WHY NETWORK FAILOVER PROTECTION
IS A BUSINESS NECESSITY

1471 Route 9, Suite 202
Clifton Park, NJ 12065
Phone: (518) 371-2295
Fax: (518) 881-1810
www.oneconnectinc.com

OneConnect

Since its early days in the 1990s, the Internet has truly transformed the world. It would be difficult, if not impossible, to find an industry that isn't impacted in some way by the Internet. Some companies are so reliant on the Internet that, without connectivity, they would soon be out of business.

Network interruptions can be costly to a company, not just in lost business and sales, but in general productivity and even in terms of reputation, branding, and market share. This is why network downtime is such a serious issue for many businesses today, and why network failover is a critical component of modern business strategy.

Market research indicates that up to 16% of a large enterprise's revenue can be lost annually due to network outages. A company's susceptibility to this varies by industry and by how distributed the operation of the business is. Whether downtime is caused by service providers, employee error, or natural disaster, the costs are real and, in many cases, largely avoidable.

WHAT IS NETWORK FAILOVER?

Network failover is the practice of providing redundant or duplicate network components so that, should the primary piece of the network fail, the backup can take over and maintain business as usual. Failover strategies can be categorized into automatic, delayed, or manual varieties, generally referred to as hot, warm, and cold standbys, respectively.

1471 Route 9, Suite 202
Clifton Park, NJ 12065
Phone: (518) 371-2295
Fax: (518) 881-1810
www.oneconnectinc.com

Different elements of a network can be configured to use any of these in various combinations depending on how mission critical the particular component is, and how quickly it needs to be brought back online in case of an interruption.

DEVICE FAILOVER

A distinction should be drawn between network failover and device failover. Most people are familiar with the concept of device failover—the provisioning of a backup device, often running in parallel with the primary, ready to take over in case of hardware failure. Network failover necessarily includes the concepts of device failover, but is broader in scope and also encompasses aspects related to services and hardware.

This white paper aims to provide an overview of the various elements of network failover strategies.

WHO NEEDS TO THINK ABOUT NETWORK FAILOVER AND WHY?

Adoption of unified communications (UC) solutions is becoming more widespread across all industries. UC enables businesses to operate in completely new ways and provides many previously impossible capabilities. It also, however, places much more importance on the network on which these services run. If a company is going to put so many of its eggs into one basket, it is absolutely vital to make the basket as safe and robust as possible.

Some industries and types of businesses are more network dependent than others. Examples of

1471 Route 9, Suite 202
Clifton Park, NJ 12065
Phone: (518) 371-2295
Fax: (518) 881-1810
www.oneconnectinc.com

businesses that need to arrange some degree of network failover include:

- Small and medium sized businesses (SMBs) that have adopted UC solutions, or that use network capabilities for other business-critical functions. A business that uses UC services is a given, as all of its voice, data, email, and instant messaging communications rely on the network. Some less obvious examples include mom and pop stores that use networked payment methods, and shipping companies that use a distributed network structure to handle logistics and tracking.
- Web hosting companies, managed service providers, application service providers, and smaller ISPs/resellers not only need comprehensive network failover protocols, they need to have them set up in such a way that the failover process is as transparent as possible to their end users.
- Any business that is organized with one central head office and several smaller branch offices spread out geographically. The smooth flow of information between geographically diverse locations relies heavily on a properly functioning network, and any impediment to that network can have negative effects on the business's ability to operate.

THE DIFFERENT LEVELS OF FAILOVER PROTECTION

Network failover strategies can be divided into three general categories: cold, warm, and hot standby.

Cold standby requires that the failover procedures, or switching over to new hardware or to a different

1471 Route 9, Suite 202
Clifton Park, NJ 12065
Phone: (518) 371-2295
Fax: (518) 881-1810
www.oneconnectinc.com

wide area network (WAN) link, be done manually. Cold standby is seldom used in real-world systems, and never for critical components. Where cold standby is appropriate, generally a variation is used where the failover is performed automatically after some form of manual approval is received.

Warm standby is when the backup system is already running in the background, although not quite ready to take over instantly. Before the backup system can become operational, some form of data synchronization needs to occur. Warm standby results in a fairly quick resumption of service, but some interactions can be lost in the service gap caused by the data sync.

The fastest and most reliable type of network failover is hot standby, where both systems are kept up and running and synchronized at all times . With hot standby, a service interruption in one system results in an automatic rerouting to the backup system without any loss of fidelity. The end user is generally unaware that anything unusual has occurred.

NETWORK ELEMENTS THAT REQUIRE FAILOVER PROTECTION

There are three major elements to most corporate networks, and all of them require some form of failover protection: the local area network (LAN), the WAN, and the network infrastructure services. Failover protection for infrastructure services depends largely on the service provider and is out of the direct control of most businesses, so this paper will focus primarily on the LAN and the WAN.

1471 Route 9, Suite 202
Clifton Park, NJ 12065
Phone: (518) 371-2295
Fax: (518) 881-1810
www.oneconnectinc.com

THE LAN

The corporate LAN deals with all network communications within a single location. Because it is confined to one location and is entirely in-house, maintenance of the LAN stays within the control of the business. This means that the sorts of events that can result in the failure of network capabilities are less likely to occur on the LAN.

There is one eventuality that does need to be addressed in terms of the LAN, however: power failure. In order to maintain internal communications capabilities in a power failure situation, internal networking infrastructure must be connected to an uninterruptable power supply (UPS). If external communications need to be maintained as well, external access devices such as WAN routers, switches, and hardware firewalls need to also be connected to a UPS.

For businesses such as banks or hospitals that need their internal communications to perform critical services, a good UPS configuration is likely sufficient. For other operations that rely more on external communications and for which a loss of networking capability would be crippling, such as call and data centers, it might be necessary to arrange utility power through more than one power company. This ensures that power will remain operational even in the event of a downed line.

THE WAN

HARDWARE REDUNDANCY

Network failover strategies include hardware failover strategies, and one of the fundamental elements of

1471 Route 9, Suite 202
Clifton Park, NJ 12065
Phone: (518) 371-2295
Fax: (518) 881-1810
www.oneconnectinc.com

hardware failover protection is device redundancy. What hardware needs to be backed up is determined on a business by business basis, but generally devices such as switches, gateways, routers, and components for the network switches are prime candidates.

DIVERSIFYING WAN LINKS

There are two different methods of providing WAN link diversity: By employing multiple types of WAN link, or by employing multiple carriers. Of the two methods, multiple link types is less expensive, but using multiple carriers is the more reliable way of ensuring Internet connectivity.

BANDWIDTH CONCERNS

Many solutions to the failure of one part of the network involve routing the traffic that would have traveled over the failed network to a part of the network that is still operational. This, however, causes some complications of its own with regards to bandwidth capacity.

Taking the peak capacities of both the failed portion of the network and the portion that will be taking up the slack, and adding them together to calculate total bandwidth required on each section isn't quite sufficient. It is recommended to add an additional 25-40% capacity on top of this when possible. Situations that result in the failure of a significant part of the corporate network quite often also result in a significant increase in communications traffic on the remaining portion of the network, as employees attempt to deal with whatever crisis caused the outage in the first place.

1471 Route 9, Suite 202
Clifton Park, NJ 12065
Phone: (518) 371-2295
Fax: (518) 881-1810
www.oneconnectinc.com

COMPREHENSIVE SOLUTIONS

For businesses that have time-sensitive, business-critical applications, there are additional measures that can be taken to ensure smooth network operation under the most adverse of conditions.

Rather than attempting to maintain network failover solutions in-house, many businesses choose to make use of WAN Optimization as a Service (WaaS). The bandwidth aggregation provided by these services allows for WAN links to be pooled into one large network pipe, or to be maintained as separate pipelines for different types of traffic, then switched back and forth from one system to the other as needed.

WAN virtualization takes this one step further, and is the process of installing WaaS at multiple physical locations on the corporate network and allowing them to direct all traffic between sites in the most efficient way possible across all available WAN links.

1471 Route 9, Suite 202
Clifton Park, NJ 12065
Phone: (518) 371-2295
Fax: (518) 881-1810
www.oneconnectinc.com

SUMMARY

The Internet has become such an important part of doing business today that losing access to it can be crippling for a company. Many modern business applications are decentralized and require networks to be flexible in order to accommodate different load needs at different times.

- Good network failover strategies perform a number of key functions within the framework of maintaining network functionality. They
- eliminate costly network downtime and ensure application and communication availability,
- manage WAN resources across the entire network,
- provide device redundancy and monitoring,
- manage load balancing and traffic routing, and
- increase scalability and throughput in a cost-effective way.

For any business with mission-critical network applications, network failover protection is an absolute must.

1471 Route 9, Suite 202
Clifton Park, NJ 12065
Phone: (518) 371-2295
Fax: (518) 881-1810
www.oneconnectinc.com