Incorporating Wireless Into the Business Continuity Plan

Summary

Wireless networking plays an increasing role in overall enterprise business continuity plans, in part because of the dependency that enterprises – which are growing increasingly distributed across branch offices – have developed upon wide-area communications. While the impact of some incidents may be confined to a single business site, in other instances, occurrences might be farther-reaching, taking the form of natural disasters, warfare, or pandemic illnesses. In such instances, wireless can play a critical role in helping maintain enterprise communications.

Business continuity planning involves preparing for incidents that could jeopardize an enterprise's immediate productivity and revenue, its long-term financial health and customer care. The impact of some incidents, such as a local network cable cut or a building fire, might be confined to a single business site. In other instances, occurrences might be farther-reaching, taking the form of natural disasters, warfare, or pandemic illnesses.

Wireless communications devices and network services represent just one component of an enterprise's overall disaster recovery plan. However, they play a critical role in helping maintain communications during network outages caused by the situations described. For example wireless communications might enable a single site to continue to access data resources if a terrestrial cable is cut. Similarly, connectivity might be maintained using mobile broadband in high-transaction environments, where retailers or others need to maintain credit card verification capabilities to continue selling products.

Wireless serves a broader purpose during full-blown disasters by enabling enterprises to contact employees, emergency responders and government authorities involved in recovery efforts. In addition, wireless location-based systems (LBSs) are pivotal to finding missing individuals and assets in widespread disasters. In such instances, even wireless video capabilities are coming into play. As an example, workers local to the outage or disaster might gain IT assistance from a remote specialist in making a repair. Alternatively they could transmit a video of their surroundings to remote personnel, who can determine the appropriate equipment, personnel and emergency responders to dispatch.

Why Protect the WAN?

One reason for the increased emphasis on wireless networking in disaster recovery plans is that the number of distributed branch and virtual offices is growing swiftly: branch offices will grow 6.79% in 2008 compared to 2007 and are expected to grow another 6.87% in 2009 according to Nemertes Research[1]. Also, an increasing number of business applications are Internet based. These circumstances mean that the majority of enterprise network communications travels today across a WAN. So enterprises must focus more attention than ever before on protecting wide-area communications.

There are often times when wireless connections remain live when wired network circuits – particularly those in the "last mile" access network – fail because of an accidental cut. In addition, a wireline connection anchored at both ends might fail if either the switching office or the termination point is in a disaster zone. In the wireless environment, by contrast, even if a particular cell site or switch has failed, wireless-capable devices might be able to associate with another cell tower that is functioning outside the disaster zone.

In some catastrophic situations caused by severe weather or armed conflict, wireless network services might experience an outage, too. However, airwave communications are usually faster to reinstate than terrestrial circuits because trenching and installing physical cables are not necessary. The physical requirements of cabling become particularly troublesome and time-consuming in disaster situations where cabling in need of repair may be under rubble or water.

Planning Ahead

A large portion of recovery planning revolves around conducting business impact analyses, assessing risk and putting contingency processes in place. Contingency process planning includes training employees about appropriate backup procedures in the event of an outage or widespread emergency, including the use of wireless communications. Wireless communications can assist in the communications necessary for initial alert of the event (notification), the damage assessment phase, and the initiation of the recovery and contingency plan. Additionally, during the recovery timeframe, wireless can be used to communicate with recovery teams and monitor the progress of the recovery efforts.

Another level of business continuity involves protecting critical data and communications links. Here, the enterprise IT department must identify the critical infrastructure, sites, applications and business processes needed to keep the business running. Once IT has determined what those critical sites and processes are, it can put backup systems and processes in place to protect them.

To do so, IT builds redundant components, equipment, and network services into the organization's overall network design. Redundancy helps ensure that user access, database synchronization and data backups continue to take place should some circuits or equipment fail. Many of these functions involve data and voice transmission over a WAN.

At critical sites, building multiple WAN connections to one or more data centers maximizes uptime and minimizes losses. In such cases, if one WAN service is unavailable, the other can be used to get to a primary or alternative data-hosting site. Wireless is generally a good backup candidate for the reasons described below.

Access and Backbone Network Strategies

In the last mile, a terrestrial broadband connection might be the primary connection. Multi-user mobile broadband access as a secondary or backup connection, through the use of a wireless router, makes sense to prevent the same incident that takes out the primary link from also affecting the secondary link. In other words, combining terrestrial and wireless access connections provides true local-loop diversity. Wireless routers certified to operate with a given mobile network are generally available from the mobile carrier, an integrator or wireless router maker directly.

In addition to redundant access network connections, it also makes sense to employ failover diversity in the backbone network. Once users are live from their locations, having an alternative backbone route to corporate resources helps compensate for any backbone connections affected by disasters. For example, IT might wish to build in not only frame relay or MPLS VPN connections to corporate resources, but also support alternative remote access VPN connections across the Internet. In the event that one backbone type should temporarily fail, the other is likely to be accessible.

Generally, the WAN service provider will also build in redundancy and diversity into each WAN service, so it's a good idea to find out what the carrier's own disaster recovery setup looks like. This includes the degree of redundancy in the design of the wireless provider's broadband access and backhaul networks, as well as the diversity of the routed terrestrial WAN backbone. Because WAN services managed by the network operator are an extension of the enterprise network, both the carrier's and the enterprise's disaster recovery plans and the execution of these plans affect the enterprise's operations.

The cost of business continuity grows with each level of redundancy that is added. So it is vital to conduct a thorough analysis of how prone a given site is to an outage and how much the business stands to lose if critical locations and applications are inaccessible for an hour, day, week or month. There will be some appropriate balance of risk and redundant infrastructure for each enterprise that is contingent on the enterprise's type of business, physical locations and degree of distributed communications.

Stockpiling Mobile Equipment

The wireless component of the business continuity plan often has a heavy regional emphasis. Some companies, for example, make plenty of standby mobile phones, mobile broadband devices, wireless routers and subscriber identity modules (SIMs) available in specific regions during hurricane season, where outages have a greater probability of occurring. SIMs are components of GSM-based mobile phones that store the identity credentials and billing information of the subscriber. Subscribers can change phones by simply removing the SIM card from one mobile phone and inserting it into another one.

Sometimes, enterprises will elect to store these backup mobile components in multiple places. In the case of a full-blown outage in a given region that might destroy local standby equipment, this enables replacement devices to be shipped from another location to the area in crisis.

Enterprises can purchase and set aside these types of mobile equipment and use them only in emergency situations. In such cases, this avoids recurring monthly usage fees for standby equipment intended only to be used in exceptional cases. Generally, carriers sell these devices at their suggested retail price, rather than at the lower, subsidized rate that usually accompanies the concurrent purchase of a mobile service with a service contract of a year or more.

Alternatively, enterprises can purchase subsidized devices with an inexpensive basic cellular service plan as a form of insurance. Generally, if and when these services are used, the wireless provider caps the fee that can be charged to that device in a given month. With preset caps, the provider can monitor usage and if it is reached more than a predetermined number of months running (such as three months in a row), then the subscriber is automatically moved to a different plan.

On-Demand Communications

In the heat of a disaster, telecom managers or other personnel in non-impacted regions can usually go to an online site hosted by their mobile provider and order accessories for users who do not have them yet. They can also add services on demand, such as international capabilities and paging.

Text-messaging is a communications option that uses paging technology to help avoid wireless network congestion and to work around failed email servers. Paging uses the control channel of the wireless network rather than the data channel so it can often be available even when traditional voice and data capabilities over the wireless network are not.

Wireless priority services are available for first responders, which is a requirement that the government has imposed on wireless operators during periods of congestion or disaster. Those organizations eligible for wireless priority services generally show the mobile carrier proof of eligibility and the carrier then activates the service.

If congestion occurs because a region is in crisis and wireless networks are over-utilized, wireless providers are capable of rolling in additional network capacity in the form of a portable cell site (with base station radios, on-board power, tower, and antennas) mounted on the back of a truck. Portable capacity can be requested as needs merit, but note that the federal government has the ultimate power to commandeer where the cellular-on-wheels capacity is provisioned.

Bandwidth and Coverage Considerations

The types of wireless network service available in a given geographic area and their throughput potential will determine which applications will be able to run over a wireless backup link. It is important for IT to determine ahead of time which applications can be supported by the wireless service available in a given area.

For example, Enhanced Data Rates for GSM Evolution (EDGE) mobile data services, which carry wireless data at a theoretical maximum throughput of 384 Kbps, are comparable to ISDN bandwidth. Applications well served by ISDN can also be well served by EDGE services, provided they are available in the affected area. EDGE services are the most widely available GSM-based data services.

Depending on the severity and duration of a disaster, some local operations or emergency responders might set up a temporary workplace. In such cases, wireless LANs become an option for local communications, because they are quicker and less expensive to build and tear down than cabled Ethernet networks. Wi-Fi also supports ad hoc (peer-to-peer) communications for on-the-fly direct communications between individuals. It also offers multi-megabit speeds, accommodating more users and higher-bandwidth applications.

Workers connected to the wireless LAN can communicate directly with one another locally over the temporary Wi-Fi infrastructure. Additionally, they are able to access remote corporate resources over the wireless network via a wireless router in cases where no terrestrial landline is available.

There are also some all-wireless local options for allowing fairly small temporary workspaces to communicate with their WAN backbone services. For example, remote access services are available that involve installing IPsec VPN client software and a 3G mobile broadband card in a laptop, which wirelessly sends encrypted traffic to a local wireless router. The local wireless router forwards the IPsec-encrypted traffic to VPN termination equipment (gateway) in the wired WAN provider's backbone. There, the user's frame relay or MPLS VPN user group is identified and the user authenticated, and the gateway routes the traffic onto the corporate VPN service.

Summary

Wireless networking plays an increasing role in overall enterprise business continuity plans, in part because of the dependency that enterprises – which are growing increasingly distributed across branch offices – have developed upon wide-area communications. Wireless is pivotal to disaster recovery plans for employee safety, asset tracking and faster return to operations. Wireless services are attractive for disaster recovery because they usually remain live when terrestrial communications are taken out by debris, water, or cable cuts. In the event that wireless service does fail, it is generally faster to reinstate than cabled connections.

IT departments must plan ahead for wireless in their business continuity plans, document specifically the escalation process for usage and train employees on those processes. To do so, they must assess the risk and cost of downtime of a particular application or location. From there, they can determine whether it makes financial sense to install cellular routers for multi-user wireless access connections as a truly diverse backup alternative to terrestrial local-loop connections. Part of that decision will rest on finding out ahead of time what cellular network services are available in high-risk geographic areas, determining which applications will be able to run over a wireless backup link and setting up the process for application failover accordingly.

As part of their plan, many enterprises may stockpile unsubsidized, “standby” mobile equipment to be used only in the case of emergency for which they are charged only when the devices are used. Alternatively, enterprises can purchase subsidized devices with an inexpensive basic wireless service plan as a form of insurance.

Both Wi-Fi and wireless networks can be used in temporary office setups for direct peer-to-peer communications (though in the cellular environment, it is necessary to select devices that support the peer-to-peer capability). These temporary sites can also communicate to data center resources using a wireless connection through a wireless router.

Each enterprise will strike a slightly different balance of risk and redundant infrastructure as appropriate to the business. In determining where and what role wireless should play in the organization’s business continuity plan, IT departments will consider a mix of factors. Among them are the enterprise’s type of business, physical locations, application types, susceptibility to severe weather and degree of distributed communications.

Reference

1. http://www.nemertes.com/market_analyses/nemertes_market_analyses_unified_communications_collaboration

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

at&t
Your world. Delivered.