Network Element Service Specification for Low Speed Networks

Status of this Memo

This document is an Internet-Draft. Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress".

To learn the current status of any Internet-Draft, please check the "1id-abstracts.txt" listing contained in the Internet-Drafts Shadow Directories on ftp.is.co.za (Africa), nic.nordu.net (Europe), munnari.oz.au (Pacific Rim), ds.internic.net (US East Coast), or ftp.isi.edu (US West Coast).

This draft is a product of the Integrated Services Working Group of the Internet Engineering Task Force. Comments are solicited and should be addressed to the working group’s mailing list at int-serv@isi.edu and/or the author(s).

Abstract

This document defines the service mappings for controlled load and guaranteed services over low-bitrate networks. These low-bitrate networks typically include components such as analog phone lines, ISDN connections and sub-T1 rate links. The document specifies the per-network element packet handling behavior, parameters required, traffic specification, policing requirements, and traffic ordering relationships which are required to provide both Guaranteed and Controlled Load service capabilities. It also includes evaluation criteria for elements providing the service.

This document is a product of the IETF ISSL working group and is based on [1] and [2] which describe modifications to the PPP protocol to enable these services.
# Table of Contents

1. Introduction

2. End to end Behavior

3. Motivation

4. Network Element Data Handling
   4.01 Rate and delay
   4.02 Link Aggregation
   4.1 Controlled Load Versus Guaranteed Service
   4.2 Controlled Load and Guaranteed Service Data Handling
   4.3 Controlled Load and Guaranteed Service Class Mapping

5. Invocation Information

6. Exported Information

7. Policing

8. Ordering and Merging

9. Guidelines for Implementors
   9.1 Bit and Byte Stuffing Considerations
   9.2 Compression Considerations
   9.3 Admission Control
   9.4 Fragment Scheduling Considerations

10. Evaluation Criteria

11. Security Considerations

12. References

13. Authors’ Addresses

Appendix A - Additional Admission Control Issues for PPP Links
1. Introduction

The ISSLOW subgroup of the ISSL working group has focused on defining mechanisms to permit flow differentiation and QoS capabilities for mixed traffic over low speed links. This has been accomplished through a series of extensions to the PPP protocol which permit fragmentation and/or suspension of large packets in favor of packets on flows which require QoS. These protocol extensions are presented in [1] and [2].

This document describes the service mapping required to implement the controlled load and guaranteed services over these PPP protocol extensions. It is modeled on the Network Element Service Specification Template described in [3]. It is assumed that the ISSLOW Network Element is one portion of a PPP service available to the system.

2. End-to-end Behavior

Unlike many of the other specific link layers addressed in the ISSL working group, ISSLOW operates only over low speed point to point links or connections. Examples of these links include dial up lines, ISDN channels, and leased lines. As such, ‘end to end’ simply means between two points. In today’s inter/intranet environment, this will include:

- host to directly connected host.
- host to/from network access device (router or switch).
- Edge device (subnet router or switch) to/from router or switch.
- In rare circumstances, the link may run from backbone router to backbone router.

Thus, the endpoints are two network elements as described above. The Controlled Load and Guaranteed services for ISSLOW links are applied on the link between these elements and often represent the first or last wide area hop in a true end to end service. It is important to note that these links tend to be the most ‘bandwidth constrained’ along the path.

ISSLOW services are only provided if both endpoints on the link support ISSLOW. This is determined during the PPP negotiation. Because of the unique characteristics of a point to point link with both endpoints supporting ISSLOW, traffic is automatically shaped. That is, incoming traffic will be TSpec conformant, and except for some special considerations for Guaranteed Service (below), the admission control function can make decisions based on local state: it does not need to coordinate with the network element on the other end of the link. As described in [5], Guaranteed Service should approximate the functionality of a leased line. Since ISSLOW runs over point to point links, when rate control and delay bounds are provided for individual flows, the link inherently acts like a leased circuit.

Thus, even for Guaranteed Service, because this hop is the most bandwidth constrained, and because the connection is dual simplex (e.g., not a shared link for send & receive), all admission control decisions can be made locally.
3. Motivation

Previous sections described the motivation for the ISSLOW capabilities. Dial up users are now treating their relatively low-bitrate connections as they would a higher speed connection. They are mixing multiple flows of data and expect performance similar to what they see in a LAN environment. However, it is deployment of realtime applications which is the primary motivation for hosts to implement Integrated Services.

Realtime applications typically have tight delay constraints to achieve consistent performance, requiring small packets. When these are mixed with flows consisting of large packets (e.g. HTTP, FTP), delay variance increases and absolute delay suffers as these small packets wait in the queue behind even a single large packet being transmitted on the link. Because of the jitter tolerance and adaptive nature of many modern realtime applications, just providing a controlled load service would satisfy most of the needs of this class of applications.

Another consideration in handling of packets over low speed links occurs when looking at the end-to-end issues. The low speed link is usually just one hop on a longer path between endpoints. As such, it is usually the limiting factor in performance. While this needs to be considered in the host to router configuration, it becomes more critical between edge devices and backbone routers where there is a multiuser subnet as source and destination for traffic and a low-bitrate link to the router. To ensure some performance bounds end-to-end, guaranteed service should be considered over these links even if it cannot be offered end to end in the network.

4. Network Element Data Handling Requirements

The ISSLOW Network Service element may be implemented in hardware or software. As described in [1] and [2], for systems which can perform bit-oriented transmission control, the suspend/resume approach optimizes the available bandwidth by minimizing header overhead associated with MLPPP fragmentation. For systems which provide frame-oriented transmission control, the fragmentation approach can be implemented with no hardware changes. Choice of suspend/resume versus fragmentation should be made based on the hardware’s capability to handle the new HDLC framing described in [1] and the system overhead associated with byte by byte scanning (required by suspend/resume).

To provide controlled load or guaranteed service with the suspend/resume approach, when a packet for an IntServ admitted flow (QoS packet) arrives during transmission of a best effort packet and continued transmission of the best effort packet would violate delay constraints of the QoS service flows, the best effort packet is preempted, the QoS packet/fragments are added to the transmission, and the best effort packet transmission is then resumed: usually all in one transmission. The receiving station separates the best effort packet from the embedded QoS fragments. It is also conceivable that one IntServe Flow’s packet might suspend another flow’s packet if the delivery deadline of the new packet is earlier than the current packet.
For systems which use fragmentation, since suspend/resume is not possible, all packets longer than the maximum tolerable delay for an IntServ packet are fragmented prior to transmission so that a short packet for another flow can be interleaved between fragments of a large packet and still meet the transmission deadline for the IntServ flow.

Note that the fragmentation discussed in this document refers to multilink PPP (MLPPP) fragmentation and associated MCMLPPP modifications as described in [1], not IP or other layer 3 fragmentation. MLPPP fragmentation is local to the PPP link, and does not affect end-to-end (IP) MTU.

4.01 Rate and Delay

ISSLOW assumes that the nature of point to point links is such that rate, transmission time and delay are fixed and consistent. The rate of the link is determined at connection time, and the devices on the link (adapters, modems, DSU/CSUs, etc) exhibit fixed delay characteristics. Unfortunately this is not always true.

POTS modems can have varying rates, but the rate for a particular POTS modem connection tends to converge over time to a particular value as the modems adjust to line conditions. Implementations may need to adjust their admission control policies to reflect this convergence. Refer to Appendix A for more considerations on link characteristics and associated delay.

4.02 Link Aggregation

Although certain link types, like ISDN, permit dynamic allocation of Bandwidth across multiple links, it is assumed that the Admission Control service will consider the impact of multiple physical links over the point to point logical connection.

Note that because of the load balancing effect of Multilink PPP (MLPPP), two 64 Kbps links should exhibit the delay and transmission characteristics of a single 128 Kbps link. However, MLPPP implementations may approach load balancing and fragmentation differently. The mechanism used should be taken into consideration when implementing the scheduler (especially token bucket) for packets, fragments, and suspend/resume on top of existing MLPPP services to ensure that adequate rate and delay characteristics are maintained.

4.1 Controlled Load versus Guaranteed Service

With most link layers, Guaranteed Service requires more tightly controlled service by the Network Element, and in most cases, acceptance of a Guaranteed Service request results in over-provisioning of link level resources. Controlled Load (CL) Service is usually less constrained and permits more flexibility in scheduling of packets for the link.
Controlled Load requires that the delay associated with packet transmission be ‘closely equivalent to unloaded best effort service.’ Because ISSLOW operates over point to point links, unloaded best effort service means that best effort packets will incur no more than burst packet delay: \( M/r \) where \( M \) is the maximum packet size and \( r \) is the transmission rate. Thus maximum permitted delay for a Controlled Load packet \((\text{CLmDELAY})\) is bounded by \( M/r + P/r \) where \( P \) is the size of the outgoing packet.

4.2 Controlled Load and Guaranteed Service Data Handling

Upon arrival of a QoS flow’s packet, the ISSLOW Network Element determines if the packet is conformant. If it is not, Policing is applied (see Policing). Conformant means:

1) The flow does not exceed the associated TSpec peak rate (RSpec rate for Guaranteed Service: \( rT+b \) with \( T=\)time period).
2) The packet does not cause a token bucket overflow.

If the packet is conformant, it is compressed as required, fragmented (if necessary), and scheduled. If there is no conflicting best effort traffic, the packet is queued along with the rest of conformant QoS traffic and scheduled with respect to any other IntServ flows such that its transmission deadline is met.

For the suspend/resume implementation to achieve controlled load, any packets being transmitted whose transmission would violate the CLmDELAY are suspended. Otherwise, the QoS packet/fragments are scheduled ahead of any queued best effort traffic.

For CL Fragmentation implementations, the packet/fragment is scheduled ahead of any best effort packets. Note that all best effort packets must be divided into fragments less than or equal to the smallest MRU (or associated fragment size) of all the QoS flows. This incurs at most one fragment delay for the QoS traffic: closely equivalent to unloaded best effort service.

For Guaranteed Service for both fragmentation and suspend/resume, the scheduler determines if continued transmission of the best effort packet being transmitted would cause delay greater than the acceptable delay. If so, the best effort packet is preempted or, in the case of fragmentation, the QoS packet is scheduled ahead of the rest of the best effort packets’ fragments.
4.3 Controlled Load and Guaranteed Service Class Mappings

Supporting integrated services over PPP links which implement MCML or RTF can be accomplished in several ways. Guidelines for mapping these services to PPP links are presented below. Note that these guidelines assume that some sort of signaling is used to indicate desired quality of service to both the sender and receiver of a flow over a PPP link. These guidelines also assume that it is unlikely that a series of PPP links be connected to each other. It is noted that even if a series of PPP links were to be connected together, it is likely that each link would have different characteristics, and further, that frames would have to be reassembled at the terminus of each link for error correction purposes, requiring that class assignment be performed on each hop of the link, rather than just forwarding frames with identical segmentation or fragmentation. These assumptions remove any requirement on the service-mapping implementation that quality of service information be implicit in the class selection applied to particular flows, allowing the sender of an integrated services flow on a PPP link complete freedom in assigning classes to flows (or packets within flows).

One important observation that must be made is that the classes that MCML and RTF provide can be viewed purely as PPP-specific segmentation/fragmentation mechanisms. That is, while the class number must remain constant on an intra-packet basis, it may vary on an inter-packet basis for all flows transiting a PPP link. Actual assignment of particular flows to fixed classes is unnecessary, as the class numbers are not required to have any meaning other than in the context of identifying the membership of fragments/segments as part of a single packet. This consideration is very important, in that it offers implementers with a large degree of flexibility in providing integrated services over PPP links. This observation implies that the queuing discipline used to differentiate different flows does not have any ties to the class numbers used. This point is sufficiently important that an example is provided below.

Consider a PPP link using the MCML short sequence number fragment format (that is, four classes are provided). Assume that in addition to carrying best effort traffic, this link is carrying four guaranteed service flows, A, B, C, D, and E. Further assume that the link capacity is 100kbit/s and the latency is 100ms. Finally, assume the BE traffic is sufficient to keep the pipe full at all times and that GS flows A-E are each 10kbit/s and all have delay bounds of 145ms.

<table>
<thead>
<tr>
<th>Time (ms)</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>BE traffic is queued up</td>
</tr>
</tbody>
</table>
| 0         | 2kbit fragment from 10kbit packet of BE traffic sent, cls 0 (…)
| 8         | 2kbit fragment from BE sent, cls 0 (10kbit BE packet done) |
| 9         | 8kbit packet from flow A arrives |
| 10        | 2kbit fragment from A sent, cls 1 (8kbit flow A packet start) |
| 11        | 8kbit packet from flow B arrives |
This example shows several things. First, multiple flows may share the same class, particularly in the case where there are more flows than classes. More importantly, there is no reason that a particular flow must be assigned to a fixed class – the only requirement is that a each packet, when fragmented, must have the same class value assigned to all fragments.

One suggestion to implementers of integrated services on MCML and RTF links is that all BE and non-conformant traffic be logically separated from conformant traffic, and mapped to a fragmentable (MCML classes 0-3 in short sequence number fragment format, 0-15 in long sequence number fragment format) or suspendable (RTF classes 0-6) class. Since BE and non-conformant traffic will in most implementations not be scheduled for transmission except when a link is empty (that is, no CL or GS traffic is ready for transmission), it is possible to recommend use of class number 0 for BE/non-conformant traffic. Whether BE and non-conformant traffic are treated differently in regards to transmission (e.g., BE is given priority access over non-conformant traffic to the link) or whether within each type of traffic special treatment is afforded to individual flows (e.g., WFQ, RED, etc.) is implementation dependent.

In the case where fewer reservations are expected than the total number of classes negotiated for a PPP link, it is possible to assign individual flows to fixed class numbers. This assignment is useful in the case where the protocol identifier associated with one or more flows is known at LCP negotiation time and the bandwidth of the connection is relatively small. If these conditions hold true, then for those flows that are known, a specific class can optionally be assigned to them and the prefix elision PPP option can be used for those classes to achieve a small bandwidth savings.
5. Invocation Information

To invoke Controlled Load and Guaranteed Services, both traffic characteristics and the flow itself must be identified to the Network Element. Several methods can be employed to identify the flows. For RSVP, filtering can be used to identify the flows. For non-RSVP implementations, mechanisms such as the FlowID field in IP Version 6, or the TOS field in IP version 4 can be used. As described above, the Network Element can then use the specified values to apply the appropriate QoS and to map the flows to a particular class.

A number of major router and switch vendors currently support use of the TOS bits to signal priority and class of service. As a result, applications and host proxies have been developed to enable users and network managers to apply policies requesting differential services via TOS. Use of these bits is the easiest way to identify flows without the overhead of filtering.

If the Network Service Element is running on a system that doesn’t support application or proxy use of the TOS or FlowID fields, then filtering must be applied and:

As described in [4], Controlled Load Service is invoked by specifying the flow’s traffic characteristics through a TSpec (see [5]).

As described in [5], Guaranteed Service is invoked by specifying the flow’s TSpec and a requested reservation via an RSpec (see [6]).

6. Exported Information.

For Controlled Load Service, there is no requirement to export information.

For Guaranteed service, both C and D terms for delay computations must be made available for export through the Adspec or other means. See Sections 9.1 (Admission Control) for guidelines on computing the C and D terms.


7. Policing

Policing is applied to non-conformant QoS traffic and to best effort traffic whose transmission would violate the Controlled Load or Guaranteed Service constraints. This document does not designate a specific packet scheduling implementation. Ideally, best effort traffic can be serviced through separate queues and a weighted queuing mechanism, or when a conflict with QoS traffic arises, best-efforts traffic can simply be discarded.

Both Controlled Load and Guaranteed Services permit scheduling of non-conformant traffic as well as the option to discard non-conformant packets. See [4] and [5] for additional information on policing options for Controlled Load and Guaranteed Services.
8. Ordering and Merging


9. Guidelines for Implementors

9.1. PPP Bit Stuffing and Byte Stuffing Effects on Admission Control

An important consideration in performing admission control for PPP links is reductions in effective link rate due to bit stuffing. Typical bit stuffing algorithms can result in as much as 20% additional overhead. Thus, admission control implementations for guaranteed service over links where bit stuffing is used should take the RSpec rate of all flows and multiply by 1.2 in determining whether a new flow can be admitted or not. Admission control implementations for controlled load reservations may use a similar algorithm using the TSpec peak rate or may attempt to measure the actual degree of expansion occurring on a link due to bit stuffing. This characterization can then be used to adjust the calculated remaining link capacity. Such measurements must be used cautiously, in that the degree of bit stuffing that occurs may vary significantly, both in an inter- and intra-flow fashion.

Byte stuffing is also used on many PPP links, most frequently on POTS modems when using the v.42 protocol. Byte stuffing poses a difficult problem to admission control, particularly in the case of guaranteed service, due to its highly variable nature. In the worse case, byte stuffing can result in a doubling of frame sizes. As a consequence, a strict implementation of admission control for guaranteed load on byte stuffed PPP links should double the RSpec of link traffic in making flow admission decisions. As with bit stuffing, implementations of controlled load service admission control algorithms for links with byte stuffing may attempt to determine average packet expansion via observation or may use the theoretical worst case values.

9.2 Compression Considerations

The ISSLOW specification supports several PPP options. When deciding whether to admit a flow, Admission Control must compute the impact of the following on MTU size, rate, and fragment size:

Header compression: Van Jacobson or Casner-Jacobsen.
Prefix Elision.
CCP.
CRTP.
Fragment header option used.
Fragmentation versus suspend/resume approach.

If any of the compression options are implemented for the connection, the actual transmission rate, and thus the bandwidth required of the link, will be reduced by the compression method(s) used.
Prefix elision can take advantage of mapping flows to MLPPP classes to elide prefixes which cannot be compressed at higher layers. By establishing agreement across the link, the sender may elide a prefix for a certain class of traffic and upon receiving packets in that class, the receiver can restore the prefix.

Both compression gain and elision gain must be included as described in the admission control section below.

### 9.3 Admission Control

Admission Control must decide whether to admit a flow based on rate and delay. Assume the following:

- **LinkRate** is the rate of the link.
- **MTU** is the maximum transmission unit from a protocol.
- **MRU** is the maximum receive unit for a particular link.
- **CMTU** is the maximum size of the MTU after compression is applied.
- **eMTU** is the maximum effective size of the MTU after fragmentation.
- **FRAG** is the fragment size including MLPPP header/trailers.
- **Header** is the size of the header/trailers/fragments for MLPPP/Fragments.
- **pHeader** is the additional header/framing overhead associated with suspend/resume. This should include FSE and worst case stuffing overhead.
- **pDelay** is the delay associated with suspend/resume packets.
- **b** is the bucket depth in bytes
- **R** is the requested Rate.
- **D** is the fixed overhead delay for the link (Modem, DSU, etc).
- **C** is the delay associated with transmission and fragmentation.
- **eRate** is the effective rate after compression and fragmentation.

The D term may be configured by an administrative tool once the network is installed; it may be computed using the Adspec or other realtime measurement means; or it may be available from hardware during link setup and/or PPP negotiation. Refer to Appendix A for more considerations on PPP link characteristics and delays.

Admission Control must compute CMTU, eMTU, and eRate for Controlled Load Service, and it must compute CMTU, eMTU, eRate, and C for Guaranteed Service:

To determine whether the requested rate is available, Admission Control must compute the effective rate of the request (eRate) - worst case - as follows:

\[
\text{*_of_Fragments} = \frac{\text{CMTU} + \text{FRAG}}{\text{FRAG-Header}}
\]

\[
\text{eMTU} = \left(\text{*_of_Fragments}\right) \times \text{FRAG}
\]

\[
\text{eRate} = \frac{\text{eMTU}}{\text{CMTU}} \times \text{R}
\]

Admission Control should compare the eRate of the request against the remaining bandwidth available to determine if the requested rate can be delivered.
For Controlled Load Service, a flow can be admitted as long as there is sufficient bandwidth available (after the above computation) to meet the rate requirement, and if there is sufficient buffer space (sum of the token bucket sizes does not exceed the buffer capacity). While some statistical multiplexing could be done in computing admissibility, the nature of the low-bitrate links could make this approach risky as any delay incurred to address a temporary overcommitment could be difficult to amortize.

Guaranteed Service requires delay computations. These computation are based on the standard formula for delay:

\[
\text{Delay} = b/R + C/R + D
\]

Note that for suspend/resume, an additional term is required:

\[
\text{pDelay} = b/R + C/R + D + p\text{Header}/R.
\]

This term exists because of the additional overhead associated with the suspend/resume headers created when suspending a packet. In the worse case, every transmission of a QoS packet could require suspension of a best effort packet and thus incur the overhead. In most networks, this term will be nominal at most. However, on some low-bitrate links, the overhead may be worth computing.

Since MLPPP includes fragmentation, the C term is not fixed and must be represented by the worse case fragmentation as computed in the effective MTU size:

\[
C = e\text{MTU}.
\]

Note that because ISSLOW runs on point to point links, Guaranteed Service can be offered over a link without any negotiated agreement from the next hop. However, if these services are used in conjunction with RSVP, the C and D values above should be used in the Adspec.

### 9.4 Fragment Scheduling Considerations

As described in Section 4, large packets should be fragmented to a size sufficiently small to allow higher priority flows to get a hold of the line quickly enough to not violate their reservation constraints. As such, the upper bound for fragment sizes should be no larger than the smallest MTU of all QoS flows. While a very small fragment size is desirable from the point of view of efficient link utilization, the overhead associated with highly granular fragmentation makes it necessary to strike a balance between these considerations. While this document will not specify a particular scheduling algorithm, the following example should help illustrate the issue:
Assume we have three different priority flows, A, B, and C. Packets from flow C take 100ms, flow B takes 30ms, and flow A takes 30ms to transmit. B’s required maximum latency is 70ms, while A’s is 50ms. The above scenario results in flows B and C needing to be segmented into 20ms long fragments — that way a lower priority frame will hold the link at most 20ms before A gets to the link, taking another 30ms to transmit, totaling 50ms — all well and good. B has a problem, however — in the scenario where a fragment from C is just starting to transmit the link when packets from A and B arrive (call this time 0). The fragment from C will transmit until time 20ms. After that, the A packet will transmit — finishing by time 50ms, just in time. At this point, the fragment from B starts to transmit — taking 30ms more, finishing by time 80ms (thus violating its reservation).

The important point above the scenario is not that it is possible to overcommit a link, but that a link can be underutilized by using too large a fragment size — in the above case, a 10ms fragment size would have allowed both A and B to honor their reservations, a 20ms size does not.

10. Evaluation Criteria

For Controlled Load Service, the ISSLOW network element must ensure that the service requested via the TSpec is delivered to the requesting QoS flow such that the PPP link appears to be a ‘lightly loaded link.

As a baseline, it is suggested that performance measurements on throughput, delay, and packet error measurements be performed on an unloaded link with just the QoS flow using various packet sizes. The baseline should measure performance for both conformant and non-conformant traffic when overloading the link with a single flow. Once these measurements are complete, measurements of the Controlled Load Service should be performed as follows:

1) Request QoS flows in the presence of best effort traffic and ensure that the QoS flows’ performance approximate the unloaded baseline measurements.

2) Request QoS flows whose aggregate throughput would exceed the link capacity. Admission Control should deny these service requests or admit them as best effort only.

3) Generate traffic on a QoS flow which exceeds its TSpec commitment. Ensure recovery of the flow once the traffic becomes conformant.

For Guaranteed Service:

1) Ensure that Admission Control will deny service requests or convert them to best effort when link capacity or delay bounds would be exceeded.
2) On a best-efforts loaded link, ensure that the number of lost packets does not exceed those established in the baseline measurements.

3) On a best-efforts loaded link, ensure that delay and rate commitments can be met for QoS flows.

4) With multiple QoS flows, ensure that an admission of additional QoS flows does not cause a violation in rate, error rate, or delay constraints of any QoS flow.

11. Security Considerations

General security considerations for PPP links are addressed elsewhere. A specific security consideration relevant to providing quality of service over PPP links appears when relying on either observed or theoretical average packet expansion during admission control due to bit- or byte-stuffing. Implementations based on these packet-expansion values contain a potential vulnerability to denial of service attacks. An adversary could intentionally send traffic that will result in worst case bit- or byte-stuffing packet expansion. This in turn could result in quality of service guarantees not being met for other flows due to overly permission admission control. This potential denial of service attack argues strongly for using a worst case expansion factor in admission control calculations, even for controlled load service.

12. References


Appendix A: Admission Control Considerations for POTS Modems

The protocols used in current implementations of POTS modems can exhibit significant changes in link rate and delay over the duration of a connection. Admission control and link scheduling algorithms used with these devices must be prepared to compensate for this variability in order to provide a robust implementation of integrated services.

Link rate on POTS modems is typically reported at connection time. This value may change over the duration of the connection. The v.34 protocol, used in most POTS modems, is adaptive to link conditions, and is able to recalibrate transmission rate multiple times over the duration of a connection. Typically this will result in a small (~10%) increase in transmission rate over the initial connection within the first minute of a call. It is important to note, however, that other results are possible as well, including decreases in available bandwidth. Admission control algorithms must take such changes into consideration as they occur, and implementations must be able to gracefully handle the pathological case where link rate actually drops below the currently reserved capacity of a link.

Delay experienced by traffic over POTS modems can vary significantly over time. Unlike link rate, the delay often does not converge to a stable value. The v.42 protocol is used in most POTS modems to provide link-layer reliability. This reliability, which is implemented via retransmission, can cause frames to experience significant delays. Retransmissions also implicitly steal link bandwidth from other traffic. These delays and reductions in link bandwidth make it extremely difficult to honor a guaranteed service reservation. On a
link that is actually lightly or moderately loaded, a controlled load service can to some extent accept such events as part of the behavior of a lightly loaded link. Unfortunately, as actual link utilization increases, v.42 retransmissions have the potential of stealing larger and larger fractions of available link bandwidth; making even controlled load service difficult to offer at high link utilization when retransmissions occur.