QoS-Aware Layer-2 VPNs over EPON-WIMAX

Ahmad R. Dhaini*, Pin-Han Ho*, Xiaohong Jiang†
*Department of Electrical and Computer Engineering, University of Waterloo
†Graduate School of Information Sciences, Tohoku University

***Abstract*—This paper proposes a novel framework for realizing layer-2 virtual private networks (VPNs) over the integration of Ethernet Passive Optical Networks (EPONs) and IEEE 802.16 (WIMAX). Layer-2 VPNs support a bundle of service requirements that are stipulated in the service level agreement (SLA) and should be fulfilled by a suite of effective bandwidth management solutions. For achieving this, we propose a novel VPN-based admission control (AC) and bandwidth allocation scheme that will provide per-stream QoS protection and bandwidth guarantee for real-time flows. The proposed AC is implemented on a three-stage system, which is involved in the collaboration among the users, base stations (BS), and service provider. The bandwidth allocation is performed via a common medium access control (MAC) protocol working in both the optical and wireless domains. An event-driven simulation model is implemented to study the effectiveness of the proposed framework.**

I. Introduction

The integration of Ethernet Passive Optical Network (EPON) and WIMAX has been lately presented as an attractive broadband access network (BAN) solution [1], [2]. The complementary features of these networks can take advantage of the bandwidth benefit of fiber communications, and the mobile and non-line-of-sight features of wireless communications.

Building up virtual private networks (VPNs) directly on the EPON-WIMAX integration has never been investigated in the literature. Such VPNs are referred to as *layer-2 VPNs* in the sense that the VPNs are built upon the layer-2 protocols. VPNs have been known as a superb technology that are provisioned over a public or third party network infrastructure, and are positioned to provide dedicated connectivity to a closed group of users with a strong per-flow quality-of-service (QoS) guarantee [3]. Compared with layer-3 VPNs, layer-2 VPNs can do a better job in resolving the complications due to network dynamics, communication media heterogeneity, and fast changing channel status, at the expense of a more complicated design that considers any possible layer-2 issue. Due to its support for premium services with custom-designed control, diverse QoS requirements and security assurance intrinsically provided by the layer-2 MAC protocols [3], building up layer-2 VPNs is considered the best suitable when an EPON-WIMAX integrated network is deployed. As an alternative, building up layer-1 VPNs on PONs was investigated in [4]. Nonetheless, the specific hardware technologies utilized cannot be applied over EPON-WIMAX due to the physical layer heterogeneity of the two systems. Supporting layer-2 VPNs entitles the emergence of resource management challenges; especially in the upstream/uplink shared media. To resolve these issues, the proposed framework serves as a new paradigm of VPN-based admission control (AC) and dynamic bandwidth allocation (DBA) that will provide guaranteed bandwidth for each VPN service. This paradigm will ensure and protect end-to-end QoS (i.e., in both the wireless and optical planes) for new and existing per-flow traffics, respectively, while maintaining their expected performance as defined in the service level agreement (SLA). To the best of our knowledge, this is the first work that considers the support of layer-2 VPNs over EPON or WIMAX and over the EPON-WIMAX integration as well.

The rest of the paper is organized as follows. The realization of layer-2 VPNs over EPON-WIMAX is presented in Section II, and its potential advantages and the related design issues are demonstrated. The proposed three-stage admission control (AC) framework is described in Section III, and the VPN-based dynamic bandwidth allocation (DBA) scheme is presented in Section IV. Section V presents the performance evaluation and we conclude in Section VI.

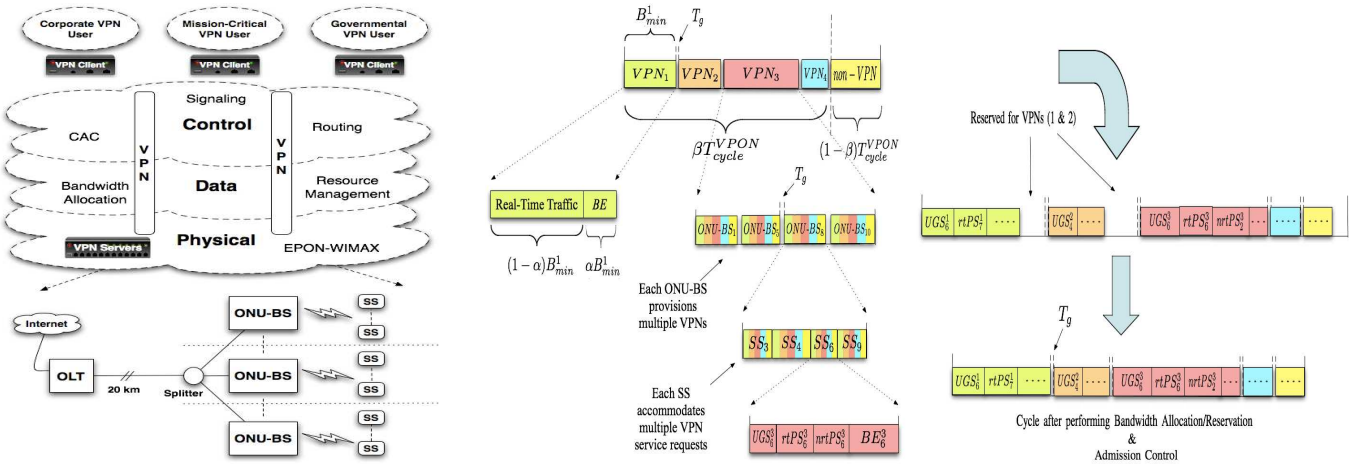
II. Layer-2 VPNs over EPON-WIMAX

A. Network Model

To support VPN services on EPON-WiMAX networks, one approach is to deploy VPNs in the network layer (i.e., IP layer) in the ONU-BSs. This is certainly at the expense of higher control and management overhead due to the protocol overlay and potentially longer delay. A layer-2 VPN over the EPON-WiMAX domain is expected to achieve a much more efficient and light-weight network management, which is necessary to support a multi-service and multi-customer environment. In the proposed framework, each VPN serves as a *shim layer* that maps those service requirements and commands to the MAC layer routing, resource allocation, and call admission control (CAC) mechanisms, via a suite of service access points (SAPs) and primitives. Typically, a VPN consists of three planes 1) control, 2) data and 3) physical. The control plane handles operations such as connection establishment, routing and call admission control. The data plane is concerned with the bandwidth management for VPN services and meeting their SLA-based QoS requirements. The physical plane is basically the underlying network infrastructure (here, EPON-WIMAX). The realization of multi-planed VPNs over EPON-WIMAX is illustrated in Fig. 1(a).

B. System Model

The integration of EPON-WIMAX requires the identification of multiple design and operation themes. In this section, we discern these matters in order to complete the support of layer-2 VPNs over EPON-WIMAX.



(a) Layer-2 VPN over EPON-WIMAX

(b) Proposed VPN-PON (VPON) Cycle Framework

Fig. 1. QoS-Provisioned Layer-2 VPNs over EPON-WIMAX

1) Wireless Channel Model: The wireless channel is modeled as Rayleigh fading channel [5] that is suitable for flat-fading channels as well as frequency-selective fading channels encountered with orthogonal frequency division multiplexing (OFDM). We assume that multiple transmission modes are available, with each mode representing a pair of a specific modulation format and a forward error correcting (FEC) code. Based on the channel state information (CSI) estimated at the receiver, the adaptive modulation and coding (AMC) controller determines the modulation-coding pair/mode, which is sent back to the transmitter through a feedback channel for the AMC controller to update the transmission mode. In our framework we adopt the seven transmission modes of the HIPERLAN/2 and the IEEE 802.11a standards [6]. We also adopt the OFDM-TDMA air interface for the wireless channel access [2]. For a transmission mode x, the transmission rate for an SS n is noted as R_n^x.

2) QoS Mapping: The IEEE 802.16 standard defines five classes of services, namely Unsolicited Grant Service (UGS), real-time Polling Service (rtPS), extended real-time Polling Service (ertPS, defined in 802.16e), non-realtime Polling Service (nrtPS) and best-effort (BE) [5]. On the other hand, an 802.3ah optical network unit (ONU) is allowed to support and report up to eight queues. Typically, three classes of services are supported in an EPON: (1) Expedited Forwarding (EF) for constant bit rate (CBR) traffic (2) Assured Forwarding for variable bit rate (VBR) traffic, and (3) BE [7]; each assigned one buffering queue. To simplify the bandwidth allocation operation, we perform a one-to-one mapping between the classes of service (CoS) queues in the WIMAX's BS and the ones in the ONU [2]. Hence each mounted ONU-BS will have totally five queues for all classes of services.

3) Requesting and Granting: *Requesting* and *granting* are two fundamental operations standardized in EPON and WIMAX [5], [7], and are used to exchange bandwidth allocation control messages. In the wireless plane, the *polling mode* is adopted to achieve better sensitivity in QoS guarantee. The polling mode enables every ONU-BS to poll its SSs in each OFDM frame so as to gather the bandwidth requirement of each SS. Once available, each ONU-BS performs the proper bandwidth allocation and the granting in a Grant Per Connection (GPC) fashion [5]. In the optical plane and according to multi-point control protocol (MPCP), each ONU is allowed to request bandwidth for up to 8 queues in each REPORT message in every cycle. To preserve the REPORT structure, each ONU-BS will report the buffering queue occupancies for real-time flows, and will use the remaining four fields to report up to four BE VPN bandwidth needs. If an ONU-BS provisions more than four VPNs, multiple REPORT messages may be used to report the rest of VPNs. On the other hand, a GATE message includes a grant for each real-time buffer request and an aggregate grant for VPN BE traffic requests, for defining the transmission window in the next cycle.

C. VPN-based QoS provisioning

With our QoS provisioning framework, each upstream VPN-PON cycle T_{cycle}^{VPON} is divided into two *sub-cycles*. The first sub-cycle βT_{cycle}^{VPON} is shared among all the K VPNs. The second sub-cycle $(1-\beta)T_{cycle}^{VPON}$ is shared among non-VPN services. Let B_{min}^k be the bandwidth reserved for VPN k (denoted as V_k) in each transmission cycle. T_g denotes the guard time that separates the transmission windows of two consecutive ONU-BSs, and R_N the transmission speed of PON in Mbps. In addition, let each V_k be given a weight w_k to determine its *paid/committed* bandwidth. Therefore, B_{min}^k (in bytes, therefore divide by 8) can be computed as follows:

$$B_{min}^k = \frac{(\beta T_{cycle}^{VPON} - K \times T_g) \times R_N \times w_k}{8}, \text{where} \left(\sum_{k=1}^{K} w_k = 1 \right). \quad (1)$$

An important parameter in the proposed cycle framework is the minimum per-VPN throughput that allows the BE traffic to be free from starvation. Such reserved quota for BE traffic takes a portion of αB_{min}^k, while the real-time flows will share

the remaining bandwidth, that is $(1-\alpha)B^k_{min}$.
A graphical illustration and example of the proposed VPON cycle is given in Fig. 1(b). Here, once all the QoS metrics are specified at both the ONU-BS and the optical line terminal (OLT), a "proper" bandwidth allocation is performed, and a VPN-based cycle is formed.

D. Traffic Characteristics and QoS Requirements

CBR traffic (such as UGS) is non-bursty and can be simply characterized by its mean data rate (μ) in bits per seconds (bps). On the other hand, VBR traffic (such as rtPS and nrtPS) is bursty in nature and is characterized by the following parameters: 1) Peak Arrival Data Rate (σ) in bits per second (bps), 2) Maximum Burst Size (ρ) in bits, 3) Delay Bound (θ) which is the maximum amount of time in units of seconds allowed to transport a traffic stream, and 4) MAC service data unit (MSDU) maximum and minimum sizes (L_{max} and L_{min}). For fixed frame size streams of size L, the mean frame size $\bar{L}$ = L. Finally, BE traffic is bursty and requires neither delay requirements nor bandwidth guaranteed. For CBR traffic, a flow may be admitted in case its mean data rate can be supported by the current system. For VBR traffic, the AC may admit a VBR stream according to either its peak rate or its mean data rate [8], which obviously causes a dilemma between the boost of network utilization and a more secured service guarantee, respectively. With the proposed framework, we define a suite of new traffic parameters via a dual-token bucket model for traffic regulation. The dual-token bucket is situated at the entrance of the MAC buffer and is associated with each stream. The bucket size is defined by $S = \rho \times (1-\mu/\sigma)$. Accordingly, the arrival process of the stream passing through the filter is computed as follows [8], [9]: $A(t, t+\tau) = \min(\sigma\tau, S+\mu\tau)$. Where $A(t, t+\tau)$ is the number of cumulative arrivals during $(t, t+\tau)$. The arrival rate curve could be constructed from the above equation. Therefore, the guaranteed rate for every real-time flow i belonging to V_k can be easily derived using the distance formula [8], [9]:

$$g^k_i = \frac{\rho_i}{\theta^k_i + \frac{\rho_i}{\sigma_i}} \tag{2}$$

In the wireless domain, transmissions are error-prone due to fluctuating channel conditions. Hence, one may compute a larger guaranteed rate than the one used in the optical domain. By assuming a frame error probability $P_{error,i}$ for stream i, the guaranteed rate can then be obtained as follows:

$$g^k_i = \frac{\rho_i}{(\theta^k_i + \frac{\rho_i}{\sigma_i})(1-P_{error,i})} \tag{3}$$

Similarly, the transmission rate for statistical guarantee of a CBR flow perceived bandwidth pertaining to a specific frame error rate, $P_{error,i}$, can be obtained as follows:

$$g^k_i = \mu_i(1-P_{error,i}) \tag{4}$$

Note that $P_{error,i}$ is a function of the channel condition (i.e., the signal-to-noise ratio, SNR), which is random in nature.
Due to the fact that V_k could be simultaneously provisioned at multiple ONU-BSs, the AC decision making needs to consider the network architecture and the subscriber stations' (SSs) distribution. For this reason, we propose a three-stage AC, where the SSs, ONU-BSs and OLT collaboratively perform AC to satisfy the conditions defined in Eqs. (3) and (4).

III. Three-Stage Admission Control Mechanism

This section describes the proposed three-stage admission control mechanism for real-time flows. Note that the BE traffic requests are always admitted. The admitted flows will be further distinguished according to a dynamic bandwidth allocation algorithm (which will be provided in Section IV).

A. SS-based Admission Control (SAC)

Let M_k be the number of ONU-BSs that provision VPN V_k and share the total allocated bandwidth αB^k_{min} for maintaining the minimum BE bandwidth. Each ONU-BS is allocated an equal portion of the currently available bandwidth at the OLT for the BE traffic of V_k, namely $\frac{\alpha B^k_{min}}{|M_k|}$. This information is broadcasted by the OLT to all the ONU-BSs in the registration phase. Let $R^k_{j,BE}$ denote the rate (in bps) reserved for BE traffic of V_k at each ONU-BS j, which can be expressed as:

$$R^k_{j,BE} = \frac{\alpha B^k_{min} \times 8}{|M_k| \times \beta T^{VPON}_{cycle}} \tag{5}$$

Let N_k denote the number of SSs using the services of V_k via ONU-BS j. Thus, the reserved BE rate for each user n of V_k at ONU-BS j, which is denoted as $R^{n,k}_{j,BE}$, and expressed as:

$$R^{n,k}_{j,BE} = \frac{\alpha B^k_{min} \times 8}{|N_k| \times |M_k| \times \beta T^{VPON}_{cycle}} \tag{6}$$

By applying measurement-based AC [8], a new real-time (RT) flow $i+1$ by SS n could be admitted to VPN V_k at ONU-BS j if the following condition is satisfied:

$$g^k_{n,i+1} + \sum_k (\sum_i g^k_{n,i} + R^{n,k}_{j,BE}) \leq R^x_n \tag{7}$$

where $g^k_{n,i+1}$ is the guaranteed rate (bps) for the flow computed according to either Eq. (3) or (4).
Using SAC, a new flow is admitted at the SS-side if its guaranteed bandwidth plus the already existing traffic (real-time and best effort) is less than or equal to the SS PHY transmission rate.

B. ONU-BS-based Admission Control (OBAC)

Once a flow is conditionally admitted at the SS level, it is reported to its connected ONU-BS j. The ONU-BS then locally performs rate-based AC according to the bandwidth requirement of the arriving flow along with the overall wireless bandwidth availability. The condition for flow $i+1$ of V_k from SS n to be admitted at ONU-BS j is defined as follows.

$$\frac{g^k_{n,i+1}}{R^x_n} + \sum_k \sum_n \sum_i \frac{g^k_{n,i}}{R^x_n} \leq NBR - \sum_k \sum_n \frac{R^k_{n,BE}}{R^x_n} \tag{8}$$

Here *nominal bandwidth ratio* is defined as $NBR = (1 - C_o)$, where C_o represents the control overhead ratio caused by

the signaling required to perform resource allocation and will be evaluated via simulations. $\frac{g^k_{n,i}}{R^x_n}$ is the ratio of channel rate required to transmit flow i of V_k in one-second time interval at SS n. If sufficient bandwidth is available to accommodate the flow, it will be reported to the OLT for the final stage of AC in the VPN level.

C. OLT-based Admission Control (OLAC)

After passing the first and second stages, flow $i+1$ is admitted by the OLT if sufficient bandwidth is available in V_k. The condition of admission is defined as follows:

$$g^k_{i+1} + \sum_i g^k_i \leq \frac{(1-\alpha)B^k_{min} \times 8}{\beta T^{VPON}_{cycle}} \tag{9}$$

In summary, the proposed three-stage AC scheme is used to achieve end-to-end (from SS to OLT) bandwidth guarantee for each admitted flow. It is designed for the scenario where the users of a VPN may connect to any ONU-BS, but are not allowed to utilize more bandwidth than their predefined bandwidth share in the upstream channel.

As a complement to the AC scheme in the course of per-flow QoS guarantee, we provide a VPN-based dynamic bandwidth allocation (VPN-DBA) scheme and will be introduced next.

IV. VPN-based Dynamic Bandwidth Allocation (VPN-DBA)

The proposed VPN-DBA is installed at both OLT and ONU-BSs, in order to arbitrate the transmission of ONU-BSs and SSs over the shared upstream and uplink channels. Moreover at the ONU-BS, VPN-DBA takes into consideration different channel conditions of each SS reported through the CSI, where the allocated time share is adaptive to the fluctuating channel condition in order to achieve the desired bandwidth guarantee. To determine the time share for a flow, each ONU-BS j calculates the aggregated rates of the admitted real-time flows (denoted as $G_j = \sum_k \sum_i g^k_i$), as well as the total reserved VPN BE rates (denoted as $R_{j,BE}$) by the following :

$$R_{j,BE} = \sum_k R^k_{j,BE} \times \epsilon_k \tag{10}$$

where ϵ_k is a binary integer, such that $\epsilon_k = 1$ if an SS belonging to V_k is available, and 0 otherwise.

In our scheme, each cycle/frame is divided into $K+1$ sub-cycles, where sub-cycle 1 is for real-time flows, while the rest K sub-cycles are for all VPNs' BE traffic. The size of each sub-cycle should be determined in each polling interval so as to adapt to the bandwidth request fluctuation of each flow. Thus, $T^{802.16}_{RT}$ (i.e., the sub-cycle assigned to real-time flows) can be computed as follows:

$$T^{802.16}_{RT} = \frac{G_j \times T^{802.16}_{cycle}}{G_j + R_{j,BE}} \tag{11}$$

Where $T^{802.16}_{cycle}$ is the total wireless cycle/frame length/duration. In addition, the proposed AC scheme differentiates the SSs with real-time flows from those who only have BE flows. For a real-time SS n, the time share in the real-time sub-cycle $T^{802.16}_{n,RT}$ is expressed by:

$$T^{802.16}_{n,RT} = \frac{(1/R^x_n) \times T^{802.16}_{RT}}{(1/\sum R^x_{n,RT})} \tag{12}$$

Where R^x_n is the computed transmission rate for SS n, and $\sum R^x_{n,RT}$ is the sum of transmission rates for all real-time SSs. The inverse of the transmission rate is used because an SS with lower transmission rate requires more time share to transmit an admitted flow rate. The computation of each BE V_k sub-cycle $T^{802.16}_{n,k}$ is done in the same manner.

Next and based on the admitted flow rate and reported frame size, our scheme estimates the amount of bandwidth required to satisfy each admitted flow in each frame. Thus, the estimated bandwidth $B^g_{i,n}$ for real-time flow i launched by SS n in each polling interval is determined as:

$$B^g_{i,n} = \frac{g_i \times R^x_n \times T^{802.16}_{n,RT}}{G_j \times 8} \tag{13}$$

To explore the bandwidth usage of each frame and avoid any possible resource waste, the number of packets per polling cycle estimated for flow i, denoted as $np_{i,n}$, is first obtained by $np_{i,n} = \left\lceil \frac{B^g_{i,n}}{\bar{L}_i} \right\rceil$, where $\bar{L}_i$ is the average packet size as defined in section II-D. Thus, the allocated bandwidth for flow i in the next cycle/frame, B^{alloc}_i, is then computed as follows:

$$B^{alloc}_{i,n} = \min(np_{i,n} \times \bar{L}_i, r_{i,n}) \tag{14}$$

where $r_{i,n}$ is the requested bandwidth for real-time flow i (i.e., the buffering queue occupancy) by SS n in each polling interval. UGS traffic needs not to be requested. Hence, the ONU-BS may periodically grant it the desired bandwidth.

With OFDM, one physical symbol may carry different bits of MAC layer data according to channel condition that in turn affects the modulation scheme employed. Therefore, each ONU-BS has to convert the allocated bandwidth into number of symbols accordingly. The number of OFDM symbols required for flow i by SS n, denoted as $F_{i,n}$, is computed as follows [2]: $F_{i,n} = \frac{B^{alloc}_{i,n} \times 8}{\phi_x}$, where ϕ_x represents the number of bits per OFDM symbol. For BE traffic, the allocated bandwidth $B^{alloc}_{BE,n}$ is determined in the same approach as follows:

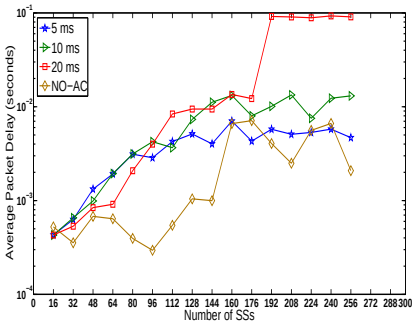
$$B^{alloc}_{BE,n} = \min\left(\frac{R^x_n \times T^{802.16}_{n,k}}{8}, r_{BE,n}\right) \tag{15}$$

where $r_{BE,n}$ is the requested bandwidth for BE traffic in each polling interval.

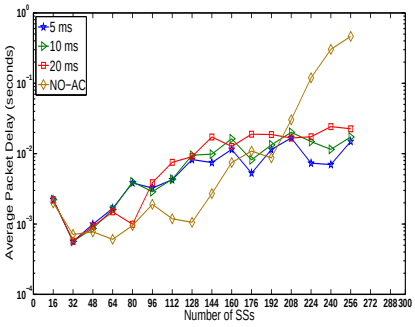
The computation of VPN-DBA at the OLT is done in the same fashion with the same transmission rate for all ONU-BSs and with βT^{VPON}_{cycle} instead of $T^{802.16}_{cycle}$.

V. Performance Evaluation

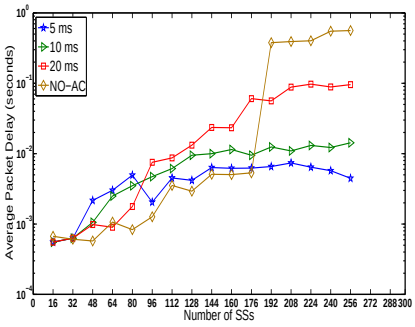
To evaluate the effectiveness of the proposed AC and DBA algorithms, we have developed a simulator using OMNET++. The total number of ONU-BS $(M) = 16$. The WIMAX total bandwidth is equal to $20MHz$ and PON's to $1\ Gbps$. Each PON's upstream cycle is $\leq 2\ ms$. $\beta = 1$ and it implies



(a) UGS Flow

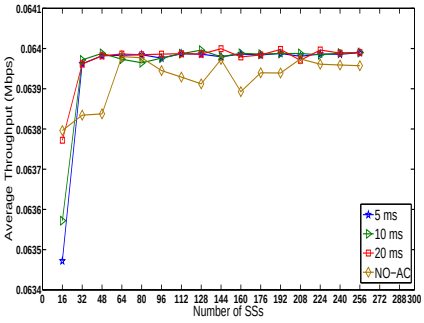


(b) rtPS Flow

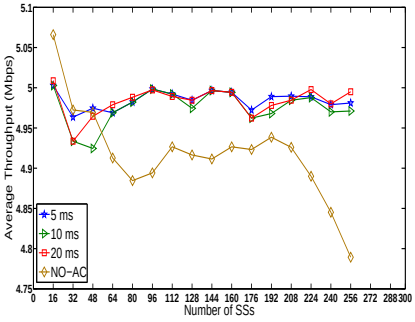


(c) nrtPS Flow

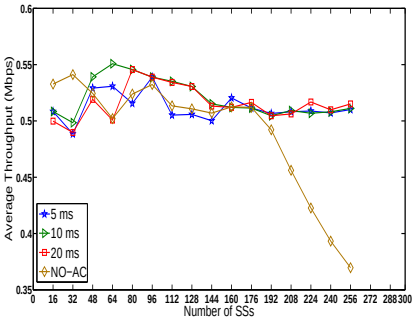
Fig. 2. Average End-to-End Packet Delay



(a) UGS Flow



(b) rtPS Flow



(c) nrtPS Flow

Fig. 3. Average End-to-End Throughput

that "non-VPN" traffic is NOT considered, and therefore the available bandwidth is divided among $K = 4$ VPNs; such that V_k is randomly generated for each incoming SS. Without loss of generality, we assume that all VPNs have equal weights (w_k). As a result, each VPN is reserved a total of $249.5\ Mbps$, out of which, $24.95\ Mbps$ are reserved for BE traffic (for $\alpha = 0.1$). To test the resilience of our proposed algorithms in handling fluctuating channel conditions, we consider various transmission modes for different SSs. The transmission mode of each SS is randomly generated ($x = random(1, 7)$). In addition, we simulate with multiple OFDM frame lengths (5, 10 and 20 ms), in order to show how this affects the overall network performance in terms of end-to-end (from SS to OLT) flow throughput and end-to-end average packet delay. Each incoming SS has four flows (UGS, rtPS, nrtPS and BE). Every UGS flow is generated with a mean/guaranteed rate of $64\ Kbps$ [5]. Each rtPS flow is generated at a guaranteed rate of $5\ Mbps$ (which is the average bit rate of a DVD-quality video [8]) and each nrtPS flow is generated at a guaranteed rate of $500\ Kbps$ [5]. Each self-similar pareto-shaped BE flow is generated at a mean rate of $2\ Mbps$. Packet sizes are uniformly distributed between 64 and $1518\ bytes$. The maximum allowable latency for voice traffic is $100\ ms$, and for video traffic is $150\ ms$ [5]. The number of SSs used in the figures increments by $|M|$ with time and reflects the arrival of a new SS in time to each ONU-BS simultaneously.

To apply the AC rule at the ONU-BS (eq. 8), we first extract NBR that is computed as follows: NBR = Total Throughput/Transmission Rate $= 59.0976$ Mbps$/64.8$ Mbps $= 0.912$. For a more conservative AC, we set $NBR = 0.9$. To study the performance of real-time traffic, we measure the instantaneous average packet delays of a selected SS's real-time flows. Figs. 2(a), 2(b) and 2(c) show these measurements with AC (i.e., VPN-DBA) and without AC (i.e., NO-AC). Note that with VPN-DBA, there is no intra-scheduling required since the bandwidth is allocated for each CoS. On the other hand with NO-AC, we apply strict priority (SP) scheduling [2].
Clearly using SP, UGS traffic shows the optimal performance where its average packet delay remains under $2 - 10\ ms$ even when the number of SSs continuously increases, regardless of the OFDM frame length. This is a direct result of the SP policy which always selects packets from a queue with a higher priority. As for VPN-DBA, it makes sure to satisfy the QoS requirements by reserving every real-time traffic with appropriate bandwidth in every cycle. Since a UGS flow is admitted only if its guaranteed bandwidth is assured in every cycle, we can see that with VPN-DBA, UGS traffic witnesses a delay variation that is affected by the OFDM frame length; where the delay might reach $\approx 90\ ms$ with a $20\ ms$ frame size. This is due to the fact that the bandwidth is allocated to each SS with respect to its transmission rate, and hence the cycle might saturate because some SSs have requested for

more OFDM symbols than others to support the required flow rate. Nonetheless, VPN-DBA still maintains a UGS packet latency less than the maximum allowable one (i.e., $\leq 100\ ms$). As for rtPS and nrtPS traffics, Fig. 2(b) and 2(c) demonstrate that VPN-DBA maintains their delay performance to meet the specified target QoS requirements of the stream (i.e., $\leq 150\ ms$) while the delay witnesses an exponential increase with NO-AC; especially after system saturation (number of SSs $= 192$). This behavior highlights the need for the application of AC in layer-2 VPNs over EPON-WIMAX, because when the system reaches saturation and all the arriving streams are admitted, the performance is no longer maintained. On the other hand, the deployment of AC allows for a bandwidth guaranteed service with guaranteed protected QoS that will meet the VPN SLA and maintain it. We further evaluate the proposed VPN-AC framework by measuring the throughput of one flow from each CoS of a common SS with AC (i.e., VPN-DBA) and with No-AC. It is demonstrated in Fig. 3 that the selected UGS flow exhibits similar performance behavior to that with No-AC, whereas the selected rtPS and nrtPS flows show different behaviors. Here, rtPS and nrtPS flows with AC maintain their derived $5\ Mbps$ and $500\ Kbps$ throughputs respectively throughout the simulation, even after the system saturation. On the other hand, when NO-AC is applied, these flows do not show a stable throughput behavior. Moreover, when the system reaches saturation, their throughput start decreasing. This is due to the fact that when more real-time flows are admitted and no AC is applied, the bandwidth that was guaranteed for the already admitted flows (before saturation) is now shared among more flows. Hence, the bandwidth is no longer guaranteed for the already admitted flows and for the newly admitted ones. This, again, shows the effectiveness of our AC framework in stabilizing and guaranteeing the throughput for all admitted flows by rejecting the flows that will break this theme. Furthermore, our framework proves that no matter what channel condition each user possesses, it can still provide its flows with the guaranteed bandwidth. This is achieved by allocating more OFDM frames to transmit the same flow rate, as described before. We now study the performance of BE traffic under different OFDM frame lengths. Since BE has no QoS requirement in terms of delay [5], we show the total BE throughput in Fig. 4, which is highly affected by the OFDM frame length. For example, with $5\ ms$ frame length, $VPN\ 3$ yields a total throughput of $10\ Mbps$ knowing that its reserved one is $24.95\ Mbps$. The total throughput increases to reach $\approx 25.5\ Mbps$ when the frame length is increased to $20\ ms$. This is due to the fact that with a smaller frame size, the VPN BE sub-cycles portion of one SS might be smaller than the head-of-line (HOL) packet in its BE queue. As a result, not only those packets cannot be transmitted, but they could be successively blocked from being transmitted; and therefore, the throughput is suppressed. On the other hand, with a larger frame length, each VPN BE sub-cycle will be large enough to accommodate most packet sizes for all SSs, and hence the throughput can reach as high as $\approx 24.95\ Mbps$ (i.e., the reserved one). This again shows

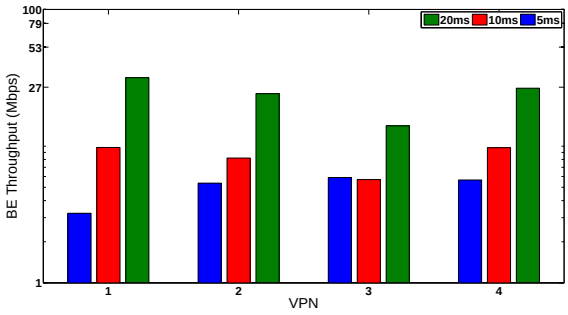


Fig. 4. Per-VPN BE End-to-End Throughput

that our proposed framework can achieve the desired/expected performance for all types of traffic, if the network parameters are set properly.

VI. Conclusion

This paper serves as the first research effort for exploring layer-2 VPNs over the EPON-WIMAX integration. The proposed framework implements novel three-stage AC and VPN-based DBA schemes, in order to achieve end-to-end bandwidth guaranteed. To validate the effectiveness and the robustness of our framework, extensive simulations were conducted, which demonstrated an improved performance in terms of maintaining the QoS requirements of the existing flows while providing an overall per-VPN acceptable minimal throughput for BE traffic even at network saturation. We conclude that the proposed framework is a promising candidate for the operation of future EPON-WIMAX access networks.

References

[1] G. Shen, R. S. Tucker, and C.-J. Chae, "Fixed Mobile Convergence Architectures for Broadband Access: Integration of EPON and WiMAX," *IEEE Communications Magazine*, vol. 45, no. 8, pp. 44–50, Aug. 2007.

[2] K. Yang, S. Ou, G. Ken, and H.-H. Chen, "Convergence of Ethernet PON and IEEE 802.16 Broadband Access Networks and its QoS-Aware Dynamic Bandwidth Allocation Scheme," *IEEE Journal of Selected Areas in Communications (JSAC)*, vol. 27, no. 2, pp. 101–116, Feb. 2009.

[3] W. Luo, C. Pignataro, A. Y. H. Chan, and D. Bokotey, "Layer-2 VPN Architecture," *CISCO Press*, 2005.

[4] N. Nadarajah, E. Wong, and A. Nirmalathas, "Implementation of Multiple Secure Virtual Private Networks Over Passive Optical Networks Using Electronic CDMA," *IEEE Photonics Technology Letters*, vol. 18, no. 3, pp. 484–486, February 2006.

[5] J. G. Andrews, A. Ghosh, and R. Muhamad, *Fundamentals of WIMAX: Understanding Broadband Wireless Networking*. Prentice Hall, 2007.

[6] A. Doufexi, S. Armour, M. Butler, A. Nix, D. Bull, and J. McGeehan, "A Comparison of the HIPERLAN/2 and IEEE 802.11a Wireless LAN Standards," *IEEE Communications Magazine*, vol. 37, no. 12, pp. 172–180, May 2002.

[7] G. Kramer, B. Mukherjee, and G. Pesavento, "IPACT A Dynamic Protocol For An Ethernet PON (EPON)," *IEEE Communications Magazine*, vol. 40, no. 2, pp. 74–80, February 2002.

[8] C.-T. Chou, S. S. N, and K. G. Shin, "Achieving Per-Stream QoS with Distributed Airtime Allocation and Admission Control in ieee 802.11e Wireless LANs," in *Proceedings of IEEE INFOCOM'05*, April 2005, pp. 1584 – 1595.

[9] A. R. Dhaini, C. M. Assi, M. Maier, and A. Shami, "Per-Stream QoS and Admission Control in Ethernet Passive Optical Networks (EPONs)," *IEEE/OSA Journal of Lightwave Technology (JLT)*, vol. 25, no. 7, pp. 1659–1669, July 2007.