

Software Based Traffic Separation at the Access Layer

Yona Andegelile*, Nixon Mtonyole**

*(Department of Computer Science and Engineering, University of Dar es Salaam, Tanzania)

** (Department of Telecommunications and Communications Networks, University of Dodoma, Tanzania)

ABSTRACT

Access Network is the subscriber part of the telecommunications network or the network connecting the subscribers to the Internet Service Providers (ISP) [1]. In many countries including Tanzania access network is still predominantly made up of the copper cable based or other point to point wireless connections. This has kept the network in large proportions passive, inflexible and relatively unreliable [2]. This traditional network has long been tailored to the services generally provided i.e. voice, leased lines, Internet, corporate data and video conference, sometimes each provided by separate equipment and networks.

This paper presents the study on approaches used by ISP in Tanzania to separate traffic in the access network. The paper also presents the effective way of traffic separation, whereby multiple hardware used to separate traffic currently has been replaced with single hardware. The traffic separation technique is based on creating logical links (software based) for each traffic type inside single physical link, providing a differentiated QoS support for each type of traffic according to its individual QoS requirements.

Keywords - Access network, ISP, QoS parameters

I. INTRODUCTION

In many countries including Tanzania access network is still predominantly made up of the copper cables or other point to point wireless connections [3]. This has kept the network in large proportions passive, inflexible and relatively unreliable [4]. This traditional network has long been tailored to the services generally provided i.e. voice, leased lines, Internet, corporate data and video conference, sometimes each provided by separate equipment and networks.

At ISPs core network, Virtual Private Networks (VPNs) have been implemented to separate these different services for different customers, and thus managed to provide bandwidth per service demand. Still there is problem on the access part where separate point-to-point links are used to separate traffic.

Software based traffic separation is a traffic separation techniques which replaces the multiple hardware's approach of separating traffic at the access layer with the single hardware but traffic separated at software level, hence the name software based traffic separation. In this approach all traffic types are passed in the same physical link but logically separated (separated on software level). Each kind of traffic is being delivered to the customer's premises with the same QoS guarantee (e. g bandwidth and delay) as when using separated physical link.

II. CHARACTERISTICS OF THE EXISTING NETWORK

In existing network, each service class is having its own link leading to unnecessary deployment and maintenance cost, also network management is also difficult due to the fact that, links are on different physical interfaces on the customer router, if any security aspect has to be implemented, it should be applied separate on each interface. With equipment duplicated for each service; scalability also becomes difficult in the existing network.

III. CHARACTERISTICS OF THE EXPECTED NETWORK TRAFFIC

Traffic passing through the network is larger file transfer between branches, Internet upload and download and voice calls between branches. The expected network is flexible in the fact that, each traffic class can be given priority according to its sensitivity.

IV. LOGICAL NETWORK DESIGN

4.1 Network topology

MPLS backbone carries customer traffic from headquarter to branches and between branches. This is owned by service provider, and consists of four stations country wide each having PE routers at which customers are connected as shown in Fig 1. At the back bone, QoS is guaranteed for each traffic class according to Service Level Agreement (SLA) with a customer. Customer's branches are connected to nearest nodes. PE edge router, each traffic type is given its own class.

CE is customer router located at customer area. At this router uplink traffic is assigned a class according to traffic type. Between PE and CE, one physical link is established, and logical links are created based on traffic types being carried by the link.

At customer site, there is switch, in which end equipments are connected to, end equipment can be VoIP phone or computer for accessing Internet or data upload and download. A trunk port is created on the interface connecting to the CE router for the purpose of carrying all VLANs traffic. At WiMAX BS logical links are created within a single physical link, and each profile management is done per traffic type i.e. each class

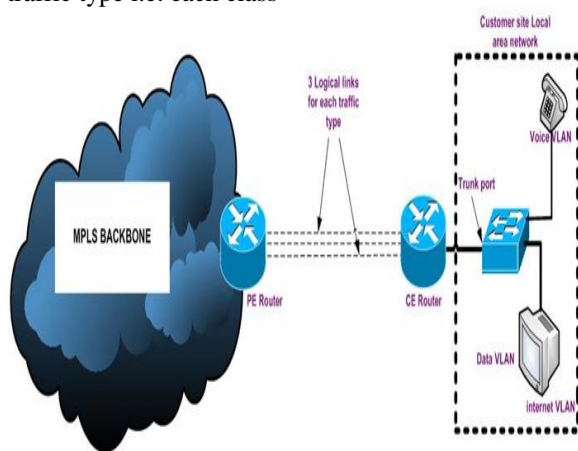


Figure 1. Logical Network Design

4.2 Models for addressing and naming

A customer has been provided with one IP version 4 (IPV4) address on the router and a default gateway for each service, each CPE was assigned IP address from address block reserved for WiMAX CPEs. Names were assigned according to company name and site name. Inside customer network, each traffic class assigned to a specific VLAN, a trunk port is configured on switch interface connecting to the router, at PE edge, marking is done for different traffic type, and same is done on customer router.

The IP address assignment was done to each traffic type in the sense that, each logical link was given a specific subnet. End user equipment addresses were chosen from given LAN subnet.

4.2.1 Provider Network

Provider network include the link between customer edge and the backhaul network. Vlan 40 was assigned to carry data traffic and given sub network IP address as follows.

VLAN 40
 Network 192.168.2.208
 Mask 255.255.255.240

Vlan 500 was assigned to carry Internet traffic and given sub network IP address as follows.

VLAN 500
 Network 41.223.4.128
 Mask 255.255.255.128

Vlan 172 was assigned to carry VOIP traffic and given sub network IP address as follows.

VLAN 172
 Network 192.168.2.16
 Mask 255.255.255.240

4.2.2 Test Site Local Area Network

Customer site LAN include customer edge router, LAN switch and end user equipments.

Data
 VLAN 40
 Network 192.168.2.0
 Mask 255.255.255.0

Vlan 500 was assigned to carry Internet traffic and given sub network IP address as follows. End user computer must also be configured with DNS server to query. Configurations were as follows.

VLAN 500
 Network 192.168.100.0
 Mask 255.255.255.0
 Primary DNS 41.223.4.96
 Secondary DNS 41.223.5.33

Vlan 62 was assigned to carry VOIP traffic and given sub network IP address as follows.

VLAN 62
 Network 10.10.100.0
 Mask 255.255.255.0

4.3 Switching, routing protocols, security strategies and Network management

Dynamic routing has been used at Core network to easy administrator task and network scalability, BGP routing protocol has been selected because, customers and provider networks must appear on different Autonomous systems. For point-to-point between PE and CE, static route has been used; this is because there are no many IPs to learn between test customer and PE [6].

Traffic has been encapsulated and tagged to enable access only for members within the VPN. Also using BGP as dynamic routing protocol serves as security approach due to the fact that, with BGP customer access to provider network is limited.

Traffic to BS was monitored at switch interfaces using NetQoS and SolaWinds , traffic to customer site was managed at BS, and all CPEs were managed at the BS.

4.4 Physical Network Design

4.4.1 Technologies and devices for the networks

WiMAX switch used was Cisco 2950 switch because of its high capacity to handle all BS traffic and its reliability [5]. WiMAX BS used was one

implemented by VODACOM, which is a case study for this paper. Equipment vender is therefore Nokia Siemens. Customer router used was Cisco 1900 router because of its capability to handle all originating and destining traffic. This was chosen to meet high speed, scalability and QoS requirement of customers. Additionally, Cisco router was chosen in preference because Cisco equipments are compatible with many Nokia Siemens products.

4.4.2 Physical network design

Physically the network has PE edge router connected to WiMAX switch (2950 WiMAX switch) as shown in the Fig 2. Switch has physical connection to Microwave transmitter (WIMAX Backhauls), which connect to WiMAX BS through Microwave link. Wireless link connect BS to CPE, which include ODU, IDU, and customer router and/or switch. 3750-01 and 3750-02 are switches which form part of provider network together with 7206-01 and 72006-02 provider edge routers.

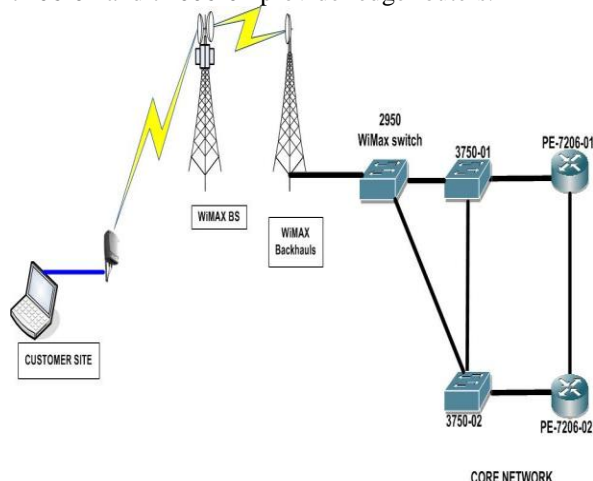


Figure 2. Physical Network Design

4.5 Testing, Optimizing, and Documenting the Network Design

4.5.1 Test the network design

The proposed network which support multiservice was implemented as per design and thereafter some tests to verify its workability followed. Few tests cases were used to verify performance of the link before implementing multiservice over single physical channel then each test case was performed after combining into single physical channel where by specified KPIs were compared. Test was done for Voice, Data and Internet as detailed bellow.

4.5.2 Voice

Voice has been tested for, Jitter, loss, Listening levels (clarity), Loudness Loss, delay in conversational and Talker echo Side tone.

Two computers laptops with 1GHz CPU, 1GB RAM and windows XP, Asterisk client application to act as

soft phone and bandwidth monitor to measure bandwidth. These have been installed with asterisk clients and then placed on two remote sides. One computer of the same specification has been installed with Asterisk server which has been used as soft PABX. Fig 3. shows set up for voice test case. Calls were initiated from one asterisk client, processed by server and reach the other client.

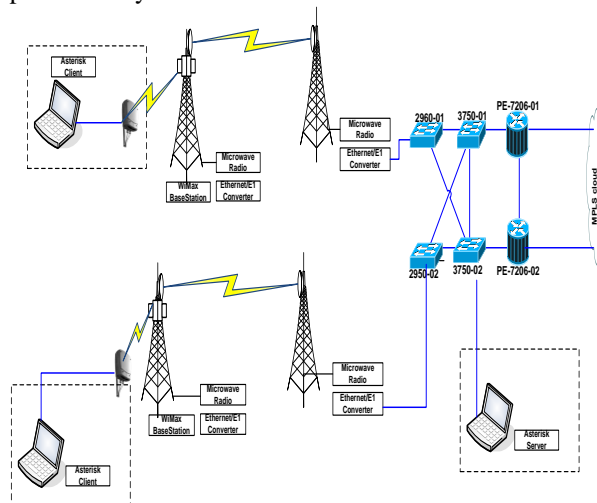


Figure 3. Set-up for Voice test case

4.5.3 Data

Data service has been tested for download speed, upload speed, delay and bandwidth allocated

One computer laptop with 1GHz CPU, 1GB RAM and windows XP, FTP client application used for download and bandwidth monitor to measure bandwidth. One computer has been installed with FTP server and bandwidth monitor, this was placed on one side then one computer of the same specification has been installed with FTP server and placed on provider side as shown in the Fig 4. Some ping results have been used to measure delay.

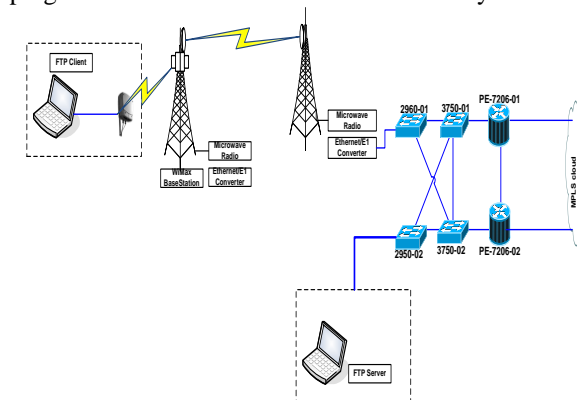


Figure 4. Set-up for Data test case

4.5.4 Internet

An Internet service has been tested for download speed and uploads speed, delay and bandwidth allocated.

One computer laptop with 1GHz CPU, 1GB RAM, windows XP and FTP client used for download and bandwidth monitor to measure bandwidth. FTP client has been placed on one network end. One computer on the Internet side has been used as FTP server. Some web browsing has been done to test BW, uplink speed and downlink speed. Some ping results were used to measure delay. Fig 5 shows set up for Internet test case.

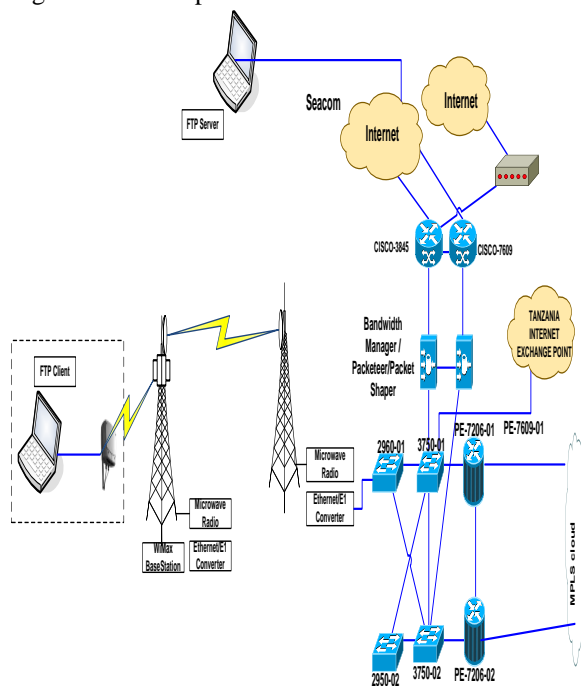


Figure 5. Set-up for Internet test case

4.5.5 Results summary

Voice throughput before implementation was constantly in average 87kbps, after implementation was constantly around 86kbps. Round Trip time to Asterisk server before implementation was average of 141ms, 1154ms maximum value and 70ms minimum value with no packet loss. After implementation, average was 611ms, with maximum of 1186ms, minimum of 124 and 1 packet loss.

Voice Quality measurement before implementation had max jitter of 74(Tolerable value), 0(good) delay, 1 packet loss, R factor of 92(good) and Mean opinion score of 4.4 which was good. After implementation, maximum jitter was 50(tolerable), maximum delay of 6ms, without any loss in packet, maximum R factor of 93, and mean opinion score of 4.4 .

Data throughput before implementation was in average 380kbps with little variations, after implementation was around 350kbps with variations. Round Trip time to FTP server before

implementation was average of 540ms, 1299ms maximum value and 57ms minimum value with 2 packet lost out of 197 transmitted. After implementation, average was 609ms, with maximum of 1198 ms, minimum of 63ms and 2 packet loss out of 109 transmitted.

Internet throughput before implementation was in average 511kbps with no variations, after implementation was around 510 kbps with no variations. Round Trip time to yahoo.com server before implementation was average of 329ms, 1406 ms maximum value and 329ms minimum value with no packet lost out of 96 transmitted. After implementation, average was 415ms, with maximum of 1508 ms, minimum of 338 ms and 3 packet loss out of 213 transmitted.

PE router voice interface utilization was very low on both cases.

Looking into comparison results before and after implementation, it can be proved that, performance of all links before and after were quite the same.

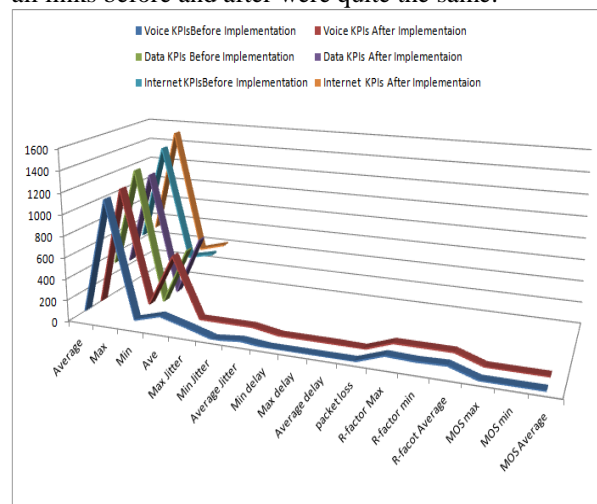


Figure 6. Summary of Results Output

All tests have been conducted successfully and results were collected, tabulated then summarized in the graph as shown in Fig 6. Note that, KPIs for various traffic types are differentiated by colours as shown in the diagram key. In summary there have been no large performance differences for all services when tested before and after implementation.

V. CONCLUSION

Finding simple, cheaper and scalable ways to deliver ICTs services to end user has been and is still a study where a lot of work has been done and is still being done. This paper looked at removing complexity in the last mile when ISP has to deliver multiservice to a client, in particular design and implement link in a way that all services are delivered through a single physical link, with the general idea being that this technology can give a new last mile implementation style, and that it's a

cheaper technically viable solution compared to, currently, methods being used.

Basic advantages accruing from such an implementation are, lowering implementation costs to both customers and providers, reducing complexity and costs in maintaining the network and reducing environmental pollution.

REFERENCES

- [1] Steven T. Karris, *NETWORKS Design and Management, Second Edition*, (ISBN 978-1-934404-16-4, Orchard Publications, 2009)
- [2] Telia AB, Ericsson AB, Studentlitteratur AB, *Understanding Telecommunications*, 2009.
- [3] William Stallings (2001), IEEE 802.11: Moving Closer to Practical Wireless LANs, *IT Professional*, vol. 3, no. 3, pp. 17-23.
- [4] Ericsson Telecom AB, Telia AB, Studentlitteratur AB, *Understanding Telecommunications 2*, pp. 223-225, 1998.
- [5] Allan Leinwand and Bruce Pinsky, *Cisco Router Configuration, Second Edition* (ISBN: 1-57870-241-0, Cisco Press, 2001)
- [6] Bennett Geoff, *Designing TCP/IP Internetworks*, (ISBN 0-4712-8643-5. John Wiley & Sons, 1997)