Multi-Timescale Internet Traffic Engineering

Richard M. Mortier, Microsoft Research Ltd.

ABSTRACT

The Internet is a collection of packet-based hop-by-hop routed networks. Internet traffic engineering is the process of allocating resources to meet the performance requirements of users and operators for their traffic. Current mechanisms for doing so, exemplified by TCP's congestion control or the variety of packet marking disciplines, concentrate on allocating resources on a per-packet basis or at data timescales. This article motivates the need for traffic engineering in the Internet at other timescales, namely control and management timescales, and presents three mechanisms for this. It also presents a scenario to show how these mechanisms increase the flexibility of operators' service offerings and potentially also ease problems of Internet management.

INTRODUCTION

Traffic engineering is "concerned with the performance optimization of networks" [1]. It addresses the problem of efficiently allocating resources in the network so that user constraints are met and operator benefit is maximized. A common way to decompose the problem of network resource allocation is to consider three timescales over which resources are allocated [2]: *data timescales* deal with allocating resources to individual packets; *control timescales* deal with allocating resources to aggregates of packets, or flows; and *management timescales* deal with allocating resources to aggregates of flows, such as occur when traffic is transferred between two networks. As all three timescales affect user perceptions of service, this article argues that traffic engineering in the Internet is required at control and management timescales in addition to current approaches at data timescales, and presents mechanisms for such purposes. Thus, this article continues with brief descriptions of approaches to network service offerings, the network in question (the Internet), and finally resource allocation in the Internet in particular. Subsequently, it presents two mechanisms for controlling resource allocation at control timescales: an admission control scheme for TCP, an ECN proxy for RTP, and a mechanism for controlling resource allocation at management timescales through pricing for the BGP routing protocol. It ends by considering how these mechanisms can be applied to increase service differentiation between operators.

APPROACHES TO NETWORK SERVICE PROVISION

Current approaches to service provision by operators fall into two categories. *Service-oriented* approaches, such as those offered by telephone companies and cable providers, offer a tightly specified range of predefined services to limit management complexity. Unfortunately, discrepancies between operators' expectations and user requirements of these services means that some will use them in unexpected ways. This can cause such services to perform less well than they should, for example due to incorrect assumptions for provisioning. Solutions to such problems tend to be ad hoc and often require management intervention.

Conversely, *technology-oriented* approaches assume that all users of a particular technology place equal value on the use of that technology. Examples include the complex ATM Forum service classes, or more simply the standard behavior mandated by the Internet Engineering Task Force (IETF) for the Transmission Control Protocol (TCP) and associated TCP-friendly protocols. Both assume that two users always place equal value in an identical service specification.

The assumption that users place equal value in each byte transmitted across the Internet using TCP is carried through into the agreements between operators. Such service level agreements (SLAs) specify many parameters. Some are administrative, such as technical support provisions and number of peering points available. Others are more technical and cover matters such as the bandwidths available in the peering networks and the ratios of traffic to be exchanged. In general, it seems that bandwidth is the principal network resource covered, so this is the resource considered in this article.

Richard Mortier was a Ph.D. student with the University of Cambridge Computer Laboratory whilst carrying out this research. He is now with Microsoft Research Ltd. Cambridge.

0163-6804/02/$17.00 © 2002 IEEE

Different techniques are required to deal with the competing desires of the operators to simplify the services they offer while still providing sufficient flexibility for users to express their individual requirements, and incentives for them to do so accurately.

A Model of the Internet

The Internet functions as a loosely structured collection of networks, or autonomous systems (ASs). In more detail one can divide the Internet into a number of parts. At the edges of the Internet users connect to Internet service providers (ISPs) to gain access to the network. Access methods range from analog dialup services, typically at around 48 kb/s, through to cable modem and other technologies at between 128 kb/s and 10 Mb/s. A smaller proportion of users on corporate and academic networks also connect via technologies such as Ethernet or leased lines at speeds of 10 Mb/s upward.

Moving further into the network, user-facing ISPs typically use larger network operators to provide connectivity to other networks. Depending on the level of service required in terms of bandwidth, reliability, and so on, the ISP may use many such large network operators. The larger operators provide this connectivity via routing information. They advertise routes for the prefixes delegated to the ISPs so that traffic from other sources can reach the ISPs. In addition, they give the ISPs routing information about the rest of the network so that traffic originating from ISPs' networks can reach external destinations.

Finally, at the core of the network there are two types of large network operators that provide transit services for traffic injected by themselves and their customers. The first install and maintain their own physical networks requiring a large investment in infrastructure, and for this reason are often originally telephone operators. The second rent capacity on existing network infrastructure, allowing them access to the market without such high entry costs but at the cost of some flexibility.

Operators exchange traffic at *peering points*, either *public* or *private*. Public peering points, the norm until relatively recently, generally support a large number of operators. Networks are connected using, for example, 100 Mb/s and 1 Gb/s switched Ethernet, and routing information is exchanged between operators according to previously negotiated agreements and the associated imposed policies and filters.

Private peering points are usually created between pairs of operators, who often make available higher bandwidths than at public peering points. Due to the more restricted participation, management and verification of the pertinent agreements are typically much simpler. Generally, once agreement to privately peer is reached, traffic and routes are exchanged without further interference. Monitoring is likely still to be carried out to enable dealing with changes in traffic characteristics.

Resource Allocation in the Internet

Although this structure is technically highly flexible, it suffers from a lack of accountability. The Internet originally provided end-to-end connectivity between cooperating users across a small number of cooperating public networks, requiring little support for accounting, authenticating, or policing network use.

Increasing commercialization of the Internet and migration of more socially fundamental services such as telephony bring out problems due to lack of accountability in two ways. First, the commercial world requires knowledge of the quality of services provided and received in order to effectively manage and cost services and associated agreements. Second, government agencies and other regulatory bodies become involved and require that operators provide audit trails to ensure that an acceptable service is being provided at an acceptable price.

In the Internet community, work on resource allocation has generally concentrated on data timescales, including work done on congestion control schemes [3], per-packet payment mechanisms [4], and router scheduling and marking disciplines [5]. All of these address the problem of whether an individual packet should be introduced to the network at this time, whether by an end system or a router. Although such work is required for stable operation of the network, it is often not sufficient for efficient operation. For example, legacy applications may not understand modern packet marking schemes, routing protocols currently cannot route around overloaded networks, and there are situations where even modern TCP implementations can undergo congestion collapse.

It is more common to see issues of control and management timescale engineering addressed in circuit-based networks. For example, asynchronous transfer mode (ATM) generated a large body of work addressing admission control, a control timescale traffic engineering technique. Many of these techniques are also now finding application in multiprotocol label switching (MPLS) networks. In the past, the Internet community has attempted to address management timescale traffic engineering through load balancing routing [6]. However, such approaches only addressed routing within a single AS and have been abandoned as the Internet has grown in complexity.

Consequently, different techniques are required to deal with the competing desires of the operators to simplify the services they offer while still providing sufficient flexibility for users to express their individual requirements, and incentives for them to do so accurately. This article argues that this requires consistent mechanisms to control resource allocation on control and management timescales in addition to current data timescale mechanisms. Three mechanisms suitable for this purpose are now presented.

Implicit Admission Control

Implicit admission control is a mechanism enabling control timescale traffic engineering for TCP. This allows operators to better influence users' per-flow resource allocations, allowing stronger performance guarantees to be given to users and increasing service differentiation between operators.

TCP provides a reliable byte stream over the unreliable packet-based Internet Protocol (IP). It first constructs an end-to-end connection via a three-way handshake, and then uses receiver acknowledgments to indicate to the transmitter

the portion of the byte stream successfully received. The transmitter detects missing data either by expiry of a retransmission timer or through receipt of an acknowledgment for already acknowledged data, and retransmits as required.

Resource allocation for each TCP connection on a bottleneck link is effectively performed *cooperatively* by all hosts involved. They manage their windows of outstanding data, each pair ensuring that the receiver is always capable of receiving all data still in flight, and furthermore, that the network is not currently congested and unable to receive more data. Congestion is detected by the loss of packets and causes a reduction in window size. However, to allow for changes in load, the transmitter slowly increases its window if packets are not lost to see if the network is currently capable of taking more traffic. In this way the flows contending for resource on a bottleneck link should approach a fair share where all flows receive approximately equal throughputs (assuming all round-trip times are equal).

An alternative approach to allocating resource to flows is that of *admission control*, commonly used in telephone and ATM networks. In such networks, a source explicitly requests access to the network by signaling to the network that it requires a connection to a particular destination. Any network element along the path to the destination is free to refuse the connection request, denying access to the resource. Measurement-based admission control (MBAC) is an extension where the decision is based on real-time measurements of current load taken by network elements.

These mechanisms effectively trade the strength of the per-flow resource guarantee against access to the network: TCP can give no per-flow guarantee, but never denies a flow access to the network, whereas an ATM network can give strong per-flow service guarantees at the expense of sometimes denying a flow access to the network. MBAC makes the admission control process more dynamic and sensitive to changes in load, and can thus be viewed as somewhere between standard admission control and resource allocation as performed by protocols such as TCP.

To apply MBAC to the Internet there are two requirements: first, some metric of load that routers can measure; and second, some way to deny access to a connection request in a network where a source does not explicitly signal to network elements before transmitting data (packets) into the network.

The metric chosen in this implementation is buffer occupancy at the router. Using *Mtk*, the Measure Toolkit [7], an MBAC library previously developed for ATM networks, the router monitors its buffer occupancy and translates it into an estimate of the probability of dropping a packet. To deny a flow the router intercepts the first packet in the three-way handshake and then drops it or transmits a TCP reset connection packet to the source. Thus, the operator can set a desired threshold, and the router then admits or denies connections according to the current state reported by Mtk.

This system was implemented in both the NSv2 simulator to test its network impact and in Linux to test impact on applications using the IP Chains facility to intercept packets. The structure of the Linux implementation is shown in Fig. 1.

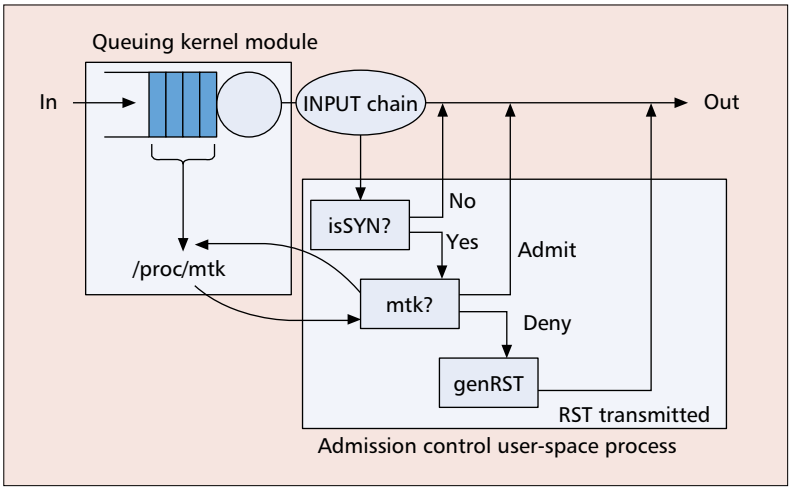

Figure 1. *Linux implicit admission control implementation.*

Threshold	Completed flows	Good flows	(%)	Bad flows	(%)
None	15,219	4595	(30)	10,624	(70)
1.0	12,065	7255	(60)	4810	(40)
0.5	11,427	7968	(70)	3459	(30)
0.1	10,192	8591	(84)	1601	(16)
0.05	9900	8634	(87)	1266	(13)
0.01	9157	8618	(94)	539	(6)

Simulation ran for 900 s, but only flows that started after the first 100 s had passed were counted to remove initial transient behavior.

Table 1. *The number of completed flows with the number that met a target of 10 packets/s over their lifetime (good flows), and the number that failed to meet this target (bad flows) at different target drop thresholds.*

Sample results are shown in Table 1. Defining a successful flow as one achieving a minimum of 10 packets/s, application of admission control causes more flows to complete successfully, increasing the likely satisfaction of users.

The success of this approach depends on users preferring to be told that they cannot currently connect to a particular destination, rather than them connecting but receiving such low throughput that they can do no useful work. Even with protocols such as TCP that operate successfully at a wide variety of bandwidths, higher-layer application semantics suggest that this can be the case. Consider, for example, Web browsing: it is perhaps less infuriating to be told that the server or network is currently too busy than it is to successfully connect and then wait many minutes for a single page to download. Further details of this approach, its performance, and how it interacts with current applications are available in [8].

An ECN Proxy for RTP

This section describes a proxy for the Real-Time Transport Protocol (RTP) that enables the operator to direct the behavior of RTP users. It

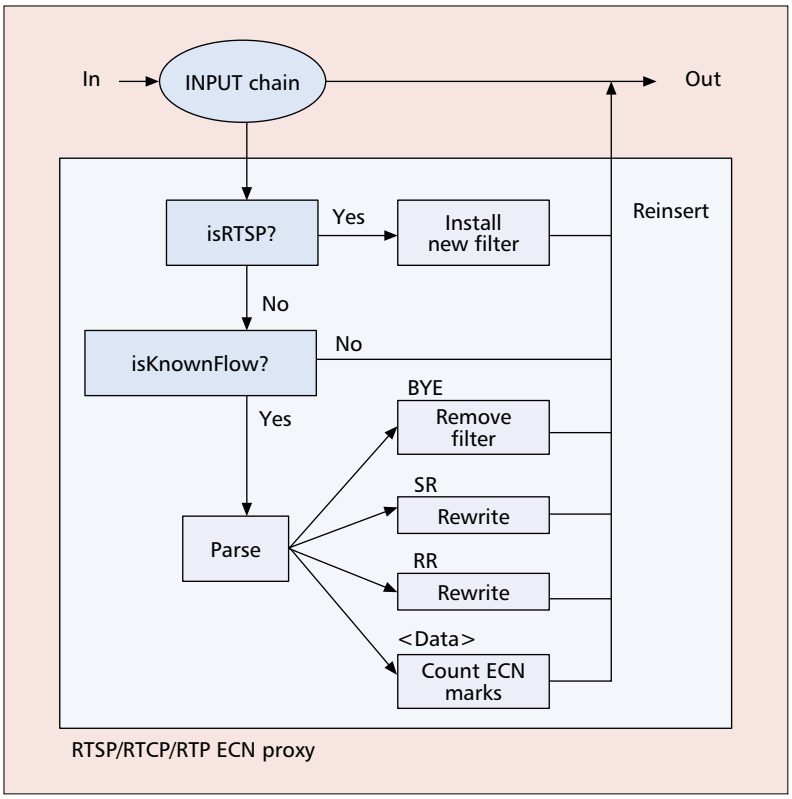

Figure 2. *Linux RTP-ECN-proxy implementation.*

allows operators to enforce behavior of legacy user applications in the face of modern congestion control signals from the network in the form of explicit congestion notification (ECN) marks.[1] This gives operators another mechanism allowing them influence at control timescales over the service achieved by users.

RTP consists of three subprotocols: RTP itself provides data transport using a number of different data format encapsulations. RTP streams then use the RTP Control Protocol (RTCP) to control the behavior of receivers and transmitters; the particular feature of interest here is the *receiver report* (RR), where the receiver uses a percentage of the bandwidth achieved by the stream to report the characteristics of the stream back to the transmitter. Finally, RTP/RTCP streams are created according to requests made via the Real-Time Streaming Protocol (RTSP).

The aim of the proxy depicted in Fig. 2 is to enable the operator to enforce correct behavior of legacy user applications in the face of congestion signals provided by ECN. As with IAC, this allows the operator to make stronger guarantees concerning their offered services.

A proxy tracks the creation and destruction of RTP/RTCP streams via RTSP, and monitors the ECN marked packets received on each RTP stream. It can then rewrite the RRs for the associated RTP stream, adding in some portion of the marked packets to the field reporting packet loss to the transmitter. The transmitter can then suitably scale its video encoding to use less bandwidth, with the aim of alleviating congestion. This effectively forces legacy platforms — both operating systems and applications — that do not understand ECN marks to behave as if they did. This system was implemented using Linux's IP Chains facility to intercept packets of interest and then either create new filters, count the ECN marks seen, or rewrite the RRs as appropriate. It was tested in conjunction with the *vic* videoconferencing tool, and the bandwidth used by video streams was controlled as described above. Further details are available in [9].

Pricing for BGP

Having presented two mechanisms for control timescale resource allocation, this section presents one for management timescale resource allocation.

Internet Routing and BGP

Internet traffic is routed by each router matching the destination address of a packet against the longest (and so most specific) address prefix known to that router. The corresponding routing table entry tells the router on which interface the packet should be transmitted in order for it to progress toward its destination. Information about which networks and routers "own" prefixes is disseminated via routing protocols.

Management timescale resource allocation is effectively implemented via these routing protocols. There are two principal classes of routing protocol: interior gateway protocols (IGPs), operating within a network and dealing with the prefixes owned by that network; and exterior gateway protocols (EGPs), operating between networks and dealing with prefixes reachable via other networks. Individual routers independently build their forwarding tables based on the information they receive via the different routing protocols they are running.

The routing protocol considered for this work was the Border Gateway Protocol (BGP). This is the EGP used throughout the Internet to disseminate routing information between operators' networks. It is a *path vector* protocol, so it disseminates prefixes with the AS path taken to get to the prefix. The lengths of these paths effectively form the weight associated with the prefixes in the absence of other metrics configured by the operator. Routers then make choices as to the preferred route, typically choosing and re-advertising the route with the associated shortest AS path.

The choice of preferred route can be controlled by the operator in two ways. First, *filters* can be applied to prevent certain routes being considered, ensuring that information about certain routes is only considered from and transmitted to certain peers. Second, BGP allows each router to associate *path attributes* with sets of prefixes. Based on the values of these path attributes, routers can be configured to treat sets of prefixes differently.

However, many of these path attributes can interact in unexpected ways, and none provide a globally transitive metric. Consequently, current deployments rely on controlling the length of the AS path by prepending multiple copies of their own AS number to routes they wish to discourage peers from using: study of sample BGP tables showed that this was done to approximately 8 percent of selected routes. This behavior is implemented by *ad hoc* agreements about

[1] *ECN is a scheme whereby two bits in the IP header are used by routers to mark a packet as having caused congestion in order that end systems can react to congestion without having to experience packet loss.*

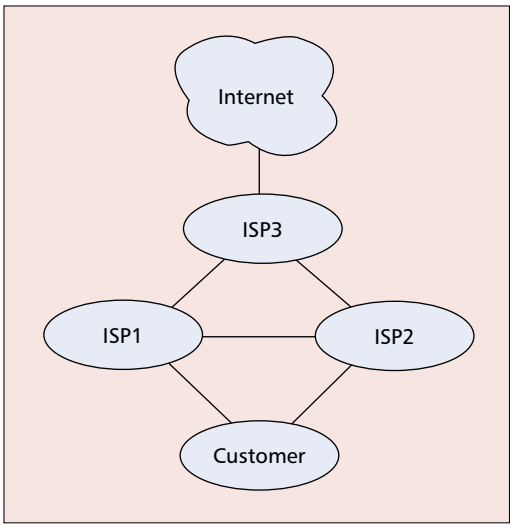

Figure 3. *A customer is multihomed to two ISPs that connect to the Internet via a third ISP.*

treatment of particular *community attributes*, optional nontransitive path attributes indicating policies concerning the associated routes. There is evidence that this behavior has a detrimental effect on the efficiency of the network by causing less efficient paths to be chosen [10].

Furthermore, situations where there is a choice between routes are on the increase due to the desirability of *multihoming* by customers for reliability. Multihoming is where a customer connects to the Internet in more than one place, either to a single ISP in multiple places or through more than one ISP, as depicted in Fig. 3.

The problematic case is the latter since care must be taken over who "owns" the IP addresses the customer will use. If the customer uses addresses delegated by one ISP, those addresses are likely to be announced by that ISP as part of an aggregated block, but by other ISPs as addresses specific to that customer (since the other ISPs cannot aggregate the addresses delegated by the first ISP). In this case "magnetic" longest-prefix-match behavior will take over and may cause traffic for the customer to arrive via all but the first ISP.

Similarly, if the customer is delegated addresses out of all the ISPs' address spaces care must be taken to avoid magnetic longest-prefix-match behavior if addresses delegated by one ISP are advertised to others for increased reliability for the customer. The alternative is for the customer to get its IP addresses from some other registry. However, this decreases the aggregatability of routes in the Internet, since all ISPs are then unable to aggregate the customer's addresses into their existing address blocks.

Although these mechanisms allow control of routing policy by the operators, they are not intuitive to use, and it is common for operators to make mistakes and implement filters that do not behave as intended. Furthermore, it is possible to implement valid configurations that cause persistent or even permanent route oscillation, typically due to conflicts or other interactions between route preferences [11].

The mechanism presented here aims to address both of these issues. Using pricing as a basis for route choice should reduce policy conflicts since operators will require good reasons to choose more expensive routes where cheaper ones exist. Such a system should also make implementation of route preferences more intuitive and thus easier for operators to implement correctly.

Implementing Pricing in BGP

The approach taken here is for each AS to measure its current load and then calculate a *price* for carrying further traffic based on the measured load. This price is then transformed into a *charge* to be advertised to the peers of the AS. The transformation into a charge allows different policies to be applied to different peers; for example, certain peers might be preferred over others, and thus could be offered discounts. The charge is advertised to peers via a new optional path attribute, enabling incremental deployment: routers or operators that do not wish to take part will simply ignore the price path attribute.

Having received price path attributes associated with prefixes, operators can choose their best routes on the basis of the charges they will incur. Hence there must be a basis for *settlement*, where the charges associated with neighboring prefixes are transformed into bills. There are likely to be two components to the final bill: a fixed charge to recoup the basic costs of exchanging traffic, and a traffic-based charge to implement the incentives required to enforce acceptable behavior. If there is no traffic-based charge, the process reverts to the current system: operators agree to bounds on the ratio of ingress to egress traffic as part of their SLAs, and can then use the price as an indicator that these bounds are not persistently violated.

Although there are a variety of metrics on which settlement might be based, this article proposes use of the traffic volume exchanged between peers. Traffic volume has a number of advantages: it is straightforward to understand and measure; it is generally slowly varying between ASs, allowing operators to make relatively accurate predictions about future bills; and many operators already have to collect such information in order to police the SLAs into which they enter.

Although there are a variety of metrics on which settlement might be based, this article proposes use of the traffic volume exchanged between peers.

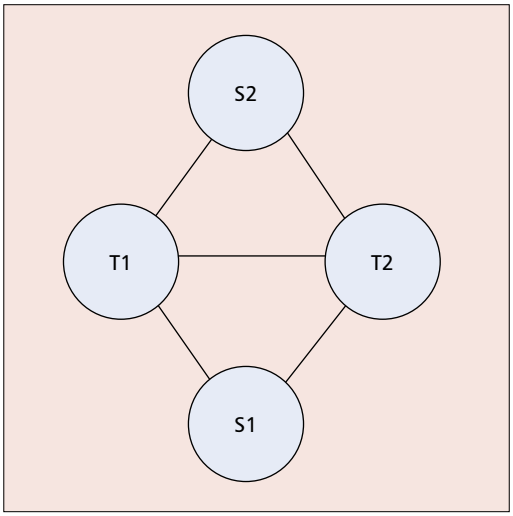

Figure 4. *The simulation topology.*

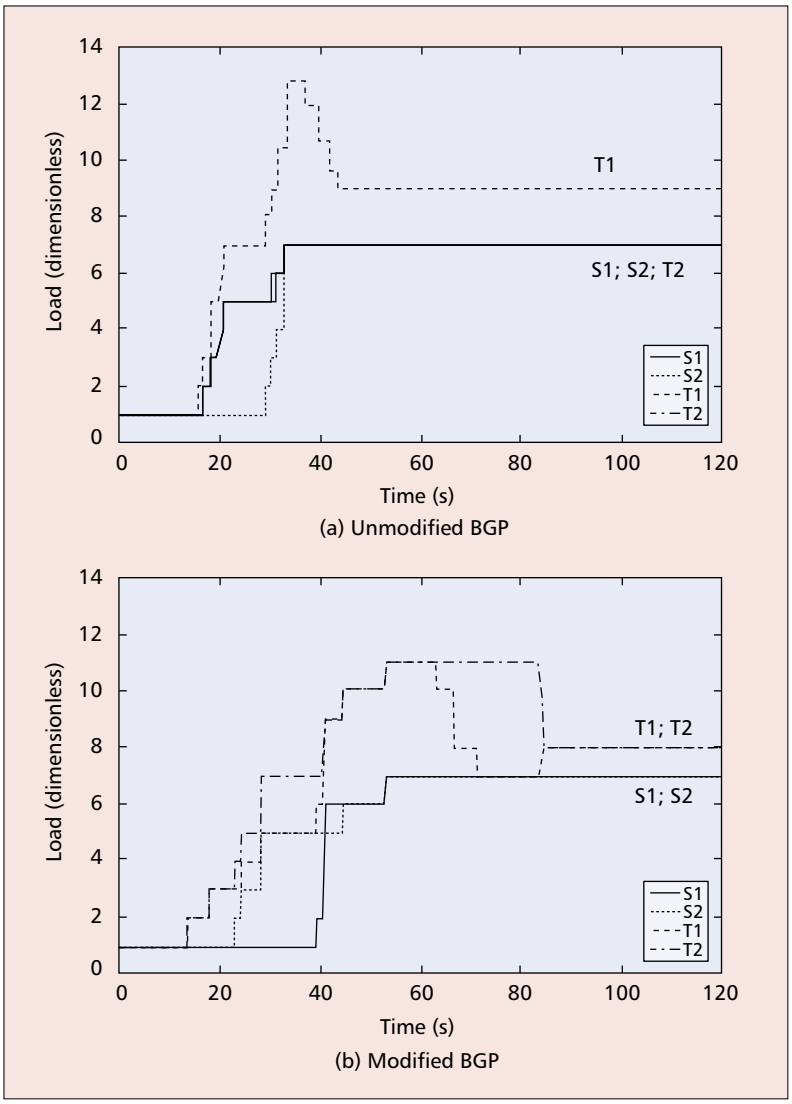

Figure 5. *Per-node load distributions for the topology shown in Figure 4.*

Of course, there is scope for more complex settlement schemes. For example, settlement might be performed based on the number of packets marked if suitable feedback could be arranged. Although this links the final bill more closely to congestion (since charges will not be levied unless congestion is occurring and hence packets being marked), such a scheme is more complex to understand and predict, and requires more infrastructure to support.

Simulating BGP Pricing

Since it is difficult to test such a proposal in the Internet at large, a simulation framework was implemented to enable it to be tested in the laboratory. The BGP daemon from the GNU Zebra routing suite was wrapped in a simple simulator harness, and this BGP daemon was then extended to support the new price path attribute. This enabled simple simulations to be carried out using a deployed implementation of the routing protocol, avoiding the need to implement BGP within an existing simulation framework with the associated likelihood of introducing bugs.

The simulator implements an extremely simple model of load. Each router is considered to carry one unit of load for each prefix it advertises, and one further unit for each entry in its neighbors' routing tables for which it is the next hop. Results are presented in [9]; Fig. 5 shows a sample for the topology given in Fig. 4. They demonstrate that the system converges both with and without pricing applied, and although it takes approximately twice as long to converge with pricing applied, it converges to a more even distribution of load, allowing the network to route around congestion.

Service Offerings

The three mechanisms presented — implicit admission control (IAC), the ECN proxy for RTP, and pricing for BGP — individually allow per-flow and interdomain control of resources; in combination they can allow operators to offer greater service differentiation.

Consider the situation depicted in Fig. 6. There are two edge ISPs, *CheapISP* and *QualityISP*, three users, Alice, Robert, and Charles, and a content provider, *BajaVista*. The core of the network is made up of a group of transit providers including *TopTransit* to which the ISPs and content provider connect directly. Alice subscribes to *QualityISP*'s platinum service, and Robert subscribes to their gold service. Charles chooses to subscribe to *CheapISP*. The content provider, *BajaVista*, wishes to ensure that all its users see a high quality service but requires that this be paid for.

Since Alice subscribes to such a high quality service, she is allowed as many premium quality flows as she likes, subject to some total limit applied by *QualityISP* to ensure that all flows can still make good progress. On the other hand, Robert has a per-user limit applied to the number of high-quality flows he can introduce. If *QualityISP* uses a mechanism to provide improved network quality for real-time media streams, this might translate to limiting the number of such streams Robert could achieve, or to utilizing a mechanism such as the proxy presented in an earlier section to limit the quality Robert's streams could achieve. Finally, since *CheapISP* offers no limit on the number of streams its subscribers can have, Charles can use as many streams as he wishes, but may see extremely poor service at times of high load. These are all examples of application of control timescale traffic engineering mechanisms used to increase the service differentiation offered to users.

BajaVista desires that all users see reasonable service. It subscribes to *TopTransit* specifying its desires. In turn, *TopTransit* advertises *BajaVista*'s prefixes with a low associated cost, and furthermore, it advertises them to other transit ISPs providing a high quality service. This should result in traffic for those prefixes typically following a high quality path to *BajaVista*. Conversely, *BajaVista* also subscribes to a high quality service from *TopTransit*, so that traffic from *BajaVista* will be transmitted efficiently toward the requester, be they Alice, Robert or Charles. This is an example of how pricing for BGP can act as a management timescale traffic engineering mechanism to improve the service experienced by users.

Settlement for the service *BajaVista* provides

will be provided by QualityISP for Alice and Robert as part of their standard service. Charles would have to subscribe to *BajaVista* directly. In all cases, the actual cost *BajaVista* incurs by attempting to appear to all users as if they were well connected to it could be monitored in terms of the number of marks arriving at the destination ISP, either *QualityISP* or *CheapISP*. The ISP could then either settle itself in the case of *QualityISP*, Alice and Robert, or it could pass the bill on to the user in the case of *CheapISP* and Charles.

The above scenario does require more work in accounting traffic, but this is offset by the increased value of the service provided, and the increased efficiency with which the network can be run. Increased accountability by providers coupled with the pricing mechanisms also provides a defense against denial-of-service attack, since the costs incurred can more easily be passed back to the instigator. However, in more complex scenarios, there are other issues such as stability and arbitrage that must be dealt with, some of which are discussed in [9].

CONCLUSION

This article motivated the need for Internet traffic engineering at multiple timescales. It then presented two mechanisms for traffic engineering at control timescales and one for traffic engineering at management timescales. All three mechanisms have been implemented and tested, and results reported elsewhere show that they achieve their aims. The simple concrete example presented demonstrates how the three mechanisms can be used to provide stronger service guarantees to users, and to increase the service differentiation operators can provide. At the same time the use of pricing as a unifying framework in which to perform resource allocation means that the presentation of such differentiation of service need not be overly complex for operators to manage, and for users to understand and use.

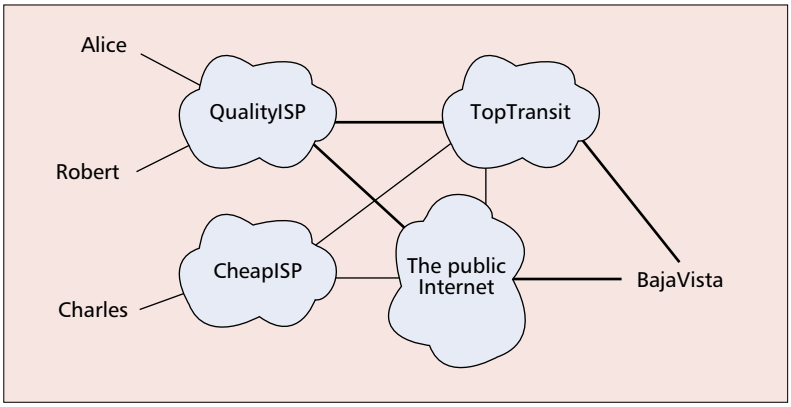

Figure 6. *A simple example.*

REFERENCES

[1] X. Xiao *et al.*, "Traffic Engineering with MPLS in the Internet," *IEEE Net.*, vol. 14, no. 2, Mar./Apr. 2000, pp. 28–33.

[2] J. Y. Hui, "Resource Allocation for Broadband Networks," *IEEE JSAC*, vol. 6, no. 9, Dec. 1988, pp. 1598–1608.

[3] K. Fall and S. Floyd, "Simulation-based Comparisons of Tahoe, Reno, and SACK TCP," *Comp. Commun. Rev.*, vol. 26, no. 3, July 1996, pp. 5–21.

[4] M. Falkner, M. Devetsikiotis, and I. Lambadaris, "An Overview of Pricing Concepts for Broadband IP Networks," *IEEE Commun. Surv.*, 2nd qtr. 2000; http://www.comsoc.org/pubs/surveys/

[5] S. Floyd, "TCP and Explicit Congestion Notification," *Comp. Commun. Rev.*, vol. 24, no. 5, Oct. 1994, pp. 10–23.

[6] D. L. Mills, "DCN Local-network Protocols," RFC 891, IETF, Dec. 1983.

[7] N. G. Duffield *et al.*, "Entropy of ATM traffic streams: A Tool for Estimating QoS Parameters," *IEEE JSAC*, vol. 13, no. 6, Aug. 1995, pp. 981–90.

[8] R. Mortier *et al.*, "Implicit Admission Control," *IEEE JSAC*, vol. 18, no. 12, Dec. 2000, pp. 2629–39.

[9] R. M. Mortier, Internet Traffic Engineering, Ph.D. thesis, Univ. of Cambridge Comp. Lab., Oct. 2001; also CUCL tech. rep. 532, http://www.cl.cam.ac.uk/TechReports/UCAM-CL-TR-532.pdf

[10] H. Tangmnarunkit *et al.*, "The Impact of Routing Policy on Internet Paths," *Proc. IEEE INFOCOM 2001*, Anchorage, AK, Apr. 2001.

[11] T. Griffin and G. T. Wilfong, "An Analysis of BGP Convergence Properties," *Comp. Commun. Rev.*, vol. 29, no. 4, Oct. 1999, *Proc. ACM SIGCOMM 1999*, pp. 277–88.

BIOGRAPHY

RICHARD MORTIER (mort@ieee.org) is a researcher with Microsoft Research Ltd., Cambridge, United Kingdom. His research interests are in systems and networking, covering operating systems, distributed systems, and local and wide area networking. Prior to joining Microsoft Research, he received a Ph.D. from Systems Research Group at the University of Cambridge Computer Laboratory, and a B.A. in mathematics, also from the University of Cambridge.