Abstract

This document describes a framework for Pseudo Wires Emulation Edge-to-Edge (PWE3). It discusses the emulation of circuits (such as T1, E1, T3 and E3) and services (such as ATM and Frame relay) over packet networks using IP, L2TP or MPLS for transport. It presents an architectural framework for pseudo wires, defines terminology, specifies the various protocol elements and their functions, overviews some of the services that will be supported and discusses how pseudo wires fit into the broader context of protocols.
# Introduction

1.1 What Are Pseudo Wires? .................................
1.1.1 Definition ...........................................
1.1.2 Functions ............................................
1.2 Goals of This Document ...................................
1.3 Non-Goals .............................................

# Background and Motivation

2.1 Current Network Architecture ..........................
2.1.1 Multiple Networks ..................................
2.1.2 Convergence Today ..................................
2.2 The Emerging Converged Network ......................
2.3 Transition to the New Network .........................

# Architecture of Pseudo Wires

3.1 Reference Model ........................................
3.2 Terminology ...........................................
3.3 Architecture Assumptions .............................
3.4 Comparison of Relevant Applications ..................

# Layer 1 (Circuit) Applications

4.1 Reference Model ........................................
4.2 Operational Considerations ...........................
4.2.1 Transparency .........................................
4.2.2 Framed Versus Unframed Mode For TDM Circuits ... 
4.2.3 Fractional T1/E1 ......................................
4.2.4 Loopbacks ............................................
4.2.5 Performance Processing ..............................
4.2.6 LOS/LOF/AIS/RAI .....................................
4.2.7 SONET/SDH STS Unequipped .........................
4.3 Encapsulations .........................................
4.3.1 Criteria ................................................
4.3.2 SONET Encapsulation ................................
4.3.2.1 SPE ............................................... 
4.3.2.2 Section/Line ......................................
4.3.2.3 VT ................................................
4.3.3 ATM AAL1 Encapsulation ............................
5.1 Layer 2 PW Reference Model ...........................

# Layer 2 (Packet/Cell) Applications

5.2 Ethernet ................................................
5.2.1 Reference Model Scope ..............................
5.2.2 Operational Considerations ........................
5.2.2.1 Operational Modes ................................
5.2.2.2 Quality Of Service Support Considerations ....
5.3 Frame Relay ............................................
5.3.1 Reference Model ......................................
5.3.2 Operational Considerations ........................
5.3.2.1 Frame Sequence ...................................
5.3.2.2 Frame Size ........................................
5.3.2.3 End-to-end Transport Characteristics .......... 
5.3.2.4 Connection Management and Congestion Control 
5.3.2.5 Link Management Support .........................
5.3.2.6 DLCI Association .................................
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.7 ANSI</td>
<td>42</td>
</tr>
<tr>
<td>11.8 Telcordia</td>
<td>42</td>
</tr>
<tr>
<td>12 Security Considerations</td>
<td>42</td>
</tr>
<tr>
<td>13 Authors’ Addresses</td>
<td>42</td>
</tr>
<tr>
<td>14 Full Copyright Section</td>
<td>43</td>
</tr>
</tbody>
</table>
1. Introduction

This document describes a framework for Pseudo Wires Emulation Edge-to-Edge (PWE3). It discusses the emulation of circuits (such as T1, E1, T3 and E3) and services (such as ATM and Frame relay) over packet networks using IP, L2TP or MPLS for transport. It presents an architectural framework for pseudo wires, defines terminology, specifies the various protocol elements and their functions, overviews the services supported and discusses how pseudo wires fit into the broader context of protocols.

1.1. What Are Pseudo Wires?

1.1.1. Definition

A pseudo wire (PW) is a mechanism that emulates the essential attributes of a service (such as a T1 leased line or Frame Relay) over a packet network. The required functions of PWs include encapsulating service-specific bit-streams or PDUs arriving at an ingress port, and carrying them across a path or tunnel, managing their timing and order, and any other operations required to emulate the behavior and characteristics of the service as faithfully as possible.

From the customer perspective, the PW is perceived as an unshared link or circuit of the chosen service. However, there may be deficiencies that impede some applications from being carried on a PW. These limitations should be fully described in the appropriate service-specific Applicability Statements (ASes).

1.1.2. Functions

PWs provide the following functions in order to emulate the behavior and characteristics of the desired service.

- Encapsulation of service-specific PDUs or circuit data arriving at an ingress port (logical or physical).

- Transporting the encapsulated data across a tunnel.

- Managing the signaling, timing, order or other aspects of the service at the boundaries of the PW.

ASes for each service will describe any shortfalls of the emulation’s faithfulness.
1.2. Goals of This Document

- Description of the motivation for creating PWs, and some background on how they may be deployed.

- Description of an architecture and terminology for PWs.

- Description of the relevant services that will be supported by PWs, including any relevant service-specific considerations.

- Description of methods to ensure in-order final PDU delivery.

- Description of methods to perform clock recovery, as needed or appropriate.

- Description of methods to perform edge-to-edge/inband signaling functions across the transport network as needed or appropriate.

- Description of the statistics and other network management information needed for tunnel operation and management.

- Description of the security mechanisms to be used to protect the control of the PW technology. The protection of the encapsulated content (e.g., payload encryption) of the PW is outside of scope.

- Description of a mechanism to exchange encapsulation control information at an administrative boundary of the transport network, including security methods.

- Whenever possible, relevant requirements from existing IETF documents and other sources will be incorporated by reference.

1.3. Non-Goals

The following are out of scope:

- The protection of the encapsulated content of the PW.

- Any multicast service not native to the emulated medium. Thus, Ethernet transmission to a "multicast" IEEE-48 address is in scope, while multicast services like MARS that are implemented on top of the medium are out of scope.

- Methods to signal the underlying network
2. Background and Motivation

Many of today’s service providers are struggling with the dilemma of moving to an optical network based on IP and/or MPLS. How do they realize the capital and operational benefits of a new packet-based optical infrastructure, while leveraging the existing base of SONET (Synchronous Optical Network) gear, and while also protecting the large revenue stream associated with this equipment? How do they move from mature Frame Relay or ATM networks, while still being able to provide these lucrative services? One possibility is the emulation of circuits or services, currently referred to as "pseudo wires" in the IETF. Circuit emulation over ATM and interworking of Frame Relay and ATM have already been standardized. Emulation allows the transport of existing circuits and/or services across the new infrastructure, and thus enables the interworking of disparate networks. [ATMCES] provides some insight into the requirements for such a service:

There is a user demand for carrying certain types of constant bit rate (CBR) or "circuit" traffic over Asynchronous Transfer Mode (ATM) networks. As ATM is essentially a packet- rather than circuit-oriented transmission technology, it must emulate circuit characteristics in order to provide good support for CBR traffic.

A critical attribute of a Circuit Emulation Service (CES) is that the performance realized over ATM should be comparable to that experienced with the current PDH/SDH technology.

Section 4 of [ANAVI] gives more background on why such emulation is desirable:

The simplicity of TDMoIP translates into initial expenditure and operational cost benefits. In addition, due to its transparency TDMoIP can support mixed voice, data and video services. It is transparent to both protocols and signaling, irrespective of whether they are standards based or proprietary with full timing support and the capability of maintaining the integrity of framed and unframed DS1 formats.

2.1. Current Network Architecture

2.1.1. Multiple Networks

The current "network" for any given service provider delivering multiple services usually consists of parallel networks. Each of these networks implements a specific service, such as voice, Frame Relay, internet access, etc. This is quite expensive, both in terms of capital expense as well as in operational costs. Furthermore,
multiple networks complicates planning. Service providers wind up asking themselves these questions:

- Which network do I build out?
- How many fibers do I need for each network?
- How do I efficiently manage multiple networks?

2.1.2. Convergence Today

There are some examples of convergence in today’s network:

- Frame Relay is frequently carried over ATM networks using \([\text{FRF.5}]\) interworking.
- T1, E1 and T3 circuits are sometimes carried over ATM networks using \([\text{ATMCES}]\).
- Voice is carried over Frame Relay and IP networks.

Deployment of these examples range from limited (ATM CES) to fairly common (FRF.5 interworking) to widespread (VoIP).

2.2. The Emerging Converged Network

Many service providers are finding that the new IP-based and MPLS-based switching systems are much less costly to acquire, deploy and maintain than the systems that they replace. The new systems take advantage of advances in technology in these ways:

- The newer systems leverage mass production of ASICs and optical interfaces to reduce capital expense.
- The bulk of the traffic in the network today originates from packet sources. Packet switches can economically switch and transport this traffic natively.
- Variable-length switches have lower system costs than ATM due to simpler switching mechanisms as well as elimination of segmentation and reassembly (SAR) at the edges of the network.
- Deployment of services is simpler due to the connectionless nature of IP services or the rapid provisioning of MPLS applications.
2.3. Transition to the New Network

The emergence of a converged network solves many of the problems faced by service providers, but the old networks and services don’t just go away. Use of PWs can help facilitate this transition with these benefits.

- Leverage the low capital and operational expenses of packet networks.
- Simple provisioning.
- Provide a transition path to a converged network.

Editor’s Note: this section needs more work.
3. Architecture of Pseudo Wires

3.1. Reference Model

Figure 1 below shows the reference model for PWs.

```
|<---------- pseudo wire ----->|
|                            |
| service                    |
| +-------+ access +-------+ |
| |PW-PDU| -> service |
| +-------+ access +-------+ |
|         | PWE1 | ............... | PWE2 | ------- |
| SE1 | --------| SE2 |
| +-----+ access +-----+     +-----+ access +-----+
PW endpoint 1               PW endpoint 2

<---------------- emulated service ---------------->
```

Figure 1: PW Reference Model

As shown, the PW provides an emulated service between the service endpoints. Any bits or packets presented at the service access are encapsulated in a PW PDU and carried across the underlying network. The PW endpoints (PWE) perform the encapsulation, decapsulation, order management, timing and any other functions required by the service. The underlying transport network is not involved in any of these service-specific operations.

3.2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALLNOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119. Below are the definitions for the terms used throughout the document.

Pseudo Wire
The Pseudo Wire (PW) is a mechanism that emulates the essential attributes of a service, providing this emulation over a packet network.

Pseudo Wire Domain
A PW Domain (PWD) is a collection of instances of PWs that are within the scope of a single homogenous administrative domain (e.g. PW over MPLS network or PW over IP network etc.).

Pseudo Wire Endpoint
The PW Endpoint (PWE) is a device that provides the adaptation between the end service and the PW.
Pseudo Wire PDU  The PW-PDU is a PDU sent on the PW that contains all of the data and control information necessary to provide the desired service.

Service Endpoint  The Service Endpoint (SE) is the point of termination for the emulated service.

Network Interworking  Network Interworking means that the ingress and egress of the PW interfaces are identical (e.g. ATM-to-ATM, Frame Relay-to-Frame Relay etc.). The interworking function (IWF) at the edge of the PW performs the service mapping (e.g. ATM Cell Loss priority (CLP) maps to EXP field in MPLS header) on the service data unit (SDU) (e.g. ATM cell) to ensure the service transparency while transporting the SDU data transparently across the PWD.

Service Interworking  Service Interworking means that the ingress and egress of the PW interfaces are different (e.g. ATM-to-Frame Relay). The interworking function at the ingress edge of the network terminates the SDU transport (e.g. ATM AAL5 PDU transport) and performs service mapping between the ingress SDU and the pseudo-wire PDU (e.g. ATM CLP to MPLS EXP) while it is converting the incoming SDU into the PW SDU (e.g. transcoding ATM AAL5 PDU into MPLS PDU) and transports converted PDU across the PWD. The same operation may be repeated in the reverse order at the egress PW if the outgoing interface does not have the same SDU type as the PW.

Applicability Statement  Each PW service will have an Applicability Statement (AS) that describes the particulars of PWs for that service, as well as the degree of faithfulness to that service.

3.3. Architecture Assumptions

1) The current design is focused on a point-to-point and same-to-same service interface at both end of the PW. Only network interworking will be performed at the edge or the PW. Support for service interworking is for further study.

2) The initial design of PWE3 is focused on a single homogenous administrative PWD (e.g. PW over MPLS or PW over IP etc. ONLY). Interworking between different pseudo-wire types and the support of inter-domain PWs are for further study.
3) The design of PW will not perfectly emulate the characteristics of the native service. It shall be dependent on both the emulated service, as well as on the network implementation. An AS shall be created for each service to describe the degree of faithfulness of a PW to the native service.

4) Only the permanent emulated circuit type (e.g. PVC/PVP) is considered initially. The switched emulated circuit type (e.g. SVC/SVP) will be for further study.

5) The creation and placement of the tunnel to support the PW is not within the scope.

6) The current PW encapsulation approach considerations are focused on IPv4, IPv6, L2TP, GRE and MPLS. Other encapsulation approach is for further study.

7) Current PW service applications are focused on Ethernet (i.e. Ethernet II (DIX), 802.3 "raw", Ethernet 802.2, Ethernet SNAP, 802.3ac VLAN), Frame Relay, ATM, TDM (e.g. DS1, DS3, T1, SONET etc.) and MPLS.

8) Within the single administrative PWD, the design of the PW assumes the inheritance of the security mechanism that has been applied to the emulated services. No PW specific security mechanism will be specified.
3.4. Comparison of Relevant Applications

When considering PWs as a means of providing a service, the following questions must be asked:

- Preservation of Order - Does the application require in-order delivery of data?
- Preservation of Timing - Does the application require fine-grain preservation of timing?
- Natural Delineation - What is the "natural" boundary for delineation of data for encapsulation?
- Packet Size - Are the encapsulated packets variable or fixed in size?
- Data Rate - Is the data rate presented at the interface fixed or variable?

Figure 2 below shows a summary of the applications relevant to pseudo wire transport, along with a comparison of their attributes.

<table>
<thead>
<tr>
<th></th>
<th>Preserve Order</th>
<th>Preserve Timing</th>
<th>&quot;Natural&quot; Delineation</th>
<th>Packet Size</th>
<th>Data Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>TDM Circuits</td>
<td>yes</td>
<td>yes</td>
<td>125 us frame</td>
<td>fixed</td>
<td>fixed</td>
</tr>
<tr>
<td>SONET Circuits</td>
<td>yes</td>
<td>yes</td>
<td>125 us frame</td>
<td>fixed</td>
<td>fixed</td>
</tr>
<tr>
<td>Frame Relay</td>
<td>yes</td>
<td>no</td>
<td>frame</td>
<td>Variable</td>
<td>Variable</td>
</tr>
<tr>
<td>ATM AAL1</td>
<td>yes</td>
<td>no</td>
<td>cell</td>
<td>fixed</td>
<td>fixed</td>
</tr>
<tr>
<td>ATM AAL2</td>
<td>yes</td>
<td>no</td>
<td>cell</td>
<td>fixed</td>
<td>variable</td>
</tr>
<tr>
<td>ATM AAL5</td>
<td>yes</td>
<td>no</td>
<td>cell or PDU</td>
<td>variable</td>
<td>variable</td>
</tr>
<tr>
<td>Ethernet</td>
<td>yes</td>
<td>no</td>
<td>frame</td>
<td>variable</td>
<td>variable</td>
</tr>
</tbody>
</table>

Figure 2: Summary of Applications and Attributes
4. Layer 1 (Circuit) Applications

For these applications the entire bit stream needs to be transported to the far end. As with SONET transport or ATM CES, the physical layer coding is terminated and re-generated on the far end. In addition, framing may be terminated and regenerated, depending on the application.

4.1. Reference Model

Figure 3 below shows a pair of T1s being carried over a TDM/SONET network. The node marked "M" is an M13 multiplexer, while the nodes marked "S" are SONET Add-Drop Multiplexers (ADMs).

Figure 3: T1/SONET Example Diagram

Figure 4 below shows the same pair of T1s being carried over a packet network. Here the emulation is performed by the boxes marked "E", and the routers marked "R" carry the resulting packets. Note that the emulation, routing and/or SONET functions could be combined in the same device.
4.2. Operational Considerations

4.2.1. Transparency

Circuits such as T1/E1/T3/E3 lines need a greater degree of transparency than Layer 2 services. These circuits may be carrying the services described in the section on Layer 2 services, but in the Layer 1 scenario the higher layer application is irrelevant and is ignored. In general, these are "bits in, bits out" applications.

In this application a circuit or bit stream is encapsulated in fixed-size frames that are sent at a fixed rate. The emulated stream must be delivered in a reliable and predictable fashion to the far end. Absolute delay and delay variation (also called jitter or wander) must be minimized.

This encapsulation of TDM data must be transparent. The emulated circuit could be carrying one or more types of data (ATM, Frame Relay, TCP/IP, etc.), voice traffic, video or anything else. The data is not interpreted; it is simply transported.

4.2.2. Framed Versus Unframed Mode For TDM Circuits

As discussed in [ATMCES], emulation of a T1, E1 or other circuit can be done in a framed mode or in an unframed mode. Framed mode requires the use of a framer to generate the outgoing framing pattern. More importantly, it is needed to detect a LOS condition or reception of an Alarm Indication Signal (AIS). A framer is also needed to generate and terminate the Facility Data Link (FDL) overhead channel used for communication of loopback commands and performance reports. The capabilities described in the rest of this section (except for LOS) are predicated on the presence of a framer.
4.2.3. Fractional T1/E1

A fractional T1 or E1 is composed of a number of concatenated DS0s and is sometimes referred to as NxDS0. It may be emulated by replicating the contents of the relevant DS0s at the other end of the tunnel. The value of the other timeslots and/or framing are irrelevant and are not transported in leased line application. Even though the framing is not transported, a framer is still needed to delineate the timeslots for encapsulation.

4.2.4. Loopbacks

It is desirable for a PWE node to process loopback messages as defined in [T1.403]. This would allow for isolation of faults in a network. It also facilitates the certification of equipment for operation in a carrier’s network.

There are also inband loopbacks that are used for voice equipment. These are falling out of favor due to their incompatibility with data services. A PWE device that implements inband loopbacks must have the capability to disable them.

4.2.5. Performance Processing

[T1.403] defines a Network Performance Report Message (NPRM) that carry periodic reports on the performance of the link. It is desirable for a PWE node to generate these messages, as they are frequently used for surveillance and trouble-shooting.

4.2.6. LOS/LOF/AIS/RAI

Figure 5 shows an example for the generation of AIS and RAI.

```
<-- Upstream    Downstream -->

LOS +-------+ AIS
------X-----+\   /|----->
|\ / |
|/ \|
<--------|--/ \|<--------
RAI+Data +-----+ Data
```

Figure 5: Generation of AIS and RAI

A TDM multiplexer, switch or other path-terminating device must respond to an LOS (Loss of Signal), LOF (Loss of Frame) or AIS (Alarm Indication Signal) condition (collectively known as "red alarms") by:

- Generating AIS in the "downstream" direction i.e. the same direction in which the LOS was detected. AIS is conveyed by sending a certain pattern in the data stream.
- Generating RAI (Remote Alarm Indication, also known as a "Yellow Alarm") in the "upstream" direction i.e. in the other direction. RAI is conveyed by sending a certain pattern in the framing. Note that RAI does not interfere with or suppress the payload data.

Bandwidth can be saved by suppressing the AIS signal in the emulated stream and sending instead an indication in the control overhead. This also applies to a received AIS signal. [MALIS] discusses the propagation of AIS using the pointer bits in the TDM control word.

A device emulating TDM circuit must either replicate the AIS indication or indicate this condition in the control overhead.

4.2.7. SONET/SDH STS Unequipped

The "STS Unequipped" indication may be treated in a fashion similar to that for LOS/AIS. Bandwidth can be saved by suppressing the payload in the emulated stream and sending instead an indication in the control overhead.
4.3. Encapsulations

4.3.1. Criteria

Encapsulation options for TDM services may be compared on the following criteria.

- Timing - TDM services are very sensitive to timing and timing variations ("jitter"). The encapsulation may need to provide additional information to help convey timing.

- Line Signals - The encapsulation should provide a means to convey signals such as AIS and line conditions such as LOF.

- The encapsulation should minimize overhead.

4.3.2. SONET Encapsulation

4.3.2.1. SPE

The format of the SPE (Synchronous Payload Envelope) for SONET is defined in [GR253]. This mapping is used in [MALIS] as the basis for the encapsulation format. The advantages of this approach include:

- It is defined for multiples of 50.112 Mbps.
- The structures and methods for synchronization are well defined.
- The line overhead is suppressed.
- The SPE can be extracted from the packet and fed into a SONET framer. This facilitates interworking with SONET systems, as shown in Figure 4.

The disadvantages include:

- There is no support for rates below STS-1.
- There is no support for rates other than multiples of 50.112 Mbps.

4.3.2.2. Section/Line

This is similar to an SPE, but the section and line overhead are preserved. The advantages of this approach include:

- It is completely transparent. Any compatibility issues go away.
- The interface equipment is very simple because no framer is required. The output of an optical transceiver can be fed directly into the packet generation function.
The disadvantages include:

- In SONET, the user data is carried in the SPE and/or VTs, which are path functions. By analogy, an emulation device should act like SONET gear that terminates a section or path. Transporting the section or path overhead seems to violate the spirit of the SONET path/line/section model.

4.3.2.3. VT

SONET VT mapping into an SPE is defined for T1, E1, E3 and T3. An example of VT1.5 mapping is shown in Figure 6 below, reproduced from [GR253].

```
  1  2  3  * * *  29  30  31  32  * * *  58  59  60  61  * * *  87
  +--+------------------+-+------------------+-+------------------+
  1 |J1|  Byte 1 (V1-V4) |R|   |   |      |   |R|   |   |      |   |
  +--+---+---+------+---+-+------------------+-+------------------+
  2 |B3|VT |   |      |   |R|   |   |      |   |R|   |   |      |   |
  +--+1.5|   |      |   +-+---+---+------+---+-+------------------+
  3 |C2|   |   |      |   |R|   |   |      |   |R|   |   |      |   |
  +--+   |   |      |   +-+---+---+------+---+-+------------------+
  4 |G1|   |   |      |   |R|   |   |      |   |R|   |   |      |   |
  +--+   |   |      |   +-+---+---+------+---+-+------------------+
  5 |F2|   |   |      |   |R|   |   |      |   |R|   |   |      |   |
  +--1-1|2-1| * * *|7-4|-|1-1|2-1| * * *|7-4|-|1-1|2-1| * * *|7-4|
  6 |H4|   |   |      |   |R|   |   |      |   |R|   |   |      |   |
  +--+   |   |      |   +-+---+---+------+---+-+------------------+
  7 |Z3|   |   |      |   |R|   |   |      |   |R|   |   |      |   |
  +--+   |   |      |   +-+---+---+------+---+-+------------------+
  8 |Z4|   |   |      |   |R|   |   |      |   |R|   |   |      |   |
  +--+   |   |      |   +-+---+---+------+---+-+------------------+
  9 |Z5|   |   |      |   |R|   |   |      |   |R|   |   |      |   |
  +--+---+---+------+---+-+---+---+------+---+-+------------------+
 arsenal                  +--------------------+-- Fixed Stuffs
```

Figure 6: SPE Mapping of VT1.5

The advantages of this approach include:

- This mapping is well defined.

- Commercial silicon is available to implement this function.

- This mapping is fairly efficient. It requires 27 bytes per VT1.5, which is an overhead of about 10%.

The disadvantages include:

- This mapping is inefficient for transport of a few circuits. The whole SPE must be sent, regardless of how many circuits are
provisioned.

4.3.3. ATM AAL1 Encapsulation

ATM AAL1/2 is the mapping defined in [I.363.1] and [I.363.2]. It is used in [ANAVI] as the basis for the encapsulation. The advantages of this approach include:

- ATM AAL1 is defined for T1, E1, E3 and T3.

- ATM cells are fairly small. This allows for a low capture delay and low queuing delay.

- ATM cells include SRTS timing information.

The disadvantages include:

- There is no definition for rates higher than T3. This means that a different encapsulation format would have to be used for STS-1 and higher rates.

- There are 5 bytes of overhead for each 48 bytes of payload. This can be overcome by removing the header at one end of the link and restoring it at the other.

- Telcordia asserts that its U.S. Patent No 5,260,978 for Synchronous Residual Timestamp (SRTS) Timing Recovery in a Broadband Network may apply to the ATM Adaptation Layer Type 1 (AAL1).
5. Layer 2 (Packet/Cell) Applications

5.1. Layer 2 PW Reference Model

Figure 7 below shows the reference model for Layer 2 PWs. The layer 2 emulated protocols/services include ATM VCC, ATM VPC, Frame Relay DLCI, IEEE 802.1Q VLAN, IEEE 802.3x link, etc. The nodes marked "S" are protocol-specific switches e.g. Frame Relay switches.

![Layer 2 Interconnect Reference Model](image)

Figure 7: Layer 2 Interconnect Reference Model

Figure 8 below shows the reference model for PW emulation of Layer 2 services.

![Layer 2 PW Emulation](image)

Figure 8: Layer 2 PW Emulation
5.2. Ethernet

5.2.1. Reference Model Scope

PW transport of Ethernet operates as a point-to-point trunking transport in a non-shared medium. The Ethernet interface can operate in a half-duplex or full-duplex mode. Control functions such as IEEE 802.3 Carrier Sense Multiple Access with Collision Detection (CSMA/CD) [802.3] and IEEE 802.1D Spanning Tree [802.1D] are not applicable nor within the scope of PWs. However, the PW shall conform to the service definitions as defined in IEEE 802.1P,Q [802.1Q], as required. Also, it shall support all Ethernet framing i.e. Ethernet Frame and IEEE 802.3x including IEEE 802.3ac VLAN Tagging [802.3ac] as well as Jumbo Frame.

5.2.2. Operational Considerations

5.2.2.1. Operational Modes

The design of the Ethernet PW must consider the support of the two operational modes in this framework:

Both modes shall be supported for all Ethernet interfaces, i.e. from 10 Mbps to 10,000 Mbps, and the design of the Ethernet PW functions shall be agnostic to the Ethernet’s link capacity.

Both modes shall support the transparent transport of the address resolution protocols, i.e. ARP, InverseARP, proxy ARP and Ethernet-based control protocol (e.g. Generic Attribute Registration Protocol (GARP), GARP VLAN Registration Protocol (GVRP) etc.).

- Ethernet Trunking - In this mode, the trunking access pays attention only to the MAC header’s port information or other MAC header information e.g. MAC address, protocol type etc. The processing rules, e.g. classification, filtering, shall be based on configurable policy.

- Virtual LAN (VLAN) Transport - In this mode, a link can carry the traffic of multiple VLANs through the tagging scheme as specified in [802.1Q]. The Ethernet PW shall carry multiple VLANs traffic and can extend VLANs across the PWD. Each frame received at the trunking access associated with a particular VLAN indicated by the given VLAN_ID. If the received frame is tagged with a NULL VLAN_ID, it will be associated with the VLAN equal to the Port’s default VLAN. At frame transmission, all frames that are sent in this mode shall be tagged except for those assigned for the default VLAN.

The PWE may provide translation of the VLAN_ID in order to facilitate deployment. Note that this does not increase the VLAN_ID space, so it has no effect on scalability.
5.2.2.2. Quality Of Service Support Considerations

The Ethernet AS shall describe the faithfulness of the PW with respect to these attributes described in IEEE 802.1p [802.1Q].

- Service Availability - Service availability is measured as ratio between MAC service is unavailable and available.

- Frame Loss - The MAC service does not provide guarantees delivery of service data units. However, the Ethernet PW system should consider monitoring frame loss.

- Frame Misorder - The MAC service does not permit reordering frames within the same user-priority for a source and destination address pair.

- Frame Duplication - The MAC service does not permit duplicating frames.

- Transit Delay Performance - IEEE 802.1p [802.1Q] defines frame transit delay is the elapsed time between an MA_UNITDATA.request and corresponding MA_UNITDATA.indication on a successful transfer.

- Undetected Frame Error Rate - By using the Frame Checksum (FCS) calculation for each frame, the undetected frame error rate should be low.

- Maximum Service Data Unit Size - The maximum service data unit size is dependent on the access media used. In general, it is the lowest common denominator of the two adjacent Ethernet interface.

- Priority Tags and Traffic Classes - IEEE 802.1p defines eight traffic classes (priority). These are ignored by the PWE.
5.3. Frame Relay

5.3.1. Reference Model

Frame Relay service offerings often have a different physical format and speed at each end of the link. For example, a hub and spoke deployment of Frame Relay might provide fractional T1 access at the spokes and a clear channel T3 to the hub. The Virtual Circuits (VCs) are aggregated by switches in the Frame Relay network. This is shown in figure 9 below, where the Frame Relay switches are marked with an "F".

Wide Area Frame Relay Network

```
+-----+     ++++
|Site A|-------/     |
|VC #1=|-----------------|F/
|      |----------
|      |          |
+------+Trans-
Atlantic E1

|VC #2=|-----------------|
|      |----------
|      |          |
+------+
```

Figure 9: Frame Relay Example Model

Figure 10 shows an emulated network, where Carrier "A" is providing a transparent Frame Relay emulation connection to Carrier "B". Here the emulation is performed by the boxes marked "E", and the resulting packets are carried by the routers marked "R". In this case, the emulated VCs can transparently carry the PVC status signaling (if any) and need not perform any higher layer function. Also, note that the emulation and routing functions could be combined in the same device.
If the Frame Relay switches are to be completely eliminated (as shown in figure 11 below), then the emulation service must implement Frame Relay PVC status signaling and/or signaling for SVCs. As previously noted, the emulation and routing functions could be combined in the same device.
5.3.2. Operational Considerations

Frame Relay provides a connection-oriented circuit-based transport. There are two types of virtual circuits supported in Frame Relay: Permanent Virtual Circuits (PVCs) and Switched Virtual Circuits (SVCs). The following sections describe the considerations to support the operation of Frame Relay over the PW.

5.3.2.1. Frame Sequence

The PW must deliver frames in the proper sequence.

5.3.2.2. Frame Size

In general, the maximum frame size for Frame Relay is 1600 bytes per [FRF.1.2]. This can be made larger in some implementations. If the MTU of the PW is less than (1600 bytes - size of PW headers), a fragmentation and reassembly mechanism may be needed.

5.3.2.3. End-to-end Transport Characteristics

[FRF.5] and [FRF.13] define a set of traffic parameters to support Service Level Agreements (SLAs). The design of the PW should preserve these end-to-end transport characteristics.

5.3.2.4. Connection Management and Congestion Control

Each Frame Relay header contains some connection management information, including

- a command/response (CR) bit
- a discard eligibility (DE) bit
- a connection ID (DLCI)
- an address extension indicator (EA)
- Forward/Backward Congestion Notification (FECN/BECN).

All of this information is vital to the integrity of the Frame Relay circuit. The Frame Relay PW AS shall define an efficient but optimized approach to transport such information across the PWD.

5.3.2.5. Link Management Support

Frame Relay defines a set of link management functions for PVC Status Management as specified in [T1.617D] and [Q.933A]. Link Management runs on a dedicated PVC; therefore, its operation does not impact actual user data. The management functions include:
- a heartbeat exchange that verifies that the link is operational
- a report regarding the status of one or more individual DLCIs

For some networks, such as the one shown in Figure 11, this link management is the only means to verify the end-to-end integrity of the Frame Relay virtual circuit. The PWE may required to emulate such functions. These functions will be transparent to the underlying network.

Another important consideration is that there should be some coordination between the PW’s link status and the associated Frame Relay VCs. For example, it might be necessary to tear down the VCs in the presence of a network fault.

### 5.3.2.6. DLCI Association

There are two scopes of DLCI addressing that have been defined by ANSI and ITU-T: Local and Global DLCIs.

- Local DLCI addressing means that DLCI numbers are only significant at one end of a Frame Relay virtual circuit at the local interface.

- Global DLCI addressing is an extension to PVC status management that allows a DLCI number to have universal significance. A global DLCI identifies the same VC at both ends across the network.

In the case when the DLCI is locally significant, the management of the PWD must provide a mechanism to coordinate the DLCIs at the two ends of the PW. The association can be done via signaling or configuration.

### 5.3.2.7. Multiplexing VCs over PWs

To preserve PW tunnel space and to enhance scalability of PWs, it would be very valuable to allow one or more VCs to be multiplexed onto the same PW. One scenario might be to associate an entire Frame Relay logical interface to a PW. Another possibility is that the assignment of VCs to the PW could be done via signaling or management.

If such multiplexing approach is used, the earlier discussion related to the packet sequencing, end-to-end transport characteristic, SLA preservation and link status management, shall be addressed with the same considerations.

### 5.3.2.8. Signaling Transparency

Since Frame Relay supports SVCs, the PWE may need to support signaling interworking at the service access for Frame Relay. InverseARP frames should be passed on without interpretation. In either case, these frames shall be transparent to the underlying
5.3.2.9. Soft PVC Support

One type of connection service that is provided by Frame Relay networks is called the Soft PVC (SPVC). The SPVC may be considered as three parts: two peer-to-peer PVCs at each end of the edge, and a SPVC between them. Figure 12 shows the SPVC interconnection example.

```
+---+        +---+       +---+       +---+      +---+
 | E |========| C |:::::::| C |:::::::| C |======| E |
 +---+        +---+       +---+       +---+      +---+
```

Where:

- "E" is the edge switch
- "C" is the core switch
- "=" is the permanent connection
- ":" is the switched connection

Figure 12: Example of an SPVC Over a Frame Relay Network

The creation of the SPVC within the core is triggered by detecting the existence of the PVCs at the edges. This detection is done either by network management or by some proprietary signaling.

Now consider the case where the Frame Relay Network is replaced by an PW network as shown in the Figure 10. The SPVC connection within the core is replaced by the PW. The behavior of the ingress and egress edges of the IP core should still behave in the same way towards the edge of the two Frame Relay switches at each end.
5.4. ATM

5.4.1. Reference Model

As far as PWs are concerned, ATM is very similar to Frame Relay. We will use the same reference network (Figure 9) for ATM as we did for Frame Relay. Of course, the Frame Relay switches would be ATM switches instead. Likewise, the PWE networks shown in Figures 10 and 11 are applicable to ATM.

5.4.2. Operational Considerations

Like Frame Relay, ATM provides connection-oriented circuit-based transport. There are two types of virtual circuit supported in ATM: PVC and SVC. In addition to virtual circuit connections (VCCs), ATM also supports virtual path connections (VPCs). There are also permanent virtual paths (PVPs) and switched virtual paths (SVPs).

ATM transports data in fixed size (53 byte) frames called "cells". Higher layer frames are adapted to these fixed size cells via ATM Adaptation Layers (e.g. AAL1, AAL2 and AAL5) and SAR. Different types of AALs have different cell header formats, and the cells may contain signaling information.

The following sections describe the set of considerations for PW support of ATM.

5.4.2.1. Cell Sequence

The PW must deliver frames in the proper sequence.

5.4.2.2. End-to-end Transport Characteristics

ITU-T [I.356] and ATM Forum [TM4.0] defines a set of traffic and QoS parameters. The design of the PW shall be capable of maintaining the end-to-end transport characteristic for such virtual circuit.

5.4.2.3. ATM SLA

ITU-T [I.371] defines performance targets for managing ATM traffic and congestion control. These target may be used by some service providers to define their ATM SLAs. The AS for ATM PWs should specify how SLA transparency will be achieved.

5.4.2.4. Connection Management and Congestion Control

The ATM header contains some connection management and congestion control information, as defined in [I.371]:

- Cell Loss priority (CLP)
- Connection Identifier (VPI/VCI)

- Payload Type Identifier (PTI) - distinguishes between an OAM (Operations, Administration and Management) cell and a user cell

- Explicit Forward Congestion Indication (EFCI)

All of these fields are vital to the integrity of the ATM circuit. The ATM PW AS shall define an efficient but optimized approach to transport such information across the PWD.

5.4.2.5. OAM and Link Management Support

ATM [I.610] defines a set of OAM functions. Likewise, [ILMI] defines a Link Management protocol to manage the ATM link, VCCs and VPCs. ILMI Link Management runs on a dedicated PVC; its operation does not impact actual user data. The management function is designed for a "heartbeat" exchange that verifies that the link is operational. It also provides a means to detect mis-configuration.

For some networks, such as the one shown in Figure 11, this link management is the only means to verify the end-to-end integrity of the ATM virtual circuit. The PWE may required to emulate such functions. These functions will be transparent to the underlying network.

OAM is often enabled to support important or real-time intensive traffic. OAM operation differs between VCCs and VPCs. In the case of VCC, the OAM cell is sent along the same VC as the user cells. In the case of VPC, the OAM cell is sent over a dedicated VC within the VPC.

OAM emulation shall be limited at the edge of the PW only, and the entire operation shall be transparent within the core.

Another important consideration is that there should be some coordination between the PW’s link status and the associated ATM VCs. For example, it might be necessary to tear down the ATM VCs in the presence of a network fault.

5.4.2.6. VC Associations

Each ATM connection ID has only local significance in the network. This local significance means that each ATM connection identifier (VPI and/or VCI) is only significant at local ATM interface, and is independent from the ID at the other end of the network. The management of the PWD must provide a mechanism to coordinate the IDs at the two ends of the PW. The association can be done via signaling or configuration.
5.4.2.7. Multiplexing ATM VCs over PWs

See the discussion in the "Multiplexing VCs over PWs" sub-section of the previous "Frame Relay" section of this document.

5.4.2.8. ATM Signaling Transparency

See the discussion in the "Signaling Transparency" sub-section of the previous "Frame Relay" section of this document.

5.4.2.9. Soft PVC Support

See the discussion and figures in the "Soft PVC Support" sub-section of the previous "Frame Relay" section of this document.

5.4.2.10. Segmentation and Reassembly (SAR)

The bandwidth overhead of the ATM cell is about 10% (= 5 overhead bytes out of 53 bytes total). For AAL5 traffic [I.363.5], it may be more efficient in terms of bandwidth to transport the re-assembled AAL5 frames instead of the individual ATM cells. This would involve some cost in terms of a SAR operation at each end of the PW. In some cases, especially if OAM is required to be supported over the PW, the PW may have no choice but to transport the ATM traffic in cell format.

Whether the ATM traffic is transported in a frame or cell format, it is the responsibility of the PWE to emulate the OAM functions to the adjacent ATM interface at each end.
6. Timing

In the recent Ken Burns Jazz television series, it was said of Louis Armstrong that he was very economical with his notes, but that the timing of those notes was everything. The timing of the reconstructed bit stream is similarly important. This section describes the various approaches to this problem. A summary is also provided at the end of the section.

6.1. Reference Model

Consider the example network shown in Figure 13.

```
+----------+                +----------+
|   PWE1   |                |   PWE2   |
|          |                |          |
|--------|  -----|  |   |--------|  -----|  |--------|
|E1|====>|FIFO|:::|S1|::|S2|:::|FIFO|====>|E2|
|++++|  -----|++|+++|++++|  -----|++|+++|
|    ^    |    ^    |    ^    |    ^    |
|    A    |    B    |    C    |    D    |
+----------+        E       +----------+
```

Where:

"En" is the TDM edge device
"PWEn" is the PWE adaptation device
"Sn" is a core switch
"A" - "E" are clocks
"=" is the T1 Bit Stream
":" is the switched connection

Figure 13: Timing Recovery Reference Diagram

A jitter correction buffer at the receive can handle short-term differences between these two clocks, but over time any absolute difference is going to cause this buffer to overflow or underflow.

Bits are clocked into a FIFO in PWE1 according to clock A, which is derived from the clock used at E1. The bits are packed into frames and clocked out according to clock B, which is the same as clock B. Clock B could differ from A, as long as there is an indication of the number of bits contained in the PDU.

The frames arrive at switch S1, and are clocked out according to the internal oscillator on the output interface of switch S1. The frames will depart at the same average rate at which they arrived, but the instantaneous bit rate will be different on each side of S1. Note that there could be short-term variations due to congestion, but S1 can’t experience long-term congestion with respect to the frames.
carrying emulated data, or the service won’t work.

The frames travel on to switch S2, which again forwards them. Note that switch S2 introduces yet another clock, which it uses to transmit the packets toward PWE2. Again the average rate is preserved, but the instantaneous rate will vary.

The frames arrive at PWE2 and are clocked into the FIFO when they arrive (using clock C). Note that clock C will have the same average frequency as B, but will have short-term variations. The bits are clocked out of the FIFO according to clock D.

6.2. Recreating the Timing

The big question is: where does clock D in Figure 13 come from? There are 5 possibilities, and these are detailed in the following sections.

1) Clock D is the same as clock A, and is delivered by clock E, which is an "External Timing" source, as described below.

2) If the switches S1 and S2 were synchronous, and SONET-style pointers were used, then Clock D could be derived from Clock C and the pointers. This is described in the "SONET Pointer Justification" section below.

3) Clock D is derived from the average rate of Clock C. This is the "Adaptive Timing" scenario described in a subsequent section.

4) Clock D is derived from a combination of the local oscillator at PWE2 and received RTP or SRTS timestamps. This is described in the "RTP" and "Differential (SRTS)" sections below.

6.3. External Timing

The simplest method for communicating timing from one end of a system to the other is an external timing source. This external timing source is normally a T1 or E1. Its 8 KHz frame rate is extracted and used to directly clock the reconstructed data streams, or as an input to a phase-locked loop to synthesize the desired clock. The drawback to this method is that a common external clock is not commonly available in a data network or in a multi-carrier network.

6.4. SONET Pointer Justification

SONET defines layers of pointers that allow for the multiplexing and transmission of asynchronous signals. These pointers convey the timing of the carried signal with respect to the timing of the encapsulating signal. Each SONET ADM must manipulate these pointers to preserve the timing. This method has the advantage of being well-defined and understood.
One way to apply this method to a packet-based network would be to ensure that all of the links on a given path are synchronous. This would be difficult for Gigabit Ethernet or POS links. Another way would be for each router to update the pointers as the packet traversed the router. This would be compute intensive. A final way to use a pointer-based method would be to limit the path to one physical hop.

6.5. Differential (SRTS)

[ATMCES] describes the SRTS (Synchronous Residual Time Stamp) method:

The SRTS technique measures the Service Interface input clock frequency against a network-wide synchronization signal that must be present in the IWF, and sends difference signals, called Residual Time Stamps, in the AAL1 header to the reassembly IWF. At the output IWF, the differences can be combined with the network-wide synchronization signal to re-create the input Service Interface clock.

The requirement for a network-wide signal is reasonable in a Telco or SONET environment, where such clocks are commonly available. From an equipment implementation standpoint, this method is similar to the SONET pointer method, which also uses adjustments that are relative to a separate clock (the line rate in the case of SONET). The advantage of a SRTS approach is from a deployment standpoint. A reference clock must be available at both ends, but not at any of the intervening routers.
6.6. Adaptive Timing

Adaptive timing is used when an external reference is not available. [ATMCES] describes adaptive timing as follows:

The adaptive technique does not require a network-wide synchronization signal to regenerate the input Service clock at the output IWF. A variety of techniques could be used to implement Adaptive clock recovery. For example, the depth of the reassembly buffer in the output IWF could be monitored:

1. When the buffer depth is too great or tends to increase with time, the frequency of the Service clock could be increased to cause the buffer to drain more quickly.

2. When the buffer contains fewer than the configured number of bits, the Service clock could be slowed to cause the buffer to drain less quickly. Wander may be introduced by the Adaptive clock recovery technique if there is a low-frequency component to the Cell Delay Variation inserted by the ATM network carrying cells from the input to output IWF.

Careful design is required to make adaptive timing work well. The instantaneous buffer depth must be filtered to extract the average frequency and to reject the jitter and wander.

Adaptive timing is ideal for many network applications where there is no external timing reference available (needed for SRTS), and where the packet rate is decoupled from the line rate (as in a routed network).
6.7. RTP

[RTP] uses an absolute timestamp to play out the bits at the same rate that they were received and packetized. RTCP (RTP Control Protocol) provides a means to synchronize the transmit and receive clocks.

6.7.1. RTP Timestamps

Section 4 of [RTP] defines a timestamp that is either 32-bits or 64-bits in size:

Wallclock time (absolute time) is represented using the timestamp format of the Network Time Protocol (NTP), which is in seconds relative to 0h UTC on 1 January 1900 [NTP]. The full resolution NTP timestamp is a 64-bit unsigned fixed-point number with the integer part in the first 32 bits and the fractional part in the last 32 bits. In some fields where a more compact representation is appropriate, only the middle 32 bits are used; that is, the low 16 bits of the integer part and the high 16 bits of the fractional part. The high 16 bits of the integer part must be determined independently.

A 32-bit absolute time stamp with a 16-bit fractional part would give a 15 us granularity (= 1/65535), which is too coarse for circuit emulation. This means that the 64-bit timestamp must be used, with a granularity of 23 ns.

The transmit timestamps are created according to the internal oscillator at PWE1 and interpreted according to the internal oscillator at PWE2. These two oscillators will vary by some amount, even if they are very accurate. The effects of this difference (or drift) is considered in the next section.

6.7.2. Analysis of Clock Drift

Since the two oscillators will vary or drift over time, the FIFO at PWE2 will eventually overflow or underflow, unless this drift is corrected. Figure 14 below shows why this must happen.

<table>
<thead>
<tr>
<th>TDM Frame Boundaries</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>PWE1 Wallclock</td>
<td>125</td>
<td>250</td>
<td>375</td>
<td>500</td>
<td>625</td>
<td>750</td>
<td>875</td>
</tr>
<tr>
<td>PWE1 Timestamps</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td>PWE2 Wallclock</td>
<td>125</td>
<td>250</td>
<td>375</td>
<td>500</td>
<td>625</td>
<td>700</td>
<td>825</td>
</tr>
<tr>
<td>PWE2 Offset</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>50</td>
<td>50</td>
</tr>
<tr>
<td>PWE2 Timestamps</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td>RTCP Update</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>750</td>
</tr>
</tbody>
</table>

Figure 14: Clock Drift
In Figure 14, PWE1 has a clock that is running faster than PWE2. Note that this difference is exaggerated in the figure. PWE1 sends out packets according to its clock, with timestamps also derived from its clock. PWE2 uses its clock to decide the appropriate times to remove bits from the FIFO. It is clear that packets will arrive faster than they are being removed, and the FIFO at PWE2 will eventually overflow.

### 6.7.3. RTCP/NTP as a Solution

One possible solution is to use NTP [NTP] or RTCP [RTP] to coordinate the clocks at PWE1 and PWE2. This is shown in Figure 14 in the row marked "RTCP Update" where a value of 750 arrives at PWE2. This lets PWE2 create an appropriate offset to correct its output timing.

NTP could also be used to ensure that clocks B and D were very close in their absolute value.

### 6.8. Summary of Timing Recovery Methods

Figure 15 below shows a summary of the methods for timing recovery.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Ext.</th>
<th>SONET</th>
<th>SRTS</th>
<th>RTP/RTCP</th>
<th>Adaptive</th>
</tr>
</thead>
<tbody>
<tr>
<td>External timing required?</td>
<td>yes</td>
<td>no</td>
<td>yes</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>Per-hop manipulation?</td>
<td>no</td>
<td>yes</td>
<td>no</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>De-jitter buffer?</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Clock synthesis?</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Suitable for circuit timing?</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
</tbody>
</table>

Figure 15: Summary of Timing Recovery Methods
7. Integrity

7.1. Validation

Editor’s Note: this section will describe how the transported data is verified. It will also discuss whether the native checksum or CRC should be transported or stripped and regenerated. This section needs more work.

7.2. Sequencing

Editor’s Note: this section will discuss preservation of order. This section needs more work.

8. Management

8.1. Session Multiplexing

One way to facilitate scaling is to increase the number of PWs per underlying tunnel. There are two ways to achieve this:

- For a service like Relay or ATM, all of the VCs on a given port could be lumped together. VCs would not be distinguishable within the PWD.

- Service SDUs could be distinguished within a PW-PDU by port, channel or VC identifiers. This approach would allow for switching or grooming in the PWD.

Editor’s Note: This section needs more work.

8.2. Signaling

Editor’s Note - this section will describe the signaling used to establish and destroy sessions, as well as any variable parameters related to encapsulation or operation. This section needs more work.

8.3. Security

Editor’s Note: this section will discuss the security of signaling. Security of the transported data is out of scope. This section needs more work.

8.4. Encapsulation Control

Editor’s Note - this section will describe the control of variables related to encapsulation. This section needs more work.

8.5. Statistics

The PWE can tabulate statistics that help monitor the state of the network. Typical counters include:
- Counts of PW-PDUs sent and received, with and without errors.
- Counts of service PDUs sent and received, with and without errors (non-TDM).
- Service-specific interface counts.

Editor’s Note: This section needs more work.

8.6. Administrative Status

Editor’s Note: this section will describe the control of administrative status. This section needs more work.

8.7. Operational Status

Editor’s Note: this section will describe the monitoring of operational status. This section needs more work.

9. Transport Protocols

9.1. IP

Editor’s Note: This section describes any protocol-specific considerations for transport over IP. This section needs more work.

9.2. L2TP

Editor’s Note: This section describes any protocol-specific considerations for transport over L2TP. This section needs more work.

9.3. MPLS

Editor’s Note: This section describes any protocol-specific considerations for transport over MPLS. This section needs more work.

9.4. Common Infrastructure

Editor’s Note: This section describes the common framework used over the three transport protocols. This section needs more work.

10. Acknowledgments

This document was created by the PWE3 Framework design team.
11. References

11.1. IETF RFCs


11.2. IETF Drafts


11.3. ATM Forum


11.4. Frame Relay Forum


11.5. ITU


11.6. IEEE


11.7. ANSI


11.8. Telcordia


12. Security Considerations

It may be desirable to define methods for ensuring security during exchange of encapsulation control information at an administrative boundary of the transport network.

13. Authors’ Addresses

Prayson Pate
Overture Networks
P. O. Box 14864
RTP, NC, USA 27709
Email: prayson.pate@overturenetworks.com

XiPeng Xiao
Photuris, Inc.
2025 Stierlin Court
Mountain View, CA 94043
Email: xxiao@photuris.com

Tricci So
Caspian Networks
170 Baytech Dr.
San Jose, CA 95134
E-Mail: tso@caspiannetworks.com

Craig White
Level 3 Communications, LLC.
1025 Eldorado Blvd.
Broomfield, CO, 80021
e-mail: Craig.White@Level3.com

Kireeti Kompella
Juniper Networks, Inc.
1194 N. Mathilda Ave.
Sunnyvale, CA 94089
Email: kireeti@juniper.net
14. Full Copyright Section

Copyright (C) The Internet Society (2000). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.