Automation of Detection and Fault Management Response of Common Last-Mile Loss-Of-Connectivity Outages Within the Access Network

Alban Scribbins, Open University, Milton Keynes, UK
Kevin Curran, Ulster University, London, UK

ABSTRACT

The article to assesses whether it may be possible to recommend a solution to enable automation of the process of detection and fault management of common conclusive loss-of-connectivity last-mile outages, within the access network. To ascertain the utility of the research, UK based MPLS VPN managed service providers, their fault management staff and their business customers, were surveyed using online questionnaires for their views. UK public Internet users were additionally surveyed via five UK Internet forums. UK communication providers offering MPLS VPN solutions were characterised. Access network connectivity technologies and fault management functions were compared, contrasted and analysed. An aspiration for the solution to be beneficial to the largest potential population, meant that current non-proprietary Internet Standard technologies were selected, justified and identified which could be recommended for use. It was found that of the participating survey respondents, two-thirds were in favour of automation. Many current communication provider processes were found to be mostly automated. The article concludes with recommendations of how an automated solution could potentially be enabled. This involves further use of business-to-business interfacing between communication providers, automation of their Fault Management Systems and introducing Bi-Directional forwarding for detection between last-mile active network elements.

KEYWORDS

Internet, MPLS, Network Management, VPN

1. INTRODUCTION

In the field of Internet connectivity and wide-area-networking, communication providers (CPs) should not be complacent about the need to ensure end-to-end connection availability for connectivity services supplied to their customers. It was reported in October 2013 that a number of businesses lost critical voice and data services, when storms knocked down several telephone poles in the local access network. One company was quoted, “So far it has cost us over £6,000 since losing the connection” (Knowles, 2013). Geographically, access networks (T822a, 2003) reach most rural and

DOI: 10.4018/IJWNBT.2020010101

urban areas. Often utilising legacy national telephony infrastructure, an access network connects with a regional communication network at a point-of-presence (POP) location, often a local telephone exchange. Within a POP, or within a specialised cabinet deep within the access network, aggregation node equipment is used to converge single customer connections onto shared trunk cabling. The communications infrastructure between the CP aggregation node and the customer premises is known as the 'last-mile'. Many businesses and the general public are unlikely to invest in last-mile backup connections due to the expense involved. Occasionally a customer may experience a last-mile loss-of-connectivity outage and need to contact their CP (Jin et al, 2010). A CP fault management team then initiates manually selected tests in an attempt to diagnose the cause of the outage. Many outages are caused by common conclusive faults (Bendouda and Haffaf, 2019). The process of verbally informing CPs of outages and the manual fault management functions undertaken by CP engineers potentially increase the outage restoration time by days. Outages incur costs. The sooner an outage is detected and resolved the lower the costs incurred (Ayoubi, 2018).

The main justification for the research is based on the benefits to wide area network (WAN) connectivity users. Not all business customers are able to afford to build resilience into their national and international networks. Resilience is expensive (Wosinska and Chen, 2009) and often used for 'high value' sites. For example, national store chains such a charity shops, may not afford to have last-mile backup links to each of their sites. Customers or users of the last-mile connection may experience loss of trade, connectivity to organisational central data processing systems, telephony, staff productivity, staff confidence in WAN network administration and loss of client confidence. The CP may experience compensation payments resulting from breached Service Level Agreement (SLA), blighted brand reputation, loss of investor (Bharadway et al., 2009) and customer confidence. And costs incurred due to incorrectly instigated engineering visits. The cost is relative to the time and duration of the outage (Lyons et al., 2012). These costs may be mitigated by removing the need for customers to contact their CP and for CP fault management staff to manually diagnose common last-mile outages. With an automated solution a last-mile customer could be assured the CP would diagnose last-mile connectivity outages on their connection without being contacted and be assured that last-mile outages may be dealt with promptly and efficiently. In addition, with an automated solution a CP could reduce compensation payments (Hajdarbegovic, 2013) for breached SLAs, arrange for more timely repairs and reduce mistaken engineer call outs and remove basic tedious common diagnostic tasks from fault management staff processes permitting them to spend more time on complex fault issues. Opposition may come from proprietary fault management system manufacturers who may have designed automated systems based on specific underlying high value connectivity technologies such as Ethernet. Access network equipment manufacturers may not accept the value to be gained in adding additional functionality to their devices. CPs may not realise the savings to be gained in introducing more automation to their business environment. Fault management staff may fear for their roles due to the introduction of automation.

Therefore, this research is focused on United Kingdom based, last-mile fixed-line WAN access network connectivity technologies and topologies. These technologies may transmit data and/or voice traffic. The discussion focuses primarily on the powered (active) elements utilised within last-mile connections located between the customer premises equipment and a CPs POP equipment including elements such as aggregation node equipment. Only last-mile connectivity outages are researched. Other connectivity issues such as performance will not be included. Metallic leased lines are not included as they are being phased out by fibre Ethernet (Ofcom, 2012). The research is restricted to investigating only those CPs involved in the provision and fault management assurance of last-mile and access network connections which are physical media connectivity CPs, wholesale connectivity CPs and managed service providers (MSP) who offer Multi-Protocol Label Switching (MPLS) virtual private networks (VPN) solutions to business customers (Nyasulu et al., 2018). Primary data has been sourced from organisations providing and using MPLS/IP VPN solutions that may have at least one MPLS VPN connected site in the UK. Detailed discussion of MPLS and MPLS VPN is out-of-scope.

Related Content

Sinkhole Attack Detection-Based SVM In Wireless Sensor Networks
Sihem Aissaouiand Sofiane Boukli Hacene (2021). *International Journal of Wireless Networks and Broadband Technologies (pp. 16-31).*
www.irma-international.org/article/sinkhole-attack-detection-based-svm-in-wireless-sensor-networks/282471

Optimization of CMOS Quadrature VCO Using a Graphical Method
Hassene Mnif, Dorra Mellouliand Mourad Loulou (2012). *Advances in Monolithic Microwave Integrated Circuits for Wireless Systems: Modeling and Design Technologies (pp. 89-103).*
www.irma-international.org/chapter/optimization-cmos-quadrature-vco-using/58489

Neighborhood Overlap-based Stable Data Gathering Trees for Mobile Sensor Networks
Natarajan Meghanathan (2016). *International Journal of Wireless Networks and Broadband Technologies (pp. 1-23).*
www.irma-international.org/article/neighborhood-overlap-based-stable-data-gathering-trees-for-mobile-sensor-networks/170426

A Comprehensive Study of Security in Cloud Computing
Prasanta K. Manohariand Niranjan K. Ray (2017). *Handbook of Research on Advanced Wireless Sensor Network Applications, Protocols, and Architectures (pp. 386-412).*
www.irma-international.org/chapter/a-comprehensive-study-of-security-in-cloud-computing/162128

Secured Communication Key Establishment for Cluster-Based Wireless Sensor Networks