Considering the Wireless Internet Service Provider in a Software Defined world

Diarmuid Ó Briain[1,2]

[1]GameCORE Research Centre, Department of Aerospace, Mechanical and Electronic Engineering, Institute of Technology, Carlow, Ireland

[2]Department of Electrical and Computer Engineering, College of Engineering, Design, Art and Technology, Makerere University, Kampala, Uganda

February 13, 2016

1 Software Defined WAN

In traditional enterprise, Local Area Network (LAN) segments are interconnected across the Wide Area Network (WAN) via Multiprotocol Label Switching (MPLS) circuits operated by Internet Service Providers (ISP). While in many enterprises, small offices maybe connected over the Internet via secure Virtual Private Networks (VPN). At this stage it is common for people to use Voice over Internet Protocol (VoIP) for personal and even business voice calls over the Internet and for the most part it works. Therefore why shouldn't it be possible to manage enterprise traffic over the Internet? Quality of Service (QoS) cannot be guaranteed on the Internet so enterprises continue to employ MPLS circuits for the QoS and the Service Level Agreements (SLA) they receive from the providers. Such circuits and the enterprise routers required at each site makes the cost of such circuits quite expensive.

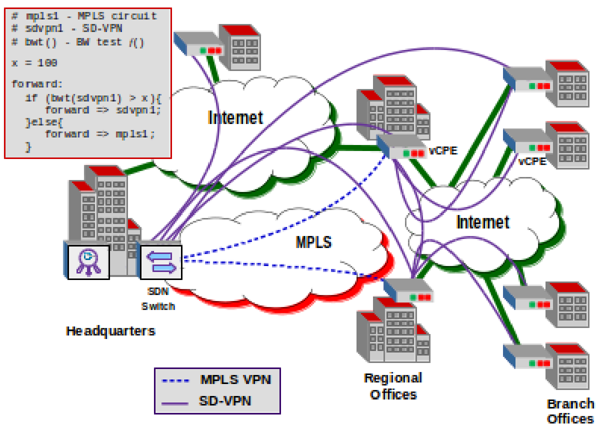

Figure 1: Software Defined WAN (SD-WAN).

Software Defined WAN (SD-WAN) as demonstrated in Figure 1 provides a solution to the problem. With SD-WAN, MPLS circuits are maintained between the critical sites, say HQ and regional sites. Each site has a virtualised Customer Premises Equipment (vCPE) instead of an enterprise router. For major sites both Internet VPN and MPLS circuits are maintained while smaller sites maintain multiple Internet circuits from more connected sites. A Software Defined Network (SDN) Controller monitors each circuit, both MPLS and Internet. Taking the example that a Regional Office requires 100 Mb/s of bandwidth at a certain latency with the Headquarters office. The SDN Controller monitors these thresholds and should the Internet circuit meet the requirements it will forward traffic over that circuit instead of the more expensive MPLS option. Should the Internet circuit fall below the threshold then the SDN Controller can redirect the traffic over the MPLS circuit to maintain the expected QoS level. In this way MPLS is only employed when the Internet circuit cannot meet the required SLA. Similar re-routing can occur for network outages as the SDN Controller has an overall view of the WAN circuits, it can detect failures and redirect accordingly.

2 The future of Broadband

It is predicted that the future of broadband [1] will be a new Global-Local paradigm that will supply an elastic network that will give the appearance of infinite bandwidth to the end-user. This paradigm will be achieved increasingly by Global Service Providers (GSP) using Local Service Provider (LSP) infrastructure. Seamless provision will be possible with the GSP providing vCPEs to the customer and LSPs allowing the GSP access to a slice of their Application Service Plane.

The changes that the elastic network bring about will also impact the cloud. Elastic compute and elastic network will link and develop together. The current centralised cloud cannot continue in its current form and cloud content will need to be brought closer to the customer. Services where latency and bandwidth are critical to the service will naturally be the first to benefit from this. The need for this change can already be seen as Netflix install Content Delivery Networks (CDN) in regions, typically through local Internet eXchange Points (IXP) [2] in Europe. Another pointer to a new model is Netflix support for the Open-IX Association (OIX) to establish European-style IXPs in the United States of America (US) [3].

A new Global-Local paradigm will evolve that creates a service chain with critical functions moving to a new edge cloud and less critical functions remaining at the central site. Virtual eXtendable LAN (VXLAN) [4] and SD-WANs will link the elements of the service chain mapped together via SDN network policies. If the edge cloud resides at the LSP it will be interesting to see how the principle of Net Neutrality can be maintained. There are many questions regarding the future evolution of the Global-Local cloud paradigm. Will the:

- LSP simply act as an Infrastructure as a Service (IaaS) provider for the GSP ?
- LSP provide a hosted Platform as a Service (PaaS) or Software as a Service (SaaS) for the GSP ?
- GSPs provide infrastructure locally as is the current case where Netflix provides CDNs at local IXPs. This model is very expensive for the GSP and will probably not scale well in the future.

It is very likely that a mix of these options will exist in the future, the selection of a particular option driven by local circumstances.

3 Wireless ISP

The Wireless Internet Service Provider (WISP) is generally a small to medium sized ISP that provides Internet access via radio. These services have traditionally been provided using the Industrial, Scientific and Medical (ISM) 2.4 and 5 GHz unlicensed bands using IEEE 802.11 style protocols or sub-6 GHz licensed bands using IEEE 802.16 WiMAX like services. As demonstrated in Figure 2 radios are mounded on the customer premises and aligned with local base station access points in a Line of Sight (LoS) or near LoS (nLoS) configuration. In lots of ways the existence of WISPs can be described as a demonstration of the failure of wireline and mobile operators to provide adequate coverage. The WISP has plugged the hole in their coverage maps.

3.1 Base Station Sites

A Base Station (BS) site consists of a number of sector radios as required to meet the coverage requirements of an

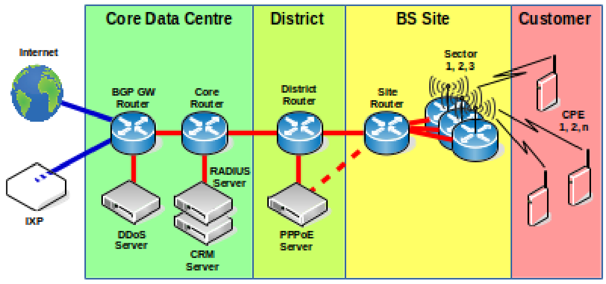

Figure 2: WISP network today.

area. Typically these radios have switch and routing functionality in their own right and can perform functions like AAA, priority and QoS. It is typical for these to be powered by a Power over Ethernet (PoE) device or even from a PoE switch or router unit as an aggregator. Power at these sites can be from the national mains but often as not in rural locations they are powered by green sources like solar or wind. To maintain a steady current to the devices and to store power a battery bank with a Uninterruptible Power Supply (UPS) is employed.

3.2 District sites

A number of BS sites are typically connected to a district site via Point to Point (PTP) radio links where back-haul is connected to the core network (National fibre Backbone Infrastructure (NBI) or trunks offered by larger ISPs). Interconnections at each of these points is facilitated by a routing function, quite commonly the Area Border Router (ABR) linking multiple site routers within the OSPF area to the OSPF backbone area (0.0.0.0) associated with the core. This routing function is most probably given a Virtual LAN (VLAN) on a metro Ethernet style circuit by the back-haul provider.

3.3 Core network

The existing WISP core network has a number of key functions today:

- A high powered router or pair of routers to peer with upstream ISPs and IXPs using the Border gateway Protocol version 4 (BGPv4) inter-domain routing protocol [5],
- Tools to mitigate against large scale Distributed Denial of Service (DDoS) attacks [6] [7],
- Internal core routing functionality, using an Interior Gateway Routing Protocol (IGRP) like Open Shortest Path First (OSPF) to route traffic downstream,
- AAA through Remote Access Dial-in User Service (RADIUS) to validate customer access to the network as well as company engineers accessing network assets for maintenance purposes,

- Customer Relation Management (CRM) to handle customer account management for sales, customer service as well as billing and financial management of company network assets functions.

4 The future of the WISP

The WISP as it exists today is under threat. Wireline providers are plugging more and more gaps in their services with fibre roll-outs to the home or to the cabinet and extending to the home with Very high bit rate Digital Subscriber Line (VDSL) or G.fast [8]. Mobile operators are also rolling out significant fibre so as to decrease cell sizes, improve coverage and throughput to their customers. Mobile operators will deploy License Assisted Access (LAA) solutions like LTE in Unlicensed spectrum (LTE-U) in the 5 GHz band [9] and while a clear channel assessment based on Listen Before Talk (LBT) [10] should be performed prior to transmission to prevent interference, it will add more traffic in an already cluttered spectrum. It is unlikely that WISPs as they exist today will be large enough to be considered as LSPs for the GSPs.

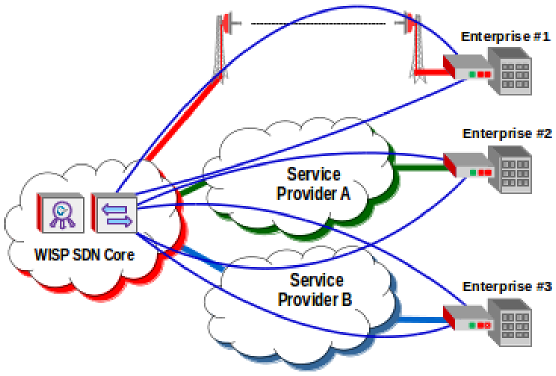

Figure 3: WISP aggregator.

The future WISP will need to become an aggregator as illustrated in Figure 3. WISPs will provide the services of other providers while continuing to plug coverage gaps with their own products. WISPs can find a niche acting to provide enterprise services where they offer seamless services using the networks and services of a number of providers by leveraging SD-WAN principles. WISP survival will require either becoming large enough to act as an LSP in its own right for GSPs or act as a partner of an existing LSP to provide extended reach to plug gaps in their coverage.
To achieve this, investment in a smart core network based on SDN to provide seamless services across their own network as well as the networks of other providers is required. Customers will be connected to the WISP core using vCPEs. The SDN network will also allow for slicing to allow GSPs to extend to their customer connected with their vCPEs and provide adequate separation in terms of privacy.

References

[1] M. K. Weldon, *The Future X Network: A Bell Labs Perspective*. CRC PressINC. 00000.

[2] N. Chatzis, G. Smaragdakis, J. Böttger, T. Krenc, and A. Feldmann, "On the benefits of using a large IXP as an internet vantage point," in *Proceedings of the 2013 conference on Internet measurement conference*, pp. 333–346, ACM.

[3] N. Chatzis, G. Smaragdakis, A. Feldmann, and W. Willinger, "Quo vadis open-IX?," vol. 45, no. 1, pp. 12–18.

[4] M. Mahalingam, D. Dutt, K. Duda, P. Agarwal, L. Kreeger, T. Sridhar, M. Bursell, and C. Wright, "Virtual extensible local area network (VXLAN): A framework for overlaying virtualized layer 2 networks over layer 3 networks,"

[5] P. I. Beijnum, I. Van Beijnum, and O. Bgp, "Reilly & associates," 00015.

[6] V. Sekar, N. G. Duffield, O. Spatscheck, J. E. van der Merwe, and H. Zhang, "LADS: Large-scale automated DDoS detection system.," in *USENIX Annual Technical Conference, General Track*, pp. 171–184. 00091.

[7] S. K. Fayaz, Y. Tobioka, V. Sekar, and M. Bailey, "Bohatei: flexible and elastic DDoS defense," in *24th USENIX Security Symposium (USENIX Security 15)*, pp. 817–832. 00000.

[8] F. Phillipson, "Planning of fibre to the curb using g. fast in multiple roll-out scenarios," vol. 2, no. 1.

[9] A. Al-Dulaimi, S. Al-Rubaye, Q. Ni, and E. Sousa, "5g communications race: pursuit of more capacity triggers LTE in unlicensed band," vol. 10, no. 1, pp. 43–51.

[10] A. Mukherjee, J.-F. Cheng, S. Falahati, L. Falconetti, A. Furuskar, B. Godana, H. Koorapaty, D. Larsson, and Y. Yang, "System architecture and coexistence evaluation of licensed-assisted access LTE with IEEE 802.11," in *Communication Workshop (ICCW), 2015 IEEE International Conference on*, pp. 2350–2355, IEEE.