WHITE PAPER

TRUE DIVERSITY

HOW TO ACHIEVE CRITICAL NETWORK REDUNDANCY

Businesses with critical applications running on their network need to regularly consider how they manage network diversity toavoid costly downtime impacts.

For example, a Telstra network outage in 2019 left consumers unable to withdraw cash at ATMs or make digital payments. This unplanned downtime cost Australian retailers an estimated $100 million[1]. The outage was attributed to higher-than-normal traffic volumes putting pressure on the network; a situation that's highly likely to be repeated.

While telecommunications carriers in Australia tend to be reliable, it's realistic to expect that all carriers will experience network problems at some point. Unplanned downtime can have potentially devastating consequences for a business. At the very minimum, unexpected outages are inconvenient and frustrating.

For some businesses, downtime for even just a few minutes can mean tens of thousands of dollars in lost sales as customers simply go elsewhere. It can cause lost productivity as staff members are unable to complete tasks until the network is back up and running. The longer this takes, the more the company loses in productive time. Then there's the hidden costs. For example, if downtime means an organisation's data backups didn't occur correctly, then data can be lost.

It's important to recognise that the cause of network downtime doesn't always rest with the carrier. Things can go wrong at any stage on the network from the carrier's core network to the customer's local area network (LAN). For example, roadworks can damage fibre connections at the front of an office building, seismic activity or insects could cause damage to cables running between capital cities, and users can be disrupted when a new service is connected.

While some businesses could potentially withstand a very short outage, most require network diversity so they can immediately switch over to an available network and avoid any downtime at all.

1. https://www.smh.com.au/business/banking-and-finance/telstra-sorry-for-outage-which-retailers-say-will-cost-them-100m-20190712-p526jy.htm

THE RISKS

Each telecommunications provider has at least one core network and, in some cases, multiple core networks. These cores can be completely diverse in their own right inside of the carrier's network. That core network is surrounded by an access network, which is the last piece of connectivity between the core network and end user locations.

Network traffic is typically always brought back to the core to be routed. Access networks connecting to the core can be from a single carrier, or from multiple carriers. The interconnect network creates connectivity between core and access networks in a process known as network-to-network interconnection (NNI). Some carriers use NNI to let providers leverage the carrier's physical infrastructure to offer carrier and geographical diversity.

However, this creates interlocking risks. If a carrier's core network is compromised and multiple providers rely on the same network, then all of those providers' end users may experience downtime.

The risks to these networks are significant, especially with fibre-based networks. Physically cut and damaged fibre is at fault for many network outages. This can occur due to animal activity, vehicle damage, vandalism and human error.

For example, in 2008 a boat's anchor cut through undersea cables providing connectivity to the Middle East and South East Asia. In 2011, an elderly woman in Georgia cut through the main fibre link between George and Armenia, likely because the weather may have exposed the fibre. Around once a year, Melbourne's Montague Street Bridge is impacted by an over-height vehicle, dislodging core infrastructure that runs over the top of the bridge. And, a length of fibre buried four feet deep running for more than 1,000km from Adelaide to Western Australia was the victim of termite damage.

When infrastructure is physically damaged, it can take hours upon hours to physically splice and repair the connection. During this time, customers can do nothing but wait for the services to be restored, unless they have true diversity in place.

In 2012, a Telstra exchange in Victoria's Warrnambool township was hit by fire, damaging 60 per cent of the exchange. The fire took down fixed and mobile voice and internet services for approximately 60,000 users for many hours, and in some cases, for days. Customers of Telstra, Optus, and many large internet service providers were also affected.

Because so many providers share the same infrastructure, even laying fibre in the same or nearby conduits around the country, it can be hard to promise true diversity even if businesses work with more than one carrier. If a carrier's network touches the network of the redundant supplier, then true diversity can't be achieved. Every time a provider opens a pit or pipe to access the network, there is a risk of adjacent networks being impacted, which can affect service quality.

Some organisations would argue that they are protected from terrestrial connectivity downtime by the mobile 4G network. However, not all mobile phone towers are connected to each other via microwave. Most are connected via fibre, which would similarly likely be affected an outage impacting the local fibre network.

IF A CARRIER'S CORE NETWORK IS COMPROMISED AND MULTIPLE PROVIDERS RELY ON THE SAME NETWORK, THEN ALL OF THOSE PROVIDERS' END USERS MAY EXPERIENCE DOWNTIME.

PROTECTING BUSINESSES WITH TRUE DIVERSITY

Organisations need to ensure they have true diversity in place. This means more than just having a redundant supplier contract. It means having a diverse portfolio of access that includes second and even third levels of diversity.

This could include a fibre-based fixed-line service, a fixed microwave solution such as a small antenna on the building, and then LTE 4G connectivity. Fixed line, fixed wireless, and mobile wireless networks can create three levels of redundancy that significantly mitigate the risk of unplanned downtime.

This approach can create cost savings by simplifying the network and providing the ability to route traffic over multiple carriers seamlessly. However, this requires a solution that lets businesses take control of their network and break free from carrier constraints.

To assist, businesses should look for a provider with heritage and expertise in terrestrial connectivity as well as fixed wireless connectivity. By separating the network geographically, i.e. having one network rely on fibre while another uses microwave, organisations can more completely insulate themselves against downtime caused by physical factors.

HOW SD-WAN IS REVOLUTIONISING THE CONCEPT OF DIVERSITY

The telecommunications industry is experiencing a revolution that means customers are no longer quite so dependent on telecommunications providers. Software-defined wide area networking (SD-WAN) is a virtual or software network that runs across existing legacy WAN infrastructures.

This once-in-a-generation technology leap separates the control plane from the networking hardware and puts it in the cloud. This puts full control in the hands of a business' network administrators without requiring a hardware upgrade. SD-WAN is able to incorporate almost every type of wired and wireless connectivity, making it the ideal solution to deliver true diversity for businesses. It's completely carrier-agnostic so organisations can start to leverage SD-WAN immediately, regardless of any carrier contracts they may have.

Organisations with existing supplier contracts for fibre networks can, for example, work with a different provider for their fixed wireless network. Breaking free from a single telecommunications carrier can deliver significant benefit, not least of which is cost.

Using an SD-WAN service, organisations can achieve the silver bullet of having a network that has physical separations via a mix of fibre and microwave or fixed wireless connectivity.

Breaking free from their telecommunications carrier is just the first of many benefits for SD-WAN customers. SD-WAN also lets them more completely see and control what's on their network. This provides visibility into what service performance carriers are providing so that customers can more clearly decide how to manage business-critical applications and how they'll be delivered in the event of service disruptions. This unprecedented level of control will give organisations the true diversity they need.

Businesses don't need to replace existing systems to gain the benefits of SD-WAN. Instead, they can overlay SD-WAN onto existing networks to achieve the required redundancy and reliability without incurring excessive costs or disruption.

HOW VERTEL DELIVERS SD-WAN

Vertel currently offers two types of SD-WAN services: an SD-WAN managed service for end user clients; and SD-WAN-as-a-Service, which offers a wholesale white label offering to channel partner organisations, with Vertel providing the technical expertise needed for back-end support.

Vertel is a privately owned Australian company with more than 40 years' experience designing, building, and operating business- and life-critical networks for customers. The first in the world to offer MEF-certified Ethernet services over wireless technology, Vertel has been offering carrier-grade Ethernet and high-capacity internet since 2000.

Vertel SD-WAN is built using technology from Nuage Networks, from Nokia. It is MEF 3.0 SD-WAN-certified and meets the requirements defined in the MEF 70 SD-WAN Service Attributes and Services standards.

Vertel SD-WAN is built on open standards. It overcomes issues around: network complexity, reliability, and outages; bandwidth shortages; security concerns; WAN dependence on a single telco; and long and complex change control times. Vertel SD-WAN is a turnkey deployment which lets organisations deploy new sites and applications with zero-touch provisioning.

NEXT STEPS

Vertel recommends organisations undertake a top-down network review to ensure their network includes true diversity. If not, it may be worth considering implementing SD-WAN to facilitate the cost-effective addition of redundant networks.

To find out how Vertel can help your organisation successfully deploy SD-WAN, contact us on 1300 837 835 (1300 VERTEL) or info@vertel.com.au. Visit us at www.vertel.com.au.