HARDENING THE LAST MILE

Overview

The "Last Mile" refers to the last, local legs of communication that connect the user to the Internet. For universities and large businesses, this is the responsibility of the IT department. For most enterprises, dependency on the Internet has soared in recent history. Email has become the primary form of communication. Desk phones are almost all VoIP now. Instant Messaging, video conferencing, and desktop sharing have become indispensable tools.

The Cloud has further intensified this trend, with SaaS applications commonly being used for Sales, HR, ERP, File Sharing, Learning Management Systems, Marketing, Service Desk and an ever expanding list of other critical services. Many providers of conventional services you might not normally associate with the Internet have now become reliant on it as well, including emergency services like fire alarms, e-911, and broadcasts. Facilities themselves may rely on them for various building controls including door locks, leak detection, and environmental controls. Voice Carriers are now putting SIP gateways in the cloud and leveraging the internet for voice services. Many Point-of-Sale vendors are leaving traditional dedicated voice lines and moving to Wi-Fi.

If the Internet is not actually used to deliver your product or service, it almost certainly is used as part of your business process. An Internet outage would cause a wide variety of processes to slow to a crawl or halt altogether. At a minimum, when the Internet is unavailable, productivity plunges. For most Fortune 1000 companies, the Internet is now just as important--or more important--than their private WAN. Many hospitals now classify Wi-Fi as Mission Critical. For Universities, no other item under the control of IT impacts the students' perception of the University more than Internet access. The importance of the Last Mile, therefore, has soared. This makes hardening the Last Mile a prudent investment.

We have helped large enterprises and major universities harden their Last Mile. This white paper is our playbook to help you harden yours.

Secondary MPOE

An institution of any size has a Main Point of Entry (MPOE) where telco service enters. For campuses and large buildings, we recommend having a secondary MPOE. Every year we see customers that have a localized event beyond the control of IT--such as broken water main--that ends up disrupting their ability to provide Internet service. The first step in minimizing such occurrences is to have more than one physical location across which you can distribute the critical infrastructure components that provide all the links in the path from your users to the Internet.

Secondary Telco

We recommend having a secondary provider of telecommunications service. While IT can control everything from the MPOE inward, it has very little control from the MPOE outward. However, a close study of providers can reveal what transmission medium they do or do not share before they reach your MPOE. Obviously the least amount of sharing, the better the redundancy.

Placement

Some of the factors that need to be considered in the placement of a secondary MPOE include:
- The likelihood of the same event impacting both MPOE's
- The location of existing service provider transmission lines
- The availability of space
- The appropriateness of the space (e.g. the first floor is bad)
- Cooling
- Redundant power (including for the Cooling)

Size

Even if every single server you have were to move to the cloud, there will still be a need for networking equipment on premises. We recommend sizing to accommodate three things:
- your wired network
- your wireless network
- a distributed antenna system (DAS)

DAS

Most of you do not have DAS yet, but there is a very good chance you will. In essence, it is used to improve cellular service throughout a campus and within individual buildings. Your mobile phone already falls back to cellular service when wireless isn't available. Much of your workforce--and perhaps some of your customers as well--have already found ways to be productively engaged via their mobile devices. We consider good cellular service to be a major step in hardening your Last Mile.

We recommend using 3rd-party DAS companies, such as Mobilitie and Simplifi, rather than purchasing and operating your own equipment. In our experience, they are much more successful in negotiating with the telcos. Typically these DAS outfits ask for 800 square feet of space for their equipment. That much space can usually serve an entire campus. If you plan your MPOE size to be able to accommodate DAS as well, then you should be future-proof.

Some DAS vendors can also include Wi-Fi antennas in their arrays, significantly

improving outdoor coverage.

In many cases, the DAS vendors can negotiate with telcos such that the cost of the DAS equipment will be completely offset. In some cases, there may even be some additional revenue from the telcos.

Critical Infrastructure Architecture

In addition to the network equipment itself (e.g. routers, switches & firewalls), there are other, closely related, components that are critical to a user being able to successfully connect to your local network and, from there, to the Internet. Each of these should be architected so that they are not only redundant, but that redundancy is split across the two MPOE's. Chief among these are:

- DHCP
- DNS
- IPAM
- Directory services (i.e. AD, LDAP)
- Time servers (if hosting on-prem, these should be distributed too)
- Access Control services (e.g. Aruba ClearPass, Cisco ACS)
- Wi-Fi Controllers (a.k.a. Wireless Controllers, Mobility Controllers)

Wi-Fi

Some universities and many hospitals now consider Wi-Fi service to be "Mission Critical". Because of the rapid proliferation of mobile devices, this is spreading into other enterprises as well. It is now common for new office construction to rely upon Wi-Fi to connect most users rather than Ethernet cables. Therefore, even if Wi-Fi is not a current priority, in order to future-proof your organization, it is important to consider both wired and wireless users.

Point-to-point Wi-Fi now can be done at Gigabit speeds. Some enterprises are now using this to provide an alternate connection between buildings. This gives them the redundancy to survive damage to the fiber that runs between their buildings, whether it be from a backhoe or a major disaster. Point-to-point systems survive disasters well because you seldom have to do more than realign the antennas to restore service. It is worth considering whether this technology has a place on your future roadmap.

Summary

Every link in the chain that allows your users to gain access to the Internet should be resilient. This means no device should be a single point of failure. Further, it means all the devices that provide a given service should not be in the same physical location. Both physical locations should be of suitable quality to stay operational during power outages. Perhaps the hardest--and certainly the most often neglected--part of that is

cooling for the equipment that stays operational during a power outage as well. Otherwise, during an extended outage, the equipment will overheat and fail anyway.

Help

If you would like help in architecting and implementing these changes, send an email to LastMile@cloudifyinc.com. We can assess and document your current environment, and even provide the financial analysis if needed. We can design new, more resilient architectures. Where appropriate, we have even worked with our customers' existing vendors (e.g. Bluecat, Microsoft) on their new architectures. We can also help implement those architectures, sending engineers on site to make the configuration changes. Our partner, Bruns-pak, is one of the top-rated Design & Build firms (a "Leader" in the upper-right corner of Gartner's Magic Quadrant). Their experts can determine the best location for a secondary MPOE. They are experienced in dealing with the telcos, and expert in designing facilities that can survive power outages. They can oversee the build of a new space, or a remodel of an existing one. We can also bring a DAS vendor to the table for you.