Design of Guaranteed-QoS VPN over Broadband Networks

Hoon Lee*, Min-Tae Hwang*, Youn Uh*, Jong-Hoon Eom** and Yong-Gi Lee**
*Changwon National University, Changwon, 641-773 Korea
** Access Network Lab., Korea Telecom, Daejon 305-718 Korea
Corresponding: hlee@sarim.changwon.ac.kr

Abstract

In this paper, we propose methods for designing the Virtual Private Network (VPN) which guarantees a strict Quality of Service (QoS) over ATM networks. The required Quality of Service is a very strict Cell Loss Probability, and it is guaranteed by providing equivalent bandwidth which is computed so that the provided bandwidth is sufficient to guarantee that requirement. We consider two network architectures for constructing VPN, the customer pipe scheme and the Hose scheme, and we propose a method to compute the amount of the required bandwidth for the two schemes. Finally, we investigate the implication of the scheme via numerical experiments.

Keywords: VPN, Bandwidth dimensioning, Broadband networks

1. Introduction

Recently, the electronic exchanges of documents and data inside and/or outside the enterprise network have become usual events, and as such the requirements for the connections have been extended to a distributed wide area network. At the same time, the development in the network technologies made it possible to use the ATM (Asynchronous Transfer Mode) or IP (Internet Protocol) networks as a part of the enterprise network. Thus, the traditional private leased lines are likely to be replaced by VPN due to high capacity and reasonable price as well as excellent performance.

There exist plenty of issues concerning the design of the VPN. To name a few, we have to consider the security, pricing, network topology and resource dimensioning. Among them the resource dimensioning, especially the bandwidth dimensioning, is one of the key issues in order to secure the QoS to the users.

In this paper, we focus on the issue of dimensioning the bandwidth for the VPN from the viewpoint of guaranteeing the strict QoS of data loss, especially the packet (or cell) loss rate of the data.

There exists a few literature which deal with the bandwidth dimensioning of VPN from the QoS guarantee. Duffield proposed a capacity management scheme for the IP-VPN under two connection schemes, the customer-pipe model and the hose model, which is applied to our VPN topology[3]. Those architectures are also discussed in [4] as an ATM version of VPN in the name of end-to-end VPN and the broadband VPN, respectively. But, neither has considered the QoS guarantee such as packet loss rate. Anerousis proposed a dynamic dimensioning method for VPN using the concept of connection-oriented network with call blocking, but the packet level QoS is not taken into account [2].

Our work is different from the previous works in the following points: First, in this paper, we assume the topologies described in [3], but we take into account the packet loss rate in the dimensioning of the required bandwidth for the packet network including the ATM or IP networks. Second, we assumed the long- range dependent traffic as an aggregated source from a customer network, which is considered to be the most typical source traffic environment in the real field. Third, via a simple approximate formula for the packet loss probability, we quantify the required bandwidth capacity for each customer network under the assumed connection topology. Note that for simplicity in the description of the mathematical basis, we assume the ATM network with fixed length packet.

This paper is composed as follows: In Section 2 we describe the VPN architecture. In Section 3 we propose a method for dimensioning the bandwidth capacity assuming the typical long-range dependent traffic. In Section 4 we present result of the numerical experiments. Finally in Section 5, we discuss implication of the work and summarize our work.

2. VPN Architecture

Consider a distributed work environment of a company composed of headquarters in area A, three branch offices located at B, C and D. There exist transactions between the headquarters and branch offices for the business processing such as sales report and human communication between the member of different departments. The company can construct a closed intra-network via several methods such as the leased line or VPN. Among them, they can save the communication cost to a large extent by building VPN between the offices. Fig.1 illustrates this environment.

There exist two typical methods for the VPN: the Customer Pipe (CP)-VPN scheme and the Hose-

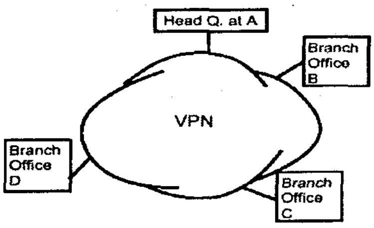

Fig. 1. VPN architecture for a company.

VPN scheme [3]. In CP-VPN, the physical network composed of the concatenation of nodes and links is mapped into a logical network shown in Fig.2, where each office is connected with the other offices by full-mesh of the nodes which access the offices in each area. This network architecture is called as a CP-VPN because each customer in VPN is connected to the other customers with a pipe like personal pipe between two end users. The path can be provided by the PVC (Permanent Virtual Circuit), which is supported by the ATM network.

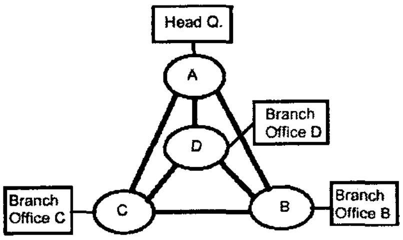

Fig.2. CP-VPN architecture.

In Hose-VPN, end-to-end paths with the same directions are packed into an aggregated big pipe, and they are distributed after that. Say, for the traffic from area A to B in Fig.3, they do not have a direct path. The traffic from area A to B is aggregated with the traffic from area A to D and A to C in the path between nodes A and D, after that they use the path between nodes D and B. This approach results in much higher statistical multiplexing effect than that by CP-VPN scheme via bandwidth sharing.

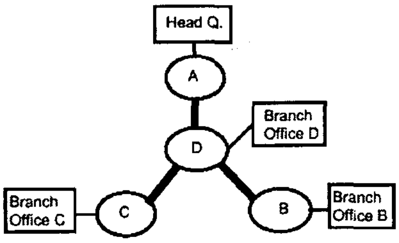

Fig.3. H-VPN architecture.

However, each scheme has pros and cons: The CP-VPN guarantees the QoS more strictly than the Hose-VPN at the expense of dedication of a path to an area.

But, the network operator has to know the traffic matrix between all the VPN sites. In addition, the connections other than a specific connection from an area can not utilize the vacant bandwidth not used by a certain path.

On the other hand, the Hose-VPN can obtain much higher statistical multiplexing effect by aggregating the traffic with the same direction. The Hose-VPN requires no traffic matrix between all the VPN sites. So, the network operator has to know just the aggregated incoming and outgoing traffic for a certain node.

3. Bandwidth Dimensioning

Referring to Fig.2 and Fig.3, we have to decide an appropriate capacity of bandwidth between the two nodes, which we call links hereafter. The capacity of the link corresponds to the capacity of Virtual Path (VP) in ATM context and the capacity of links between the two routers in IP network, and there exist lots of approach for demensioning VP capacity [10]: Peak rate dimensioning, mean rate dimensioning or some rate between those two values such as the sustainable rate.

One more approach is the QoS-free algorithm which tries to slightly over-provide the bandwidth and avoid the complexity and costly congestion control [5]. From our viewpoint, the QoS-free concept can be suitable for the dimensioning of the backbone network where the traffic is smoothed by aggregating a large number of connections. Also, that approach can be applied to the dimensioning of the access link of the VPN on which our discussion is based.

In this paper, we propose a method to quantify bandwidth sufficiently greater than the mean rate which is required to guarantee the strict CLP value in the context of the asymptotic approximation by using the large deviation theory (LDT), which also corresponds to the sustainable rate.

Let us assume that the aggregated traffic from an office i is served by a VP with capacity C_i.

The packets are segmented into a fixed size cell, and the time scale is so small that the traffic is regarded as a fluid flow by the network. Since it is usually known that the LAN/WAN traffic is characterized by self-similarity and burstiness, so we assume those traffic.

From the traffic trace of Korea Telecom R&D center, the input and output traffic showed self-similar characteristics where the Hurst parameter H is in the range of $0.5 < H < 1$, which illustrates that the LAN traffic has LRD (Long Range Dependent) over long time scale [9]. However, let us assume that the offered load between the offices are moderate or lightly loaded (From our experiments in KORNET, the Korea Telecom's public IP network, the average usage rate of the access link for the IP-VPN is about 20% for a diverse access speed types) [6], so that the node congestion can be regarded as a very rare event, which enabled us to use the LDT. However, because we assumed that the traffic is very bursty in a short time scale, cell buffering at the node is inevitable.

In order to proceed our discussion to the dimensioning of the required bandwidth for the link, let us assume as follows: The user does not have a sufficient information for his/her traffic. The customer abstractly knows that he/she needs a certain level of mean rate and he/she requires that the ceiling of CLP (cell loss probability) requirement such that their traffic meets the cell loss under a certain limit.

On the other hand, let us assume that the network operator can measure mean and variance of the cell arrival rate and the CLP. The variance here is needed to accurately estimate the variation of the user's traffic from the mean rate.

Under the above-mentioned environment, let us determine the bandwidth between the nodes connecting the customer sites. Following the discussion of Li [7] and the assumption of fluid-flow of the cell input-output, let A(t) be the number of arrivals generated by aggregated customers of the same branch office in the interval (0,t], which is given by

$$A(t) = \lambda t - \sigma Z(t) \qquad (1)$$

where λ and σ is the mean and standard deviation of the cell generation rate, respectively, and Z(t) is normalized fractional Brownian motion (fBm) with zero mean and variance equal to t^{2H}, H is the Hurst parameter (More on the Hurst parameter, refer to [8]).

If we assume that at most C cells can be served in a time interval, and if we let V(t) be number of cells in the buffer of infinite size, then we have the following formula for the remaining cell in the buffer at time t:

$$V(t)=\mathrm{Sup}_{s\le t}\{A(t)-A(s)-C(t-s)\} \qquad (2)$$

In reality, the buffer size in ATM node is finite, as such we have to approximate the infinite buffer system into a finite buffer system. Let us define that the buffer overflow event for a finite buffer system with buffer size B is equivalent to the event that the buffer occupancy level V(t) in an infinite buffer system exceeds B, and let its probability be ϕ, which is represented as follows:

$$\phi \equiv \Pr\{V(t)>B\}. \qquad (3)$$

The RHS (right hand side) of the last formula can be rewritten as

$$\Pr\{V(t)>B\} = \Pr\{\mathrm{Sup}_{t>0}(A(t)-Ct)>B\}, \qquad (4)$$

which reduces to

$$\Pr\{V(t)>B\}=\mathrm{Max}_{t>0}(\Pr\{A(t)>Ct+B\}). \qquad (5)$$

If we assume that the traffic coming into an access node of VPN is aggregated by a large number of populations, we can assume that the aggregated input process to each access node follows a Gaussian distribution. From the argument in [1], we obtain the following formula:

$$\Pr\{A(t)>Ct+B\}\approx \exp\{-(C-\lambda)^{2H}B^{2-2H}/(2\sigma^2((1-H)^{1-H}H^H)^2)\}\,. \qquad (6)$$

From (3) and (6), we obtain a formula for the amount of the bandwidth required to guarantee CLP ϕ which is given as follows:

$$C = \lambda + \left(\frac{-\log\phi}{K}\right)^{\frac{1}{2H}} \qquad (7)$$

where K is given by

$$K = \frac{B^{2-2H}}{2\sigma^2((1-H)^{1-H}H^H)^2}. \qquad (8)$$

From formula (7) we can find that the required bandwidth for guaranteeing a VPN traffic with CLP requirement ϕ is greater than the mean bit rate declared by a connection in an amount equivalent to the second item in the RHS of the formula (7). Note that the additionally required bandwidth depends on the variance of the arrival rate and the Hurst parameter as well as the required CLP under the given buffer size.

4. Numerical Experiments

Let us assume that the backbone network supports the VPN by constructing the PVC (Permanent Virtual Circuit) connections. Thus, the network uses the fixed routing algorithm with shortest path selection between the source and destination nodes. Table 1 illustrates the traffic matrix between the source-destination path for the CP-VPN architecture by assuming the weight in the amount of the data transactions between the Headquarters and the branch offices.

Table1. Load between end-to-end offices

[unit:Mbps]

	A	D	B	C
A	X	0.7	0.3	0.4
D	0.7	X	0.3	0.2
B	0.3	0.3	X	0.3
C	0.4	0.2	0.3	X

In the table, the X illustrates that the traffic inside the same location is out of the consideration in the dimensioning process. We assumed that the traffic is symmetrical (say, traffic from node A to node B is equal to the traffic from node B to node A).

On the other hand, Table 2 represents the traffic matrix of the Hose-VPN for the traffic load assumed in Table 1. For example, the traffic load of the link between the nodes A and D for the Hose-VPN is sum of the traffic between the node pairs A-D, A-B and A-C.

First, let us compute the bandwidths of the links for the CP-VPN. The end-to-end CLP requirements for all the paths are assumed to be 10^{-12}, and the buffer is provided for each originating node and buffer size is assumed to be 1000 cells. For the simplicity of calculation, let us assume that the variance $\sigma^2=10\lambda$ for all traffic and the Hurst parameter is assumed to be 0.8.

Table2. Load between Hoses [unit:Mbps]

	A	D	B	C
A	X	1.4	X	X
D	1.4	X	0.9	0.9
B	X	0.9	X	X
C	X	0.9	X	X

Table 3 illustrates the results for the bandwidth between the source-destination path of the CP-VPN architecture. Note that the network operators have to provide a bandwidth much greater than the mean source traffic rate in order to guarantee a very strict CLP requirement of 10^{-12}. In case of the source-destination pair A-D in Table 3, the required bandwidth is about seven times that of the mean source traffic rate.

Table 3. Bandwidth of the link for CP-VPN [unit:Mbps]

	A	D	B	C
A	X	4.64	2.62	3.18
D	4.64	X	2.62	2.00
B	2.62	2.62	X	2.62
C	3.18	2.00	2.62	X

This trend is shown in all the links. These results come mainly from the strictness in the CLP requirements.

Table 4 illustrates the bandwidth between the neighboring nodes for the Hose-VPN under the same conditions that have been assumed in computing Table 3. We assumed the same parameters as with Table 3 except that the buffer size prepared for aggregated traffic is summed up to be 3000.

Table 4. Bandwidth of the link for Hose-VPN [unit:Mbps]

	A	D	B	C
A	X	6.02	X	X
D	6.02	X	4.40	4.40
B	X	4.40	X	X
C	X	4.40	X	X

Let us compare the Tables 3 and 4. Consider the total output link at the node A. The total required bandwidth of the output link of the node A under the CP-VPN architecture is 10.44Mbps, whereas the Hose-VPN requires only 6.02Mbps, saving 42.3% of the bandwidth.

Now, let us compare the total bandwidth required to provide the VPN for the company.

The total one-way bandwidth for the CP scheme and Hose scheme is 17.68 Mbps and 14.82 Mbps, respectively. Thus, the Hose scheme can save about 16.3% of the bandwidth.

Summarizing the above results, we can find that the Hose-VPN scheme is more favorable than the CP-VPN scheme from the two view points. First, the Hose-VPN scheme requires less total bandwidth capacity than the CP-VPN scheme. Second, the Hose-VPN scheme aggregates the separate connections in the CP-VPN scheme in a fat pipe, so that it is simpler for the network operator to manage the network resources.

5. Conclusions

In this paper, we proposed a method for dimensioning the bandwidth required for guaranteeing the strict CLP in the VPN over the broadband networks. We assumed two typical VPN topologies: the CP-VPN and Hose-VPN. Via analytical methods we derived the bandwidth required to guarantee specified packet loss rate using the asymptotic approximation of the long range traffic which is inherent to the current data networks.

From the numerical experiments of simple four-node network, we could verify the superiority of the Hose-VPN model compared to the CP-VPN model from the economic point of view.

The result of this paper could be utilized as means to the design of VPN networks whether it is based on ATM or IP network.

Acknowledgment

This work was supported in part by Access Network Laboratory of Korea Telecom.

Reference

[1] R.G. Addie, "On the applicability and utility of Gaussian models for broadband traffic", Faculty of Sciences, USQ, Working Paper Series SC-MC-9815.

[2] N. Anerousis, "Dynamic virtual network dimensioning in cost-sensitive environments", Proceedings of Globecom'99, 1999.

[3] N.G. Duffield, P. Goyal and A. Greenberg, "A Flexible model for resource management in Virtual Private Networks",ACM SIGCOMM'99.

[4] S. Fotedar, et.al., "ATM virtual private networks" Communications of ACM, Vol.38, No.2, February 1995.

[5] H. Hosogoezawa, S. Yoneda and T. Aoki, "An IP network design rule to meet QoS demands of users", Technical Report of IEICE CS99-153(2000-02)(In Japanese).

[6] Hoon Lee, "A Usage-Rate Based Charging for QoS-Free Traffic in IP-VPN", submitted for presentation.

[7] J-S Li, "Measurement and in-service monitoring for QoS violations and spare capacity estimations in ATM network", Computer Communications, 23(2000)

[8] Z. Sahinoglu and S. Tekinay, "On multimedia networks:Self-similar traffic and network performance", IEEE Communications Magazine, January 1999.

[9] S.M. Yang, "Fractal characteristics in KORNET traffic", Korea Telecom TM, 1999(In Korean).

[10] H. Yokoi and T. Tsuchiya, "VP bandwidth design based on estimation of queue length distribution in a buffer", Technical Report of IEICE SSE99-16 (1999-05) (In Japanese