redundancy on the two primary data lines. The two existing T1 lines are replaced by fractional metered T3 or Ethernet lines with load balancing technologies. The Citrix servers
would be relocated from the private WAN to the semi-public demilitarized zone (DMZ) to allow public addresses from all three ISP connections to be assigned to both servers correcting the existing issue with effective single line access. A few sites are physically located within a few hundred yards of each other on the same campuses. These sites currently connect using PPP T1 lines which would be replaced with fiber optic Ethernet connections. A new facility is nearing completion that will replace two VPN sites connected via SDSL circuits; this facility will be connected to the WAN via multiple PPP T1 lines. Two sites are closing, eliminating the need for a PPP T1 line and a SDSL circuit. Under this design a total of net total of two PPP T1 lines and two fractional T3 or Ethernet Internet connections will be added, while three SDSL circuits are removed.

This plan capitalizes upon existing equipment, minimizing costs for replacement and additional hardware and licensing requirements. Since most existing routers are modular and have gateway routing protocol capabilities, many existing sites can add circuits through the replacement or addition of lower-cost modular components. The addition of redundant links also provides WAN performance increases by distributing traffic based upon shortest path or least congestion. While the design addresses bandwidth, redundancy, and availability the issue of remote access licensing remains. Licensing for Citrix will need to be increased to deal with emergency conditions resulting from a pandemic. This expense may be reduced by developing protocols that use shift based access to reduce concurrent usage. It may also be deferred as the additional licensing may be obtained electronically and within 24 hours direct from the vendor, thus allowing rapid scalability and agility as required.

It is important to note that this plan does focus upon the primary WAN and not smaller VPN sites. However these smaller sites often do not have local servers and rely upon the VPN to the data center for data storage and access. Under normal disaster planning, such sites would re-establish operations elsewhere through data recovery. In a pandemic, some VPN sites would close, others would continue in normal access modes, and some users would shift to remote access. This proposal retains asymmetric qualities that may constrain bandwidth yet minimizes the negative effects of the asymmetric enterprise network design.

**Conclusion**

The majority of networks today are asymmetric in design due to large variances in bandwidth of local networks compared to inter-site and Internet connections. SMBs are more likely to have highly asymmetric networks due to limited resources and increasing adoption of asymmetric communications lines such as cable Internet and ADSL. This asymmetric design has evolved through rapid advances in network and computing technologies that have been added to existing networks and have historically focused upon normal cyclic operations. Network design has largely been ignored in disaster recovery and continuity planning due to assumptions of normal operations relocating to another facility or restoration of existing services in the affected facility.

Pandemics change the dynamics of disaster recovery. Outbreaks may cover large areas and may be global in nature due to mass high-speed global travel. Containment of outbreaks may result in business closures, travel restrictions, shutdown of public transportation, closing of schools and daycare, and numerous other actions. Such actions are likely to cause substantially reduced staffing availability adding to the staffing reductions from illness. In many cases, businesses may need to continue operations without any onsite staff with all operation occurring
via remote access. In the case of a pandemic, today's asymmetric networks are not designed with the flexibility necessary to adapt to a virtual reversal in primary network traffic flows. Nor can we predict how long it will be before the next pandemic or the severity of the outbreak. Since the majority of businesses are SMBs that are more vulnerable to failure after a disaster, immediate attention to this issue is necessary. However, as shown in the case study, the solution need not be a radical or complete redesign of the network.

Numerous options exist to reduce the asymmetric nature of network design in order to provide the flexibility for rapid changes in directional traffic flows. A number of options have been presented together with a case study that reviewed two possible solutions. Not all options apply to all organizations nor are all options feasible for all organizations. Each entities needs, usage, existing networks, and existing resources must be analyzed and the solution tailored to the environment. This includes technical capacity within and available to the organization. SMBs are underrepresented in skilled tech-worker employment. This means that external support mechanisms are likely to be necessary. Potential support mechanisms include network service providers, data center operators, the Small Business Administration, industry groups or alliances, and academic resources such as the University of Maryland University College's Security Studies Lab (UMUC, 2005). The problem is not insurmountable, unless it goes unaddressed and predictions of the effects of a pandemic are correct. If unaddressed business failures are likely to increase and the severity of the global economic impact is likely to be worsened.
References


Are Network Designs Ready for a Pandemic?


Figure 1 - Typical SMB Network
Figure 2 - Catholic Charities Network Overview – July 2006
Figure 3 - Proposed Charities Network Revisions - July 2006
## Upcoming SANS Training

Click here to view a list of all SANS Courses

<table>
<thead>
<tr>
<th>Course</th>
<th>Location</th>
<th>Dates</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Chicago Spring 2020</td>
<td>Chicago, ILUS</td>
<td>Jun 01, 2020 - Jun 06, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS ICS Europe Summit &amp; Training 2020</td>
<td>Munich, DE</td>
<td>Jun 08, 2020 - Jun 13, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Budapest June 2020</td>
<td>Budapest, HU</td>
<td>Jun 08, 2020 - Jun 13, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Las Vegas Summer 2020</td>
<td>Las Vegas, NVUS</td>
<td>Jun 08, 2020 - Jun 13, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Zurich June 2020</td>
<td>Zurich, CH</td>
<td>Jun 15, 2020 - Jun 20, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS London June 2020</td>
<td>OnlineGB</td>
<td>Jun 01, 2020 - Jun 06, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>Books &amp; MP3s OnlyUS</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>