Measurement Based Characterization and Provisioning of IP VPNs

Satish Raghunath [*]
Nortel Networks
rsatish@alum.rpi.edu

K. K. Ramakrishnan
AT&T Labs - Research
kkrama@research.att.com

Shivkumar Kalyanaraman
Dept. of ECSE, RPI
shivkuma@ecse.rpi.edu

Chris Chase
AT&T Labs - Research
chase@research.att.com

ABSTRACT

Virtual Private Networks provide secure and reliable communication between customer sites. With increase in number and size of VPNs, providers need efficient provisioning techniques that adapt to customer demand by leveraging a good understanding of VPN properties.

In this paper we analyze two important properties of VPNs that impact provisioning - (a) structure of customer endpoint (CE) interactions and (b) temporal characteristics of CE-CE traffic. We deduce these properties by computing traffic matrices from SNMP measurements. We find that existing traffic matrix estimation techniques are not readily applicable to the VPN scenario due to the scale of the problem and limited measurement information. We begin by formulating a scalable technique that makes the most out of existing measurement information and provides good estimates for common VPN structures.

We then use this technique to analyze SNMP measurement from a large IP VPN service provider. We find that even with limited measurement information we can realize adaptive provisioning for a significant fraction of VPNs, namely, those constituting the "Hub-and-Spoke" category. In addition, the ability to infer the structure of VPNs holds special significance for provisioning tasks arising from topology changes, link failures and maintenance. We are able to provide a classification of VPNs by structure and identify CEs that act as hubs of communication and hence require prioritized treatment during restoration and provisioning.

Categories and Subject Descriptors: C.2.1 [Computer-Communication Networks]: Network Architecture and Design; C.4 [Performance of Systems]: Design Studies

General Terms: Measurement, Design

Keywords: VPN, Provisioning, Traffic Engineering, Traffic Matrix Estimation

1. INTRODUCTION

Virtual Private Networks (VPNs) provide secure and reliable connectivity among customer sites. The mission-critical nature of traffic carried on VPNs makes security and reliable delivery (low loss and delays) essential characteristics of such networks. With increasing popularity of IP VPNs for enterprise networking solutions, providers are faced with new challenges in provisioning and operating a complex and growing VPN infrastructure.

In the presence of accurate information about customer traffic profile and available network resources, a provider can make accurate provisioning decisions while ensuring Service Level Agreements (SLAs) are met. However, in reality it is hard to specify customer traffic statistics accurately *a priori*. Existing architectures (e.g., the Hose Model [1], the Point-to-Set model [4]) for scalable VPN services rely on adaptive provisioning strategies that require a good understanding of VPN characteristics, to avoid provisioning for peak demands.

Our goal is to develop techniques that allow a service provider to learn properties of VPNs that impact provisioning tasks. We begin with SNMP measurement information from a large IP VPN service provider. For bandwidth allocation and resizing, we need temporal characteristics of traffic exchanged between pairs of customer endpoints (CEs). Provisioning tasks involving maintenance, recovery from link failures, topology changes, and re-homing customers are better accomplished if we can prioritize these tasks especially for the hubs of communication in the VPN. Thus, a good understanding of the structure of VPN endpoint interactions is required. Traffic engineering tasks involving core network capacity management also require a good estimate of the size of customer traffic aggregates, which can also be derived from a knowledge of the CE interactions, such as the CE-CE traffic matrix.

Recent advances in traffic matrix estimation techniques [5] provide a starting point. There are important differences in the VPN case that prevent us from directly employing existing traffic matrix estimation techniques: (a) the scale of the network taken as a whole results in a computationally expensive and infeasible formulation; (b) per-VPN traffic information is not available for core network links resulting in a lack of sufficient measurement information; (c) a shared core network infrastructure with only aggregate link

[*] Supported by DARPA grant F30602-00-2-0537

IMC'04, October 25–27, 2004, Taormina, Sicily, Italy.
Copyright 2004 ACM 1-58113-821-0/04/0010 ...$5.00.

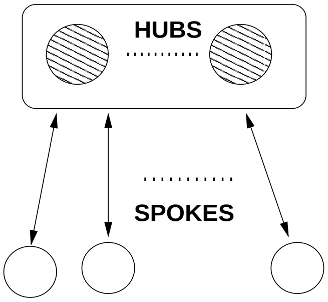

Figure 1: Schematic showing a multi-hub VPN

counts for these links introduces dependencies among the many VPNs that share those links.

Each of these issues assumes significance when we observe that with continual growth in the number of VPN customers, the scale of the problem increases. Obtaining fine-grain reliable measurement information becomes much harder. Thus we first evolve a scalable technique to compute VPN traffic matrices and then examine how to deal with the lack of sufficient measurement information. Specifically, we examine what characteristics of VPNs can be reliably estimated with existing information. In doing so, we are able to provide deployable techniques for improving the existing provisioning infrastructure. Additionally, our observations can serve as a guide to enhancement of existing measurement infrastructure for maximal gains.

We thus begin with an estimation technique that employs approximations to break the network-wide traffic matrix problem into several smaller independent per-VPN traffic matrix problems. These approximations are driven by distinct properties of VPNs. We examine the reliability of the approach and demonstrate that despite insufficient information, we can learn VPN characteristics discussed above for a large fraction of customers.

First, we find that VPNs that exhibit a Hub/Spoke structure can be efficiently handled. Such VPNs feature many "spoke" nodes that communicate with just the "hub" nodes (typically one or two, (Fig. 1)). We then employ traffic matrix estimates to obtain a classification of VPNs by their structure and show that Multi-hub/Spoke VPNs indeed constitute a significant fraction. We present analysis of Multi-hub/Spoke VPNs to show that many of these VPNs in fact feature two hubs that are part of a dual-homed site. For the SNMP data analyzed in this paper, we show that traffic matrices can be accurately computed for a significant percentage (about 57%) of the VPNs. We show that even approximate CE-CE traffic matrices can be used in thresholding techniques to identify hub nodes, which is very helpful in provisioning tasks.

Exploiting the higher accuracy in estimates of traffic matrices for Hub/Spoke VPNs, we then study temporal characteristics that affect bandwidth allocation tasks. We observe stable CE-CE traffic trends across weeks, and slowly varying trends across months. This lends support to bandwidth allocation strategies that might attempt to learn characteristics over time.

The combination of algorithms and measurement observations we present demonstrates the feasibility of adaptive provisioning. Despite the limited nature of available measurement information, we demonstrate that our techniques can be applied to a significant fraction of VPN customers implying an overall enhanced operational efficiency.

SNMP Information	CE-PE and PE-PE traffic
SNMP Aggregation Interval	CE-PE-15m; PE-PE-1hr
VPN Size Range	10s to 100s CEs
Number of PE-PE Links	≈ 6000
Duration of data examined	5 months

Table 1: Details of SNMP Information

The rest of the paper is structured as follows. We discuss related work in §2. The measurement information is briefly described in §3. A traffic matrix estimation technique is then presented in §4. We employ the technique to understand VPN structure and temporal characteristics in §6. We conclude in §8.

2. RELATED WORK

A traffic matrix provides the volume of traffic between source-destination pairs in a network. Such matrices have been computed at varying levels of detail for IP networks: between ISP Points-of-Presence (PoPs) [3], routers [5], IP prefixes [2] etc. The problem of estimating traffic matrices is ill-posed: for a network with N source-destination pairs we need N^2 demands to be estimated. However the number of pieces of information available is typically much smaller (of the order of number of links in the network). For large N, the problem becomes massively under-constrained. Existing research indicates that some kind of *side information* must be brought in while solving such linear systems. Many such proposals solve the following minimization problem:

$$\min_{\mathbf{x}} ||\mathbf{y} - A\mathbf{x}||_2^2 + \lambda^2 J(\mathbf{x})$$

where $||.||_2$ denotes the L_2 norm, $\lambda > 0$ is a regularization parameter, and $J(\mathbf{x})$ is a penalization functional. These approaches are generally called *strategies for regularization of ill-posed problems*. The regularization strategy (the choice of $J(\mathbf{x})$) guides the optimization problem in its choice of the traffic matrix that might provide a good solution to the problem.

Zhang et al [5] develop a regularization method tailored for traffic matrix estimation. Their method incorporates the gravity model solution so that the optimization simultaneously attempts to minimize the error from observed link counts and the gravity estimate. They demonstrate that the gravity model estimate for the traffic matrix provides a good starting point and hence propose to opt for the Kullback-Leibler divergence of the gravity estimate from $\mathbf{x}$ as the regularization functional (§4.1).

The problem treated here is closest to [5] in that, we adopt the same regularization technique. However, compared to the Border Router (BR) traffic matrix obtained in [5], the scale of the VPN problem is much larger. The computational expense prevents us from solving for a single network-wide problem (which is the case with BR traffic matrices). Instead we evolve approximation techniques that exploit the structure of VPNs and break the problem down to many per-VPN problems. In addition to problems with scale, the measurement information available with VPNs is aggregated across all VPNs and per-VPN information is very often unavailable (in contrast, the BR traffic matrices can exploit fine-grain NetFlow data). Hence it is not straightforward

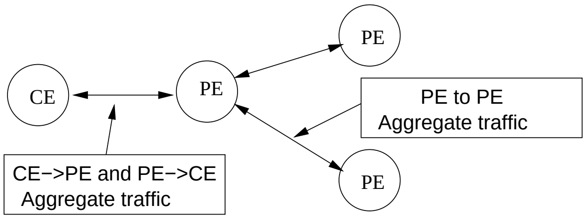

Figure 2: Schematic showing available SNMP measurement information

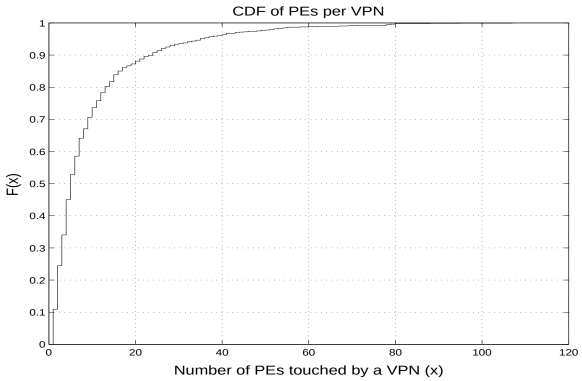

Figure 3: CDF of number of PEs touched by a VPN

to gauge the correctness of the traffic matrix estimates in the case of VPNs. We evolve a set of guidelines to help understand the applicability of the estimates and demonstrate how to obtain the most out of the coarse-grain information available in the case of VPNs, inspite of the prohibitive scale of the problem.

3. MEASUREMENT INFORMATION

In this paper, we present results from our study of measurement information from a large VPN service. Here, we provide a brief description of the data available from the service. In addition to helping us understand the results in the next few sections, this is also meant to be representative of the kind of information that is typically at the disposal of today's service providers.

Fig. (2) shows the points in the network where SNMP measurement information is available. Aggregate byte counts over one hour intervals for each provider edge (PE) to PE link are collected by SNMP. This count represents the number of bytes transmitted on the PE-PE link due to *all* VPN customers sharing that link. By PE-PE link, we mean a logical link like an MPLS tunnel. In the current dataset there was SNMP information for such logical links for every pair of PEs. The other set of SNMP data available is for the traffic for each customer endpoint (CE) to PE link in the form of aggregate byte counts over 15 minute intervals. The CE-PE link is the dedicated access link for the VPN customer and the traffic observed on that link is due only to that customer endpoint.

As one would expect, the SNMP characteristics demonstrate weekly cycles. Fig. 5 shows the daily mean of bytes coming to the CE from the network, for a representative VPN. For some VPNs, there is an increase in the magnitude over the months indicating a growth in the VPN. But there is a mean about which the variations of magnitude are seen indicating that there is a certain amount of predictability in the traffic. An additional observation is that we see stable trends in the sensitivity to time-of-day. When the trends are observed separately for mornings, evenings etc, we see the repetition in patterns more clearly - traffic at noon and evening consistently higher, those at nights always low etc.

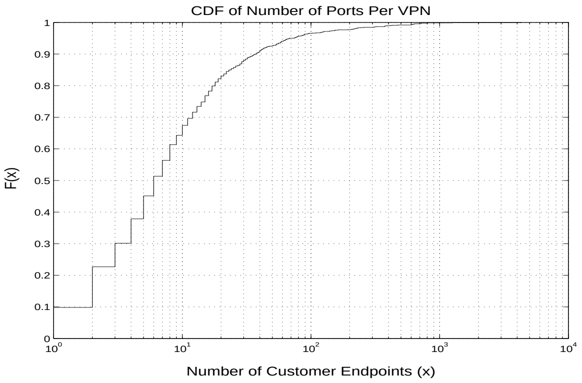

Figure 4: CDF of number of CEs per VPN

An important factor influencing our approach is the size of the service in terms of the number and size of customers, the number of PE routers involved and hence the scale of the problem. Fig. 3 shows the distribution of number of PEs that receive traffic per VPN. This measure indicates the number of links that traffic from a given VPN might influence. If there are N PEs that the CEs of a VPN communicate with, there can be $O(N^2)$ PE-PE paths that have to be factored in the estimation formulation. These PE-PE paths in turn carry traffic from other VPNs. Similarly the size of the VPN customers is an important measure of the scale of the problem. Fig. 4 gives the distribution of number of number of endpoints per VPN. The distribution shows that while there are a lot of small VPNs, there is a significant fraction with sizes in tens and hundreds. In the absence of per-VPN traffic information on a per-link basis (as is the case here - the traffic counts for PE-PE logical links are aggregated across VPNs), the estimation has to account for all pairs of CEs as potentially communicating peers. The gist of these observations is that the scale of the problem at hand is considerable.

4. TRAFFIC MATRIX ESTIMATION AND CLASSIFICATION

There are multiple uncertainties to overcome while provisioning the network for the aggregate capacity needed for the VPN service. Some of the factors a carrier may not know precisely, a-priori, are:

- The amount of traffic generated by any given source of the VPN. We may only have available the peak rate specification.
- The proportion of the source (hose) traffic that any given link in the network receives.

Often, a new VPN may be admitted as and when the customer request arrives, with very little information being provided by the customer other than peak access capacity requirements. To guarantee the SLAs requested, there is a need to ensure that adequate resources are available. Understanding the "structure" of the VPN helps us in more efficiently provisioning the capacity in the network, and adapting the capacity to changing VPN requirements. By structure, we mean the spatial distribution of the traffic flows between the different sources and destinations of the VPN. For example, knowing if there is a hub-and-spoke structure helps in appropriately provisioning capacity in the network since an end-point that is a spoke in a pure "hub-and-spoke" VPN would require capacity primarily between the hub and spoke. However, this information is rarely provided (or known) by the customer at the time when the VPN is admitted. As a result, provisioning without knowledge of the VPN structure could result in a substantial amount of wasted resources.

To infer the structure of a VPN and to achieve efficiencies through adaptive provisioning, we need to examine the way customer endpoints communicate with each other. In other words, we need good estimates of the VPN traffic matrix.

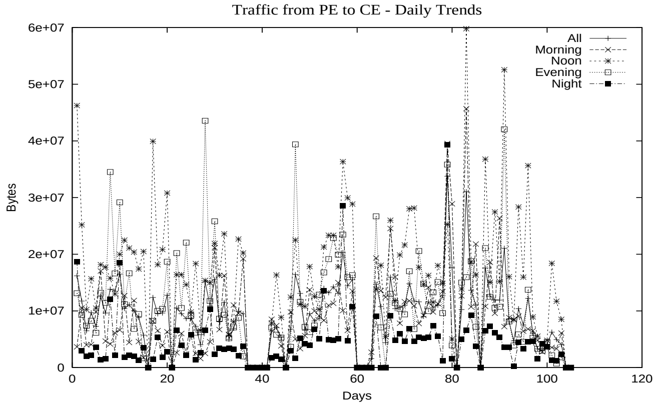

Figure 5: Aggregate bytes entering a CE over 5 months for a VPN of size 79

4.1 Estimation techniques

Traffic matrix estimation is an ill-posed problem: with N nodes in a network, the number of traffic demands to be estimated is N^2 while the number of equations we have is only proportional to the number of links. As discussed in §2 there are several approaches to solving such under-constrained problems. Two popular approaches are the gravity model approach and the information theoretic approach. We employ both.

Denote the total traffic entering an endpoint s_i by $N^{in}(s_i)$ and the traffic leaving it by $N^{out}(s_i)$. Each element of the traffic matrix indicates the amount of traffic from endpoint s_i toward d_j, denoted by $N(s_i, d_j)$. Thus some portion of $N^{out}(s_i)$ is contributing to $N^{in}(d_j)$. The gravity model attributes a portion of $N^{in}(d_j)$ to each source s_k that transmits to d_j in proportion to the size of $N^{out}(s_k)$. The underlying assumption is that the amount of traffic generated by s_i is independent of that generated by d_j. Thus the following relationship is used: [5]

$$N(s_i, d_j) = \frac{N^{out}(s_i)N^{in}(d_j)}{\sum_{k \neq j} N^{out}(s_k)} \tag{1}$$

While the gravity model is simple, it is known to be less accurate in the presence of additional information. One of the methods recently proposed [5] exploits what is generally termed *strategies for regularization of ill-posed problems.* Accordingly a penalized least-squares approach is formulated as:

$$min_x \left\{ ||\mathbf{y} - A\mathbf{x}||^2 + \lambda^2 \sum_{k:g_k>0} \frac{x_k}{T} log\left(\frac{x_k}{g_k}\right) \right\} \tag{2}$$

Here, $\mathbf{x}$ is a vector with each x_i representing the variable $N(s_i, d_j)$, with the constraint that $x_i \geq 0$. Each element y_i in vector $\mathbf{y}$ represents the traffic measured for link i, T is the total traffic in the network, and g_k is the gravity estimate for x_k obtained using Equation (1). A is the routing matrix which relates the appropriate variables x_i.

In the present context, s_i and d_j would correspond to the VPN customer endpoints. The set of variables $N(s_i, d_j)$ would be defined for each (s_i, d_j) that are part of the same VPN, since an endpoint communicates with another endpoint only if it is a part of the same VPN. For example, denote $N(s_1, d_1)$ and $N(s_1, d_2)$ by x_1 and x_2 respectively. If d_1 and d_2 are the only nodes with which s_1 communicates we have the equation $N^{out}(s_1) = x_1 + x_2$. Enumerating such equations for all VPNs in the network would give us the equations denoted by Equation (2). Thus the following would be set of equations forming the system:

1. For each source s_i, $N^{out}(s_i) = \sum_j x_j$ where x_j indicates the variables for traffic from s_i to d_j.
2. For each source s_i, $N^{in}(s_i) = \sum_j x_j$ where x_j indicates the variables for traffic from d_j to s_i.
3. For each PE-PE link, $N(PE_{ij}) = \sum_j x_j$ where x_j indicates the variables for all such (s_i, d_j) pairs that transmit on the link PE_{ij}.

In reality, the problem described in Equation (2) is too big and computationally expensive to solve. For instance, for the measurement data analyzed here, we have a sparse routing matrix (A in Equation (2)) of dimensions $(18 \times 10^3, 950 \times 10^3)$ approximately, with about 2.8×10^6 non-zero elements. In this paper, we evolve a variant of the above estimation techniques to reduce the size of the problem so that the traffic matrices can be quickly computed.

4.2 Estimation of VPN Traffic Matrices

Although many VPNs share a common core network, no two endpoints belonging to different VPNs communicate with each other. This lends a kind of separability to our problem and hints at a possible strategy to reduce its size. Instead of solving the problem for all VPNs as part of a single network, we propose to compute the traffic matrices for each VPN independently. In order to do this, we need data on a per-VPN basis to construct the problem as in Equation (2). The path from a CE to another CE consists of two segments: a) an access segment (between the PE and the CE) where there is traffic from this VPN alone, b) a core network segment (link between two PEs) which carries traffic multiplexed across multiple VPNs. Typically, we have aggregate SNMP information for each of these segments. Thus we need to infer what part of the PE-PE aggregate traffic is attributable to the VPN being solved for, at each step. But there is not enough information to deduce this quantity. Instead, we introduce a bound on the contribution of a particular VPN to the measured PE-PE link traffic.

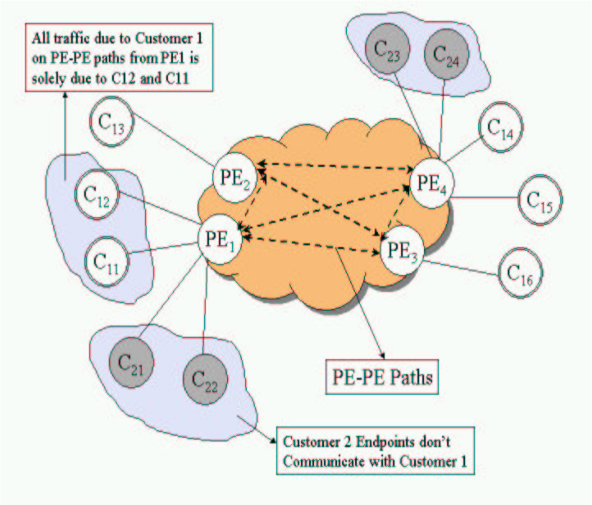
All traffic due to Customer 1 on PE-PE paths from PE1 is solely due to C12 and C11
C13
C12
C11
C21
C22
C23
C24
C14
C15
C16
PE2
PE4
PE1
PE3
PE-PE Paths
Customer 2 Endpoints don't Communicate with Customer 1

Figure 6: Schematic indicating the structural aspects of VPNs that lead to additional equations in the Traffic Matrix estimation problem

Figure 6 depicts the constraints we evolve by exploiting the structure of VPNs. We consider the set of all CEs in the VPN that can possibly transmit along a given PE-PE link. For example, in Figure 6 for the PE1-to-PE3 link, C_{21} and C_{22} are the only endpoints of Customer 2 that offer traffic. The total output from those CEs provides a loose upper bound on the contribution of that VPN to the PE-PE traffic.

Thus, for every PE-PE link which is used by the VPN, we introduce an additional equation as follows:

$$T_l = \sum_{\{(i,j)\in S\}} N(s_i, d_j) + v_l$$

where S is a set of CE pairs belonging to this VPN which could possibly transmit on the PE-PE link l and v_l is a dummy variable indicative of the contribution of all the other VPNs to the observed PE-PE traffic T_l. We can substitute T_l by $\sum_{\{(i,j)\in S\}} N^{out}(s_i)$ as a loose upper bound as discussed above. For the example in Figure 6, this would indicate the sum of $N^{out}(C_{21})$ and $N^{out}(C_{22})$. Now, we have:

$$\sum_{\{(i,j)\in S\}} N^{out}(s_i) = \sum_{\{(i,j)\in S\}} N(s_i, d_j) + v_l \qquad (3)$$

This equation focuses on the traffic related to a particular VPN. The summation in $N(s_i, d_j)$ signifies the traffic exchanged between s_i and d_j (on a given PE-PE path to d_j), whereas the left hand side includes all traffic generated by s_i (on all PE-PE paths). Hence v_l is a dummy variable that indicates the fraction of traffic from sources $\{i : \forall k\ (i,k) \in S\}$ that does not go to destinations $\{j : \forall k\ (k,j) \in S\}$ (i.e., it is the contribution of s_i of the VPN on all the other PE-PE paths.) Here, we have only used the CE-PE traffic information and not the PE-PE information. Observe that the LHS of Equation (3) is the sum of the contributions of all CEs of the VPN attached to this PE. Thus this traffic is intended toward CEs attached to many other PEs and it is possible that this is greater than the PE-PE observed traffic. Thus we can incorporate an additional piece of information in the PE-PE traffic to make the LHS tighter (assuming we are writing the equation for the PE-PE link (k,l)):

$$min\{N(PE_{kl}), \sum_{\{(i,j)\in S\}} N^{out}(s_i)\} = \sum_{\{(i,j)\in S\}} N(s_i, d_j) + v_l \qquad (4)$$

We now are in a position to solve the traffic matrix problem for each VPN separately. The introduction of a loose bound instead of the the actual traffic due to the VPN on the PE-PE link will introduce inaccuracies in the estimated matrix. In the succeeding section we show that these inaccuracies are tolerable for purposes of structural study of VPNs and provisioning decisions.

5. VALIDATION OF ESTIMATION TECHNIQUE

To verify the accuracy of the traffic matrix estimates, we could measure the actual traffic matrix and examine errors. However, the scale of the VPN network means that measuring per-VPN traffic matrices is very complex. Due to the hundreds of customers and each with tens or hundreds of endpoints, the task of building a reliable measurement architecture is formidable. The SNMP measurement information we obtained did not have per-VPN traffic matrix information but instead had only aggregate link traffic counts.

One option for validating the traffic matrix estimates is to generate synthetic data and feed it as input. The program generating the aggregate link traffic counts starts with a synthetic traffic matrix for the VPN. Thus we have the real traffic matrix for purposes of evaluating the performance of the estimation technique.

A disadvantage of this approach is that real measurement data can be very different from generated data. Due to the variety of possible errors in the process of collecting information, it is very hard to capture the nature of measurement noise. We supplement the synthetic validation with indirect checks on results with SNMP data to affirm that the estimation technique does yield reliable estimates.

5.1 Synthetic Validation

We examine the performance of the estimation technique by feeding input data derived from synthetic traffic matrices. The input data involves aggregate byte counts of the links traversed by the VPN. Thus the test involves feeding the synthetic aggregate data to the estimation technique and obtaining an estimated traffic matrix. To validate the estimation technique, we examine the error in the estimated traffic matrix compared to the actual.

The objective of this exercise is to understand the set of VPN properties that can be reliably estimated given the nature of information at our disposal. We are interested in examining whether we can reliably deduce certain VPN structural and temporal characteristics despite the lack of per-VPN information for all links involved. Our strategy is as follows. Recognizing that the traffic matrix is induced by the underlying structure in the VPN, we begin by assuming a structure of the VPN and generate synthetic input data. We then measure the error in estimating the actual traffic matrix and identifying VPN structures. E.g., in the following paragraphs we begin with the Hub/Spoke structure to generate synthetic inputs. If the estimated traffic between the hub and spokes agree with the actual and if the hubs

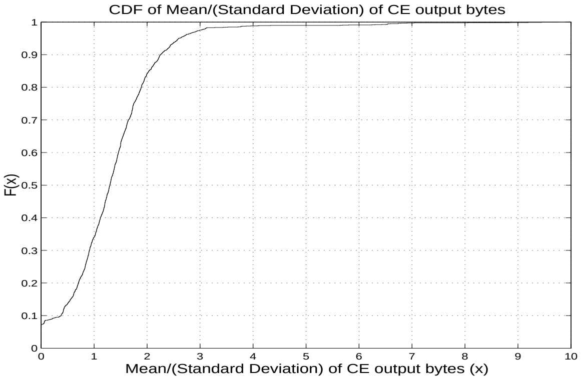

Figure 7: CDF of the spread of spoke sizes from SNMP data for Hub/Spoke VPNs

are correctly identified, we conclude that the technique can be relied upon for inferences regarding Hub/Spoke VPNs.

In the following paragraphs, we deal with Hub/Spoke VPNs with one or more hubs. As it will be clear in the later section, this structure is the most commonly occurring among VPNs. In a Hub/Spoke VPN, we have all spoke nodes communicating with the just the hub nodes. Further the spoke nodes do not communicate among themselves. We characterize such VPNs with the following parameters:

1. Size of the VPN
2. Number of Hubs
3. Variation in the size of Spokes - the amount of traffic exchanged between a spoke and a hub determines the size of that spoke.
4. Maximum number of CEs of a VPN homed on the same PE ("cluster size").

We briefly discuss the significance of these parameters. We vary these parameters over a range of values that are found to be relevant to the typical VPN as indicated in the measurement data. Thus we examine VPNs of sizes 10 and 15 which cover about 80% (see Fig. 4) of the sizes found in the data. We examine results for one and two hub VPNs exploiting an observation presented in a later section on classification of VPNs that 95% of the multi-hub VPNs feature 2 hubs (Fig. 12). With reference to Hub/Spoke VPNs, increased variation in the traffic volumes observed from a spoke can make it harder for the estimation technique to identify the hub. Fig. 7 shows the CDF obtained from the SNMP data by computing the deviation in the traffic volume across spokes for all Hub/Spoke VPNs (the methodology for classification of VPNs is discussed in the succeeding section). The deviation has been normalized by the mean. We use mean to standard deviation ratios of 1, 1.5 and 2 to examine the effect of spread of spoke sizes on accuracy. A ratio of 2 covers about 85% of the observed deviations.

The other parameter which we incorporate is the number of CEs of a VPN per PE. For a given VPN, higher the *clustering of CEs* on a PE, lower the number of equations at our disposal for the same number of variables. Thus it is important to see how accuracy is impacted with typical cluster sizes. Thus the number of CEs of the same VPN that are clustered on a given PE are varied from 1 to 4 to cover about 80% of the cases seen in the measurement data (Fig. 13). Since we are interested in examining the reliability of traffic matrix estimates, the simulation experiments involve individual VPNs that are synthetically generated. We do not attempt to simulate the interaction of multiple VPNs on PE-PE links and instead examine that case with observed SNMP data in later sections.

5.1.1 Methodology

The generation of a synthetic sample involves generating numbers that represent aggregate bytes transmitted and received at each CE and how they are split among various other CEs of the VPN. For a Hub/Spoke VPN we first generate the data observed for the spoke nodes and then sum them up to obtain the data for the hub node. In order to generate data for spoke nodes, we start with a mean and standard deviation. We then generate random numbers conforming to a Gaussian distribution of that mean and standard deviation. As discussed earlier (§5.1) we set the standard deviation using the CDF obtained from the SNMP data.

In the results presented here, we use a mean of 1 MB for the aggregate bytes transmitted and received at each CE that is a spoke. The specific value of the mean has no impact on the results. To summarize the procedure:

1. Set mean μ and standard deviation σ for spoke traffic
2. Generate a Gaussian random number $r_i \sim (\mu, \sigma)$ for each spoke i
3. $R \leftarrow \sum_i r_i$
4. R gives the traffic attributed to the hub

In order to implement the maximum cluster size, we use a uniform random variable as follows. Given a maximum number of CEs m that can be assigned to the PE, we generate an integer random number in $(1, m)$ for each PE. The CEs are assigned to the PEs sequentially till all CEs have been assigned. Thus the number of PEs in a synthetic dataset depends on the maximum cluster size setting and the sequence of uniform random numbers. We summarize the procedure below:

1. Set max number of CEs of a VPN per PE as m, size of VPN as sz
2. Set $i \leftarrow 1$, $j \leftarrow 1$
3. Generate an integer random number $r \sim Uniform(1, m)$
4. Set $r \leftarrow min(i + r - 1, sz)$
5. Assign $CE_i, CE_{i+1} \ldots CE_r$ to PE_j, set $i \leftarrow r + 1$
6. If $i < sz$, set $j \leftarrow j + 1$ and go to 3

5.1.2 Evaluation

We begin our evaluation by examining the effect of the number of CEs of a given VPN incident on the same PE (clustering). Recall that each link traversed by the VPN induces one equation relating the traffic matrix variables. Higher clustering thus gives us fewer equations for the same number of variables causing higher errors in estimation. Further, a given cluster size has greater impact on estimates if the size of the VPN is smaller. We employ the ratio of the

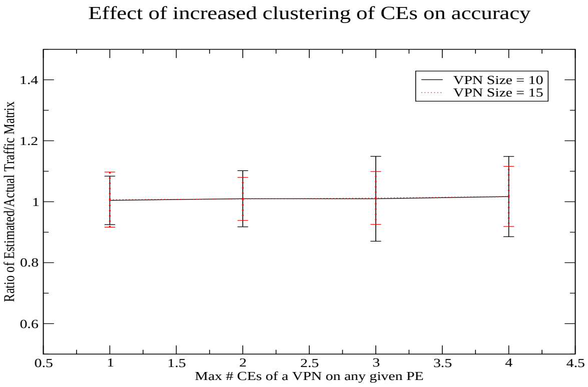

Figure 8: Error in estimated traffic matrix increases with increased clustering of a customer's endpoints on a PE

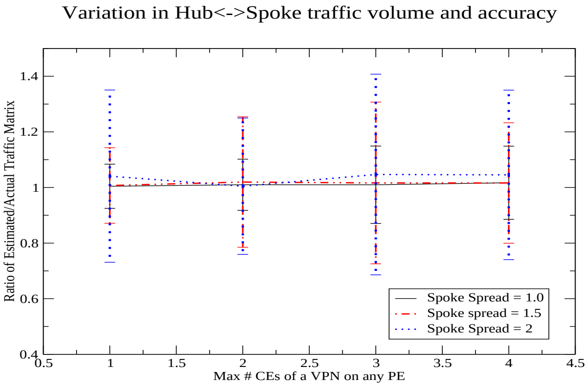

Figure 9: Effect of cluster size with varying spread in spoke sizes for VPN of size 10. Smaller VPNs are affected more by increase in spread in spoke size

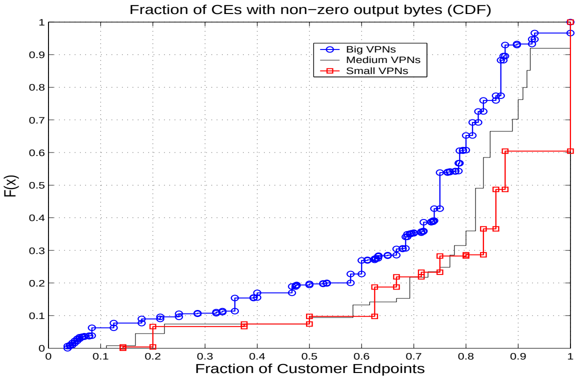

Figure 10: CDF of fraction of CEs featuring non-zero output bytes confirms larger hub/spoke VPNs have more CEs with zero output bytes. This means that accuracy of estimates for larger Hub/Spoke VPNs is better.

% VPNs with multiple hubs	≈ 18%
% Multi-hub VPNs with 2 hubs	≈ 95%
% of 2 hub VPNs dual homed	≈ 40%
% of all VPNs analyzable	≈ 57%

Table 2: Multi-hub VPNs and dual homed hubs

estimated traffic matrix to the actual as a measure of the error - closer the value to one, better the estimate. Fixing the spread of spoke sizes at 1, Fig. 8 indicates that while the standard deviation of the error increases for higher clustering, it is around 10% even at higher cluster sizes for the larger VPN. From the perspective of PE-PE bandwidth provisioning, even the errors at higher cluster sizes are tolerable.

On the other hand, varying the spread of spoke sizes for the smaller VPN, shows that accuracy suffers with increased spread (Fig. 9). This is due to the fact that in a smaller VPN, increased variation in spoke sizes can translate to some of the spokes being comparable to the hub. Larger VPNs are less susceptible to such variations in spoke sizes. Fig. 11 confirms this observation by depicting the effect of variation in spoke sizes with increase in VPN size. The estimates with the larger VPN are much better.

Thus the synthetic validation points to the following observations: (a) the estimates are reliable for Hub/Spoke VPNs over a significant range of parameter values covering a majority of such VPNs; (b) with smaller VPN size, the spread of spoke sizes and cluster size can impact the accuracy of the estimates; (c) estimates for larger Hub/Spoke VPNs are resilient to variations in cluster size and spread in spoke sizes and hence are better.

In all the test runs for Hub/Spoke VPN inputs, the hub node was accurately identified by using a criterion that such a node features more than 50% of the CEs as its peers. We elaborate more on such a thresholding scheme while classifying VPNs using SNMP data (§6).

5.1.3 Two-hub VPNs with dual-homed hubs

In general the evaluation with synthetic data indicates that, with consistent input, the accuracy of the techniques is very good in the case of Hub/Spoke VPNs. These conclusions also apply in a limited sense to multi-hub VPNs where the multiple hubs act as one unit with a load-balancing entity presenting a single interface to the spoke nodes. In such cases, if the hubs are considered as one unit and traffic matrix variables defined accordingly, these conclusions apply fully.

An analysis of the SNMP data shows that a majority of the Multi-hub/Spoke VPNs feature only two hubs (Fig. 12). Further, among these two hub VPNs, 40% have both the hubs homed on the same PE indicating that they are in the same facility. Such dual homed hubs act as one unit with spoke traffic being load balanced among them. In essence, the analysis in the previous section indicates that traffic matrix estimates will be accurate for these VPNs. Utilizing the results of classification of VPNs (to be discussed in §6) we see that about 57% of all VPNs can be accurately handled with the proposed estimation techniques (Table 2).

5.1.4 Multi-hub VPNs without dual-homed hubs

Thus far we have looked at VPNs with a single hub and two hubs to gauge the accuracy of the estimation technique. The remaining type of Multi-hub VPNs are those that have two or more hubs where the hubs communicate with different subsets of CEs in the VPN. Unlike two-hub VPNs with dual-homed hubs, the hubs in these VPNs do not appear

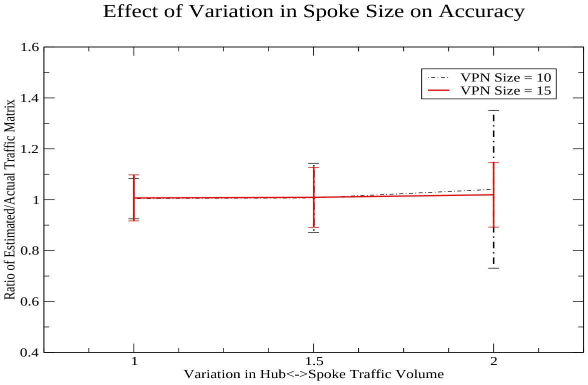

Figure 11: Size of the VPNs and clustering of CEs are more influential w.r.t the accuracy of the TM estimates.

as a single entity to the spokes. These hubs are possibly geographically spread out and feature distinct sets of spokes communicating with them.

We found that the estimation technique cannot provide reliable results in such VPNs. A typical example would be where a subset of CEs transmits zero bytes to one hub and all bytes to a second hub. Due to the absence of per-VPN information on the PE-PE links, the estimation technique has no way of discovering whether a given CE has indeed transmitted to another. The traffic matrix estimate for a given CE pair is driven in part by their traffic volume and the equations for aggregate link counts. Hence, the estimation procedure gives a non-zero estimate so long as the traffic volumes from the CEs are non-zero. In the Hub/Spoke case, this does not drastically affect the errors since the size of the hub is very large relative to spokes.

5.1.5 Validation for Large VPNs

We have examined results for hub/spoke VPNs, which are the typical cases reflected in the measurement data. We have not performed the validation for larger VPN sizes here (which are the top 20% in the measurement data) although we have employed the technique for all VPNs in the succeeding sections dealing with SNMP data. There are some aspects of the traffic that aid in solving for large VPNs. We find that not all CEs communicate in a given measurement interval. The result is that the number of variables to be solved for reduces to a large extent (since they are known to be zero).

Fig. 10 shows the CDF of fraction of CEs that featured non-zero output bytes in the SNMP data for small, medium and large VPNs (lower, middle and higher 33%-ile). The figure shows that in small and medium sized VPNs, 90% or more of the CEs feature non-zero traffic with probability 0.75. For larger VPNs, we see approximately 80% of the CEs transmitting some data with probability 0.75. This means that with larger VPNs, there are more CEs that transmit no data in a given interval, leading to simplification in system to be solved.

Coupling this with observations in §5.1.2 which showed that estimates for larger Hub/Spoke VPNs are resilient to spread in spokes and a range of cluster sizes, we see that traffic matrices can be expected to be more accurate in larger Hub/Spoke VPNs.

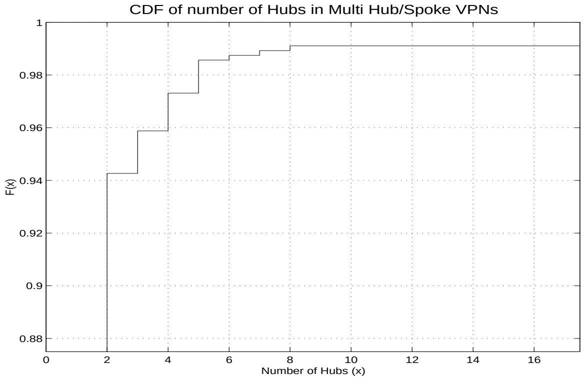

Figure 12: CDF of number of hubs in multi-hub VPNs

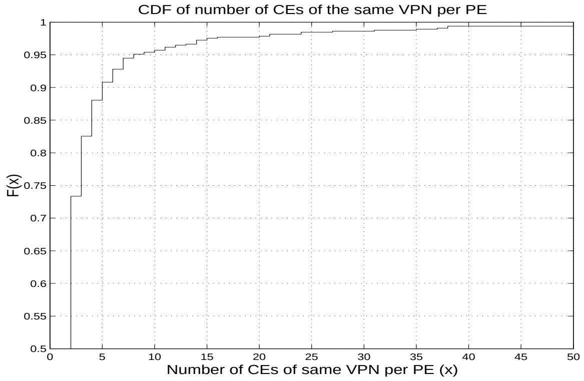

Figure 13: CDF of number of CEs of the same VPN on a given PE

5.1.6 Significance of observations

1. *Clustering:* While provisioning a VPN, the provider usually attempts to reduce clustering of CEs onto a PE so as to reduce the risk of outage for the customer. This bodes well for measurement techniques that have to work with limited information as indicated by the results in the previous sections.

2. *Identifying a hub:* Since the size of the hub is very large compared to the spokes in a Hub/Spoke VPN, a thresholding criterion can be reliably used to identify the hub. Given the traffic matrix estimates for a CE toward all other CEs, we can form a set of its peers by pruning all CEs toward which estimates are comparable to errors in the technique. The node with almost all CEs as peers would be the hub.

3. *Multi-hub and other VPNs:* Clearly more data is needed to reliably analyze multi-hub VPNs and other complex structures. With the current data, we could obtain the traffic matrix and use it only to obtain an approximate set of hubs. One could then examine whether the VPN features several localized Hub/Spoke structures or some kind of a hierarchy among hubs. We have not examined this direction with the synthetic validation in this paper.

5.2 Cleaning the dataset

Given the large-scale nature of the data that is being handled, it is natural to expect errors and inconsistencies in the collection process. It is very important to remove samples that are a manifestation of such errors so that we can understand the performance of our algorithms clearly. In order to clean the dataset, we take recourse to certain properties a valid dataset must satisfy:

1. Noting that CEs in a VPN receive traffic only from other CEs in the same VPN, we observe that whatever data any CE receives must come from a member of the VPN. Thus, the total bytes received by the CEs should be less than or equal to the total bytes transmitted by the CEs, in the same VPN.

2. For any given PE, the total bytes transmitted into the network should be less than or equal to the total bytes offered by all the CEs (of various VPNs) attached to the PE. This is considering the fact that a PE does not generate data.

3. For any given PE, the total bytes transmitted toward CEs attached to it should be less than or equal to the bytes it received from the network. That is, whatever number of bytes the CEs attached to a PE receive that should match the bytes sent to this PE from other PEs.

In reality a large fraction of the dataset does not strictly conform to all these rules. We had to relax the rules so that we have a good number of samples to work with, while still being confident that the samples are meaningful. The strategy we use is to allow a range of error - 10% error is considered tolerable here. For example, we specify that the number of bytes received by CEs in a VPN should be within 10% of the bytes transmitted by all CEs in the same VPN. This means, sometimes, the total output is allowed to be greater than total input. The causes for such cases include data sources not covered by the measurement infrastructure.

Additionally, each VPN is a geographically spread out entity. This means that measurements are usually not time synchronized and are sometimes absent due to problems with polling and dropped packets. Some error cases are handled by the measurement modules and are indicated in the data. Such samples are discarded and the rest of the samples are subject to these tests. Depending on the objectives of the analytical exercise, the threshold for error tolerance can be set to a different value.

5.3 Validation with SNMP data

In §5.1 we could test the accuracy of traffic matrix estimates by comparing them with the actual synthetic traffic matrix that was used to generate the test input. The SNMP measurement data on the other hand does not provide per-VPN information, i.e., we do not know the actual traffic matrix for the VPNs being analyzed. From the results of §5.1 we know that estimates are reliable for a large fraction of Hub/Spoke VPNs. We first examine indirect means of confirming this conclusion. This involves looking at the SNMP measurement of CE-PE link counts and comparing it with the estimates. We then compare the observed PE-PE link counts with traffic matrix estimates, with bandwidth provisioning in mind.

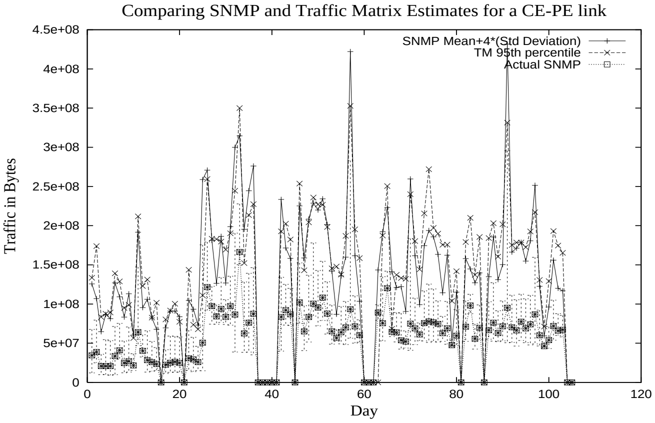

Figure 14: Comparison of estimated CE output bytes with that derived from SNMP

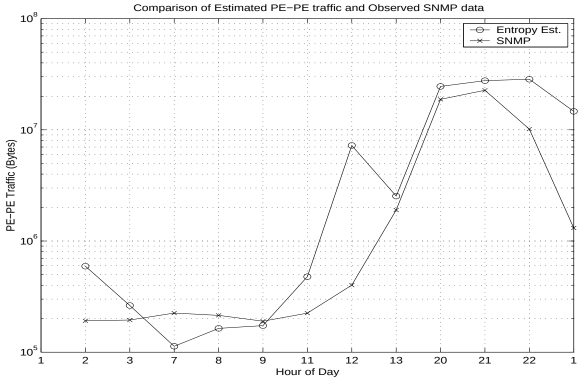

Figure 15: Estimated traffic vs Observed traffic for a PE-PE link with lower traffic volume

5.3.1 CE-PE link data

Fig. 14 examines the CE-PE aggregate traffic. The traffic matrix estimate provides us with values to all variables $N(s_i, d_j)$. Thus for a given s_i if we sum the variables $N(s_i, d_j)$ for all d_j, it should give the CE-PE link count for s_i. We compute traffic matrices for each hour of the day across 105 days and plot the sum of the 95^{th} percentile values of the relevant $N(s_i, d_j)$ values for a small and large VPN. The plots show that the mean plus four times the standard deviation of the observed SNMP measurements agrees closely with the 95^{th} percentile values obtained from the estimates. This means that the results of estimation are accurate in the aggregate, as we would expect given the way the optimization formulation was built.

5.3.2 PE-PE link traffic

We now compare the traffic on PE-PE links based on the estimated matrices to measured SNMP data for the traffic on these links. As noted previously, the CE to CE path consists of a core network segment where it is shared among multiple VPNs. By summing all $N(s_i, d_j)$ variables of a VPN that traverse a given PE-PE link, we obtain the estimated contribution of a VPN to a given PE-PE link. We then consider all VPNs that share this link and repeat the same procedure. Summing across all such results across VPNs, we obtain the estimated PE-PE traffic and exam-

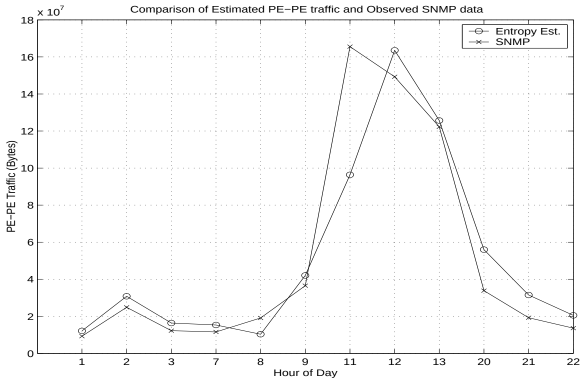

Figure 16: Estimated traffic vs Observed traffic for a PE-PE link with higher traffic features better accuracy; estimates mimic the shape and order of the actual traffic in all cases

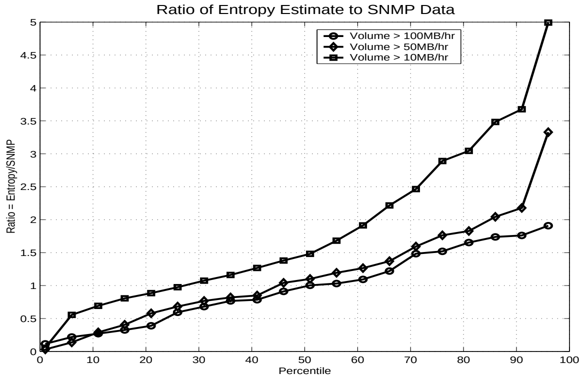

Figure 17: The error decreases when we look at links with larger volume

ine it with reference to SNMP data. Fig. 15 depicts a PE-PE link with lower traffic volumes. The accuracy of PE-PE traffic estimates reduces for links with lesser traffic. The errors are markedly lesser for links with higher traffic as depicted in Fig. 16. This is due to the fact that, the errors in SNMP measurement become comparable to traffic volume of smaller links. However, both the graphs show that the estimated numbers follow the same pattern of variation as the measured numbers in time over a complete day.

Reasonable accuracy in estimating the aggregate PE-PE links has implications for bandwidth provisioning tasks. Typically, core capacity provisioning involves a factor of safety and estimates to drive such a task need not be exact. A factor of 2 error in the estimate is usually considered tolerable. With this goal in mind, we repeat the PE-PE validation procedure with around 700 links and obtain Fig. 17. This figure indicates the ratio of the TM estimate to the observed PE-PE SNMP traffic for various link volumes. We note the following from this graph:

- For a large number of links, the estimated PE-PE traffic is within 50% of the SNMP observed traffic and most of the cases it is either close to the SNMP quantity or greater.

- Significant under-estimation happens in around 25% of links considered and these cases were traced to three problems in the data for VPNs traversing those links: (a) the PE-CE and CE-PE SNMP data was zero even when the PE-PE data seemed to be significant; (b) there were more bytes transmitted from the PEs to the CEs than what was received by the PE (measurement inconsistency); (c) the total bytes received by CEs was greater than the total bytes transmitted, i.e., there were external sources not accounted for in the SNMP data.

- Significant over-estimation occurs when the traffic volume on the link being considered is “small”. By “small” we mean it is comparable to errors in SNMP data. E.g., in cases where the difference in the number of bytes input to a PE and the number of bytes leaving it is 10MB and the PE-PE traffic volume was also about 10MB.

The validation considered here is not complete since we do not have actual per-VPN traffic data. Due to the scale of the exercise it is unlikely that such data will be available in the near future. In addition, owing to the mission critical and private nature of VPN traffic, there are a lot of administrative hurdles to obtaining access to such traffic. Thus, we need to examine traffic matrix estimates in the current framework and evolve guidelines to gauge the reliability of the estimates.

5.4 Reliability of Traffic Matrix Estimates

Estimation techniques such as those described here deal with aggregate byte counts and some additional side information to arrive at the components that led to that aggregate byte count. Even if the SNMP counts match the estimates, it is not necessary that the individual VPN matrices are correct. But we employed multiple strategies to gain confidence in our technique, viz., validation with synthetically generated data and indirect measures involving CE-PE and PE-PE SNMP data.

Observe that so long as most of the VPNs being analyzed exchange the bulk of their traffic on PE-PE links, the estimates are reliable if per-customer clustering of CEs is low. This is because, the traffic passes three segments: (a) the CE-PE link, (b) the PE-PE link and (c) the PE-CE link on the destination side. Now (a) and (c) are part of the constraints in the optimization formulation. So any solution that has the property that the variables sum to the observed access link aggregate may be acceptable. Now, consider the case when the PE-PE link counts match reasonably. If there are a number of CEs of a given VPN attached to a PE, we might still have errors in estimation - we could assign more bytes to a particular CE and still satisfy all constraints of the optimization. But if the number of CEs on a PE is small, then since all the segments of the transit route match with measurement, we must have a good estimate. Thus we evolve a set of guidelines to gauge the reliability of the estimates exploiting the observations of the previous sections.

1. If the number of CEs of a VPN homed on the same PE is low and the VPN is of Hub/Spoke type, the traffic matrix estimates are reliable.

2. Given consistent measurement data, PE-PE aggregate traffic can estimated with reasonable accuracy for provisioning purposes.

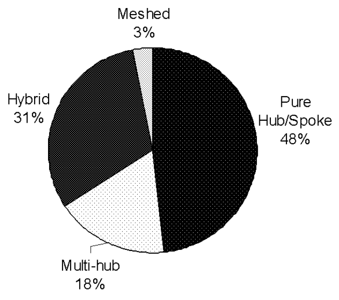

Figure 18: Structural classification of all VPNs

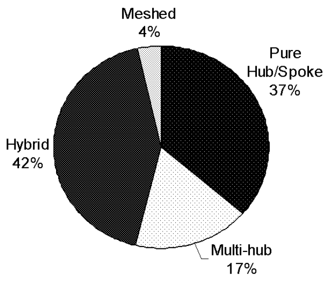

Figure 19: Structural classification of big VPNs

In the current dataset, we have found the number of CEs of a given VPN per PE to be low and that a lot of VPNs are of a hub/spoke nature. Hence we are in a position to study the structural characteristics and temporal characteristics of these VPNs.

6. SPATIAL STRUCTURE FOR CLASSIFICATION

Based on the way VPN endpoints communicate with each other (using the derived traffic matrices), three broad categories for the VPN structure can be deduced: (a) Pure Hub/Spoke, (b) Multi-Hub/Spoke, and (c) Hybrid VPNs. As the name suggests, a pure Hub/Spoke VPN features "spoke" nodes that communicate with just one node called the "hub". With Multi-hub/Spoke VPNs, there are two or more hubs with which all the CEs communicate. VPNs that cannot be grouped into either of these categories are termed Hybrid VPNs.

To identify the structure of a VPN, we obtain the set of peers for each CE by examining the estimated traffic toward all other CEs in the VPN. Note that the estimation procedure provides non-zero estimates so long as the input and output bytes of a given CE pair are non-zero. Hence even though a pair of CEs do not communicate with each other in reality, the estimate might attribute a non-zero value to the pair. Fortunately, the fact that hub traffic is far greater than that of spokes causes these spurious estimates to be small in the case of Hub/Spoke VPNs. Hence we build an approximate set of peers for a CE after pruning lower values which are more likely to be estimation errors. In the current dataset, some of the spoke traffic matrix variables are zero due to the observed input and output bytes being zero. We then prune the bottom 25% percent of possible peer CEs to mitigate estimation errors. Once the peer set is obtained, the criterion used to judge whether a node is a hub is to check if the set spans more than 50% of endpoints in the VPN.

Thus, given traffic matrix estimates for a VPN, we employ the following procedure to identify its structure:

1. Obtain the set of peer CEs for every CE after eliminating zero values and pruning the bottom 25% in terms of estimated traffic volume.

2. If a CE communicates with more than 50% of the endpoints in the VPN it is judged to be a hub node.

3. If a CE has 1 or 2 peers, it is classified as a spoke.

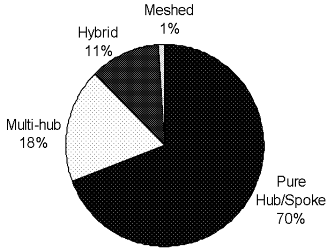

Figure 20: Structural classification of small VPNs

4. If a CE is in neither of the above categories the VPN is classified as hybrid.

5. After classifying all CEs, we examine the VPN. If the VPN has exactly one hub and all other endpoints are spokes, we classify it as a pure hub/spoke VPN.

6. If it has more than one hub but the number of hubs is less than 50% of the size of the VPN, we judge the VPN to be of the Multi Hub/Spoke nature.

7. If more than 50% of the nodes in the VPN are hubs, we say the VPN is of the meshed kind.

Fig. 18 depicts the analysis of around 600 VPNs in the dataset. The classification indicates that a significant number of the VPNs are of the Hub/Spoke nature. Frequently, the VPNs have 2 or 3 hubs for redundancy and load balancing.

The classification indicates that with larger VPNs (upper 33%-ile - Fig. 19), the structure becomes very complex and there are more of these classified as hybrid. Across various sizes of VPNs, there is a significant fraction that is of the hub/spoke nature (either Pure or Multi Hub/Spoke). This has implications for provisioning and traffic engineering as we shall note in §7.1. Small VPNs (lower 33%-ile - Fig. 20) tend to exhibit simple structures like pure hub/spoke. As an example, we look at the communication structure of a small meshed VPN. Fig. 21 shows the traffic from three endpoints in a VPN of size 4 illustrating a mesh type of communication among the endpoints. Each plot depicts the traffic from a given endpoint to other members of the VPN. The plots have been generated using traffic matrix estimates over many days. Hence there are notched boxes that denote the range of values for traffic observed toward a given endpoint. The notched box usually features three horizontal lines indicating the 25, 50 and 75 percentile values. VPN C shown

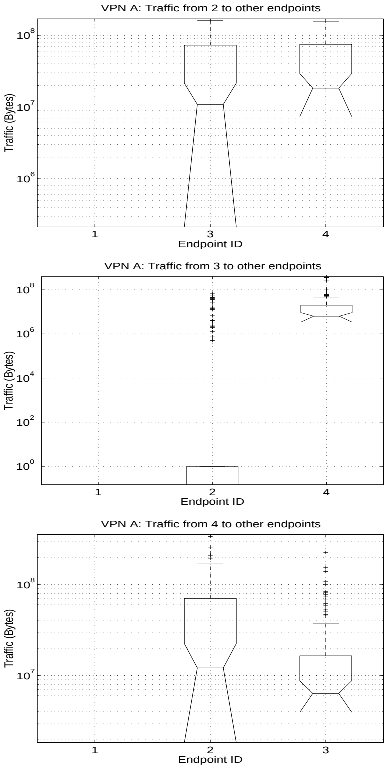

Figure 21: Small VPNs have simple structure. The one depicted above has 3 of the 4 nodes in the VPN forming a mesh

in Fig. 22(a) exhibits a hub/spoke structure. Fig. 22(a) features traffic flowing from a "spoke" to endpoint 4, which we characterize as a hub. The hub node on the other hand communicates with most other endpoints as shown by Fig. 22(b). Often VPNs cannot be categorized in either of these categories. VPN B featured in Fig. 23 shows a given endpoint communicating with many other endpoints with orders of magnitude difference in the traffic volumes.

Such structural characteristics are very important to efficiently provision network resources. Provisioning decisions can be fine-tuned over the lifetime of a VPN exploiting its structural characteristics. Instead of a mesh of N^2 reservations for a N node VPN, we could tailor allocations depending on the structure of the VPN. There is a resultant simplification in provisioning especially in the case of pure hub/spoke and two hub VPNs.

7. TEMPORAL STRUCTURE AND PROVISIONING

Once a VPN is admitted, the provider would want to ensure that irrespective of future admissions, the SLAs are met. Further, for a new VPN there is not much information regarding traffic characteristics and hence provisioning has to be approximate and conservative. In order to ensure SLAs, the provider needs to learn customer demands and how they change over time. In the case of new VPN customers, the initial conservative resource allocation can be fine-tuned over time by learning customer characteristics.

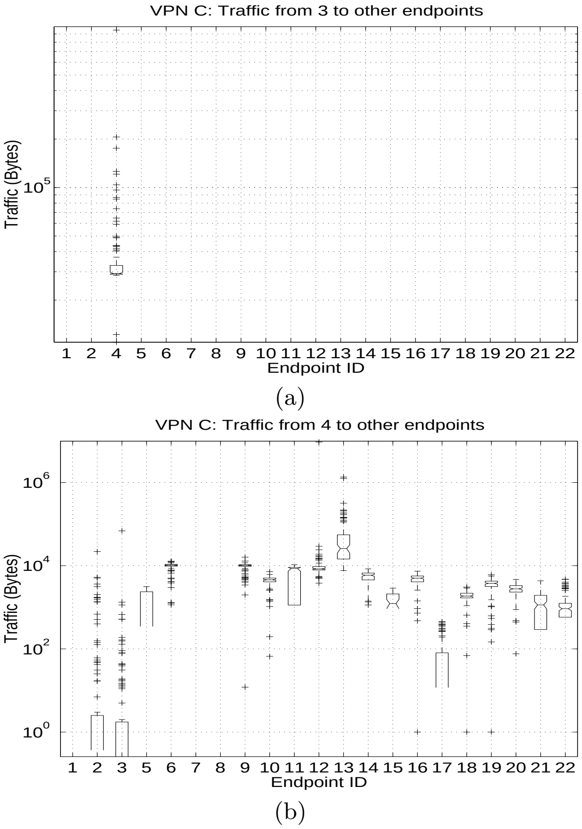

Figure 22: Hub/Spoke-like behavior can be seen with some endpoints in VPNs such as above

Faster changes in traffic characteristics imply that provisioning needs to be more responsive. Links may need to be resized to accommodate existing customers. On the other hand, slower changes in traffic would allow the provider to exploit multiplexing gains and increase the number of customers served. Thus we are interested in studying the changes in traffic matrices over time to judge whether complex dynamic provisioning strategies can yield appreciable gains.

Fig. 24 demonstrates the traffic matrix for an endpoint in a Hub/Spoke VPN for various times of the day. In this figure, SNMP data collected between 6am and 10am are counted for morning traffic, the data from 11am and 2pm is considered as noon and the duration between 8pm-12 midnight is considered as night. Each point in these graphs is the median of the number of bytes seen in those hours, computed using a set of weekdays. The error bars (the vertical lines) indicate the 25^{th} and the 75^{th} percentile values. When the 25^{th} percentile value is too low compared to the median, the error bar is truncated and this is indicated by a downward arrow.

The trend (the proportion of traffic to a given endpoint relative to the others) show a similar shape although there is difference in magnitude indicating that time of day is a distinguishing factor. With this observation, we now consider traffic matrix changes over longer timescales. In Fig. 25 we examine traffic trends across multiple weeks for a given endpoint. Each curve shows the median traffic toward an end-

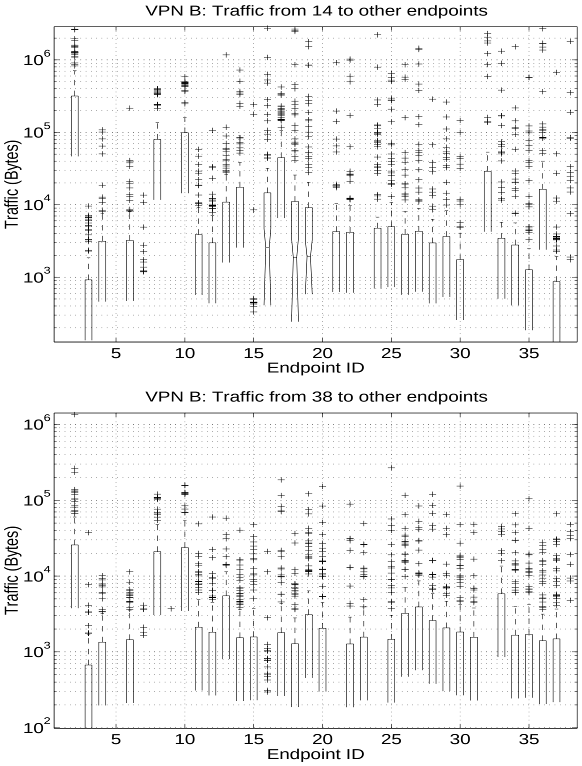

Figure 23: A larger VPN exhibiting complex interactions between various endpoints. There are orders of magnitude difference in the amount of traffic toward different CEs

point with the error bars indicating the percentiles as above. Barring one point, the trend for morning traffic across weeks is strikingly similar. This means that the trends change slowly, so that intelligent provisioning schemes have enough time to learn the traffic characteristics and act accordingly.

Extending the analysis over several months gives us some more insight. Fig. 26(a) and Fig. 26(b) depict trends for traffic from a given endpoint in two VPNs of different sizes toward the rest of the endpoints. While trends in one of the VPNs are stable over time in both shape and magnitude, the second plot shows magnitude variations over weeks with the later weeks featuring higher traffic. In such cases where either VPN traffic grows over time or VPNs add new endpoints over time, learning traffic matrices is very useful. Additionally this also means that even if initial provisioning is conservative, growth in VPN traffic might render it insufficient if adaptive mechanisms are not in place.

7.1 Impact on Provisioning

The discussion in the previous paragraphs lead us to the following important observations:

- **Traffic Engineering:** The traffic matrices provide us an estimate of the size of the customer aggregate in the core network. This allows us to conduct traffic engineering on a per-customer aggregate basis: we can re-map traffic for a given customer on to a new logical path and have an estimate of the added load and available capacity. Without this information, traffic engineering would have to handle PE-PE aggregates as a whole.

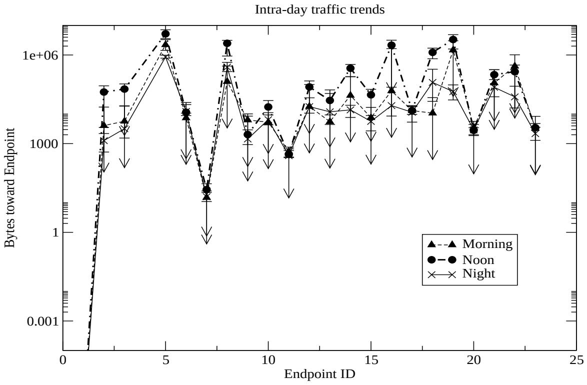

Figure 24: An Endpoint communicating with multiple peers; traffic proportions to other endpoints are very similar for different times of day, although the magnitude varies.

- **Bandwidth Allocation:** Exploiting spatial characteristics can lead to simplified provisioning and efficient resource allocation, especially in the case of endpoints which communicate with just one or two other peers. Addition of new endpoints in the VPN and growth in customer demand over time are better handled by learning traffic characteristics.
- **Customer Differentiation:** Since the traffic matrices provide an estimate of the size of the customer aggregate in the core network, the provider can choose to provide preferential treatment to a selected set of customers more efficiently. For the chosen set of customers, the provider keeps track of the aggregate demands using traffic matrices and makes allocations appropriately. The temporal characteristics of the traffic matrix indicate that the aggregate characteristics vary slowly and can be learnt.
- **Managing network failures:** The additional knowledge of customer traffic can lead to elegant management of network failure and maintenance events. E.g., the aggregates leading to a hub node can be mapped on to a new path which has more available capacity.

8. SUMMARY AND CONCLUSIONS

This paper analyzed two important properties of VPNs: (a) the structure of customer endpoint (CE) interactions and (b) the temporal characteristics of CE-CE traffic. Understanding actual customer behavior for large scale VPNs can help in many ways including dealing with traffic engineering, bandwidth allocation, moving a service to a different infrastructure, and other provisioning and maintenance operations.

We began with SNMP measurement information for 5 months from a large IP VPN service provider featuring about 6000 logical links. The VPNs had customer end points ranging from a few tens to several hundreds. With such a realistic, large scale service, there are significant barriers to obtaining detailed, per-customer measurement information.

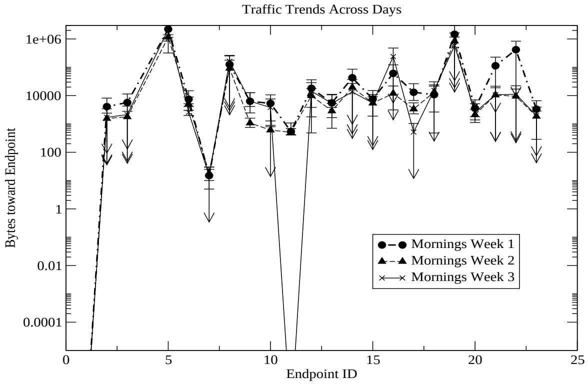

Figure 25: Traffic trend from an endpoint to others in a VPN remains similar across multiple days.

Consequently, there is only coarse grained aggregate SNMP data of traffic on the internal PE-PE links of the service. To get structural and temporal information about individual VPNs, we needed to evolve previous traffic matrix estimation approaches to overcome the problems posed by the scale of our problem (the matrix for the entire problem is in the range of nearly 3 Million elements.) Based on the characteristics of VPN traffic, we developed bounds on the traffic generated by a VPN on an individual PE-PE link, and used these in our technique to estimate the traffic matrices.

Without actual per-VPN measurements, it was difficult to directly validate our traffic matrix estimation approach. We adopted a two-pronged approach. First, we used a synthetic data set to compare the traffic matrices obtained with our technique to the actual, a-priori known traffic matrix. The synthetic data set we used was based on the broad characterization obtained from the SNMP measurement data, to allow us to have greater confidence in our approach. We showed that our approach works very well for Hub/Spoke VPNs. Second, we examined indirect measures by deriving aggregate CE-PE and PE-PE traffic volumes from the estimated traffic matrices, and then compared it with the measured aggregate SNMP count. Our estimates for the mean and the 95^{th} percentile of the CE-PE traffic agreed closely with the actual values. We also showed that estimates for the aggregate PE-PE traffic were reasonably accurate. They were more accurate for links of higher capacity, and are able to reflect the temporal characteristics that are actually present in the traffic.

We then analyzed spatial and temporal characteristics of customer VPNs. We identified three broad categories of VPNs: pure hub/spoke, multi-hub/spoke and hybrid VPNs. Overall, approximately 48% of the VPNs are of the hub/spoke category. But for small VPNs (the bottom 33% of the VPNs), hub/spoke VPNs dominate (70%). Of the multi-hub VPNs (18% of all VPNs), interestingly 95% are 2-hub VPNs. A significant portion of the big VPNs (top 33% of VPNs) are Hybrid VPNs (that are neither hub/spoke nor meshed VPNs). The percentage of pure “meshed” communication where any node talks to any other node is relatively small (at 3%).

An examination of the temporal properties of traffic matrices showed that they are quite stable over the period of a day, and even across days over a period of weeks. Thus, we can use this measurement data to get an idea of the ”stable” VPN structure for each customer VPN, and thus, have a reasonable estimate of the demand of each VPN customer endpoint on access and core links. We believe that this paper is unique in providing an understanding of VPN characteristics from an operational, large scale VPN service.

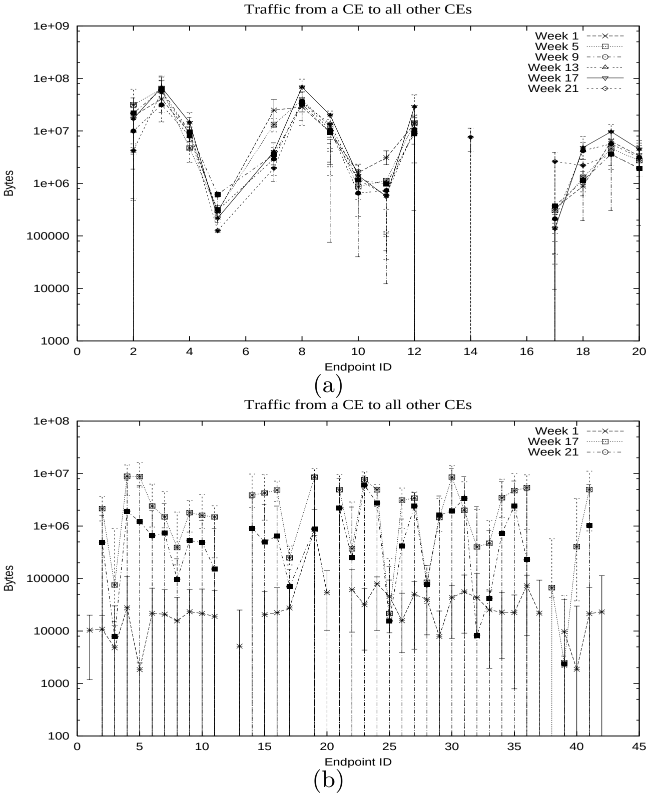

Figure 26: Long term trends for traffic from a CE to all other CEs in VPNs of higher size

9. REFERENCES

[1] N. Duffield, P. Goyal, A. Greenberg, P. Mishra, K. Ramakrishnan, and J. van der Merive. Resource management with hoses: point-to-cloud services for virtual private networks. *IEEE/ACM Trans. Networking*, 10(5):679–692, Oct. 2002.

[2] A. Feldmann, A. Greenberg, C. Lund, N. Reingold, J. Rexford, and F. True. Deriving traffic demands for operational IP networks: methodology and experience. *IEEE/ACM Trans. Networking*, 9(3):265–279, June 2001.

[3] A. Medina, N. Taft, K. Salamatian, S. Bhattacharyya, and C. Diot. Traffic matrix estimation: Existing techniques and new directions. In *Proc. of ACM SIGCOMM 2002*, Pittsburgh, USA, Aug. 2002.

[4] S. Raghunath and S. Kalyanaraman. Statistical Point-to-Set edge-based quality of service provisioning. In *Proc. of QoFIS 2003, Springer Verlag LNCS 2811*, volume 2, pages 132–141, Oct. 2003.

[5] Y. Zhang, M. Roughan, C. Lund, and D. Donoho. An information-theoretic approach to traffic matrix estimation. In *Proc. of ACM SIGCOMM 2003*, pages 301–312, 2003.