Generic
Data Communications
Service Models

Roy Bynum
IEEE 10GigE p802.3ae and EFM 802.3ah Task Forces

June 29, 2001

Table of Contents

Acknowledgments:
Chuck Mullins - For many conversations over a year's time to distinguish the language of services vs. infrastructure

Introduction and Summary

There are several distinct models that make up the data communications specific services that are provided to customers of transmission service providers, otherwise known as "carriers". This includes those service providers known as Incumbent Local Exchange Carriers (ILEC) and Competitive Local Exchange Carriers (CLEC). These are Private Line, Virtual Private Line, Best Effort, and Virtual Private Networking. Many times these are viewed only from the marketing or customer viewpoint. For those that develop service technology, implement it, or support it, a better understanding is needed.

The objective of this paper is to provide a basis for better understanding of the relationships between different data communications service types and the infrastructures that support them. It is also to make a distinction between data communications services specifically and value added services that use the same infrastructure. It is a technical paper that is intended for engineers and management that develop service infrastructure technologies and those that support the development, deployment, and marketing of data communications services.

This paper started out as an attempt to provide simple generic distinguishing descriptions of the different service provided by data communications service providers. I created those simple descriptions and sent them to the people that requested them. However as I discussed these descriptions, it became apparent that there is a lot of confusion about the differences between the services specifically and the infrastructures that supported them. There is also confusion between value added services and data communications services.

In this paper four generic service models are defined and a simple explanation of the characteristics that are use to distinguish them is provided. A source of confusion about the differences between the different data communications services and about data communications services in general is addressed. An expanded explanation of each service model, based comparisons of specific distinguishing characteristics is next provided. The original simple descriptions are provided at the end of this paper.

Note: This document is intended to reflect generic models for data communications services. Any numbers referring to performance, availability, reliability, or otherwise are intended for the purpose of comparison within this document only. In some cases the numbers provided for performance, availability, reliability, stability, etc., are optimistic compared to some of the actual services delivered. The numbers herein do not directly reflect any service level agreements that may or not be available from any service provider.

Four Distinct Models

There are four major categories of data communications services. Each becomes an independent, distinct service model based on the connection type, bandwidth type, infrastructure level, availability, reliability, stability, security, routing autonomy, operations/network management, and the customer cost structure. These are divided into "Private Line", "Virtual Private Line", "Best Effort", and "Virtual Private Networking". These tend to take on the characteristics of a hierarchy of services. Within each of these services, it is also probable to have an additional hierarchy of services and service level agreements.

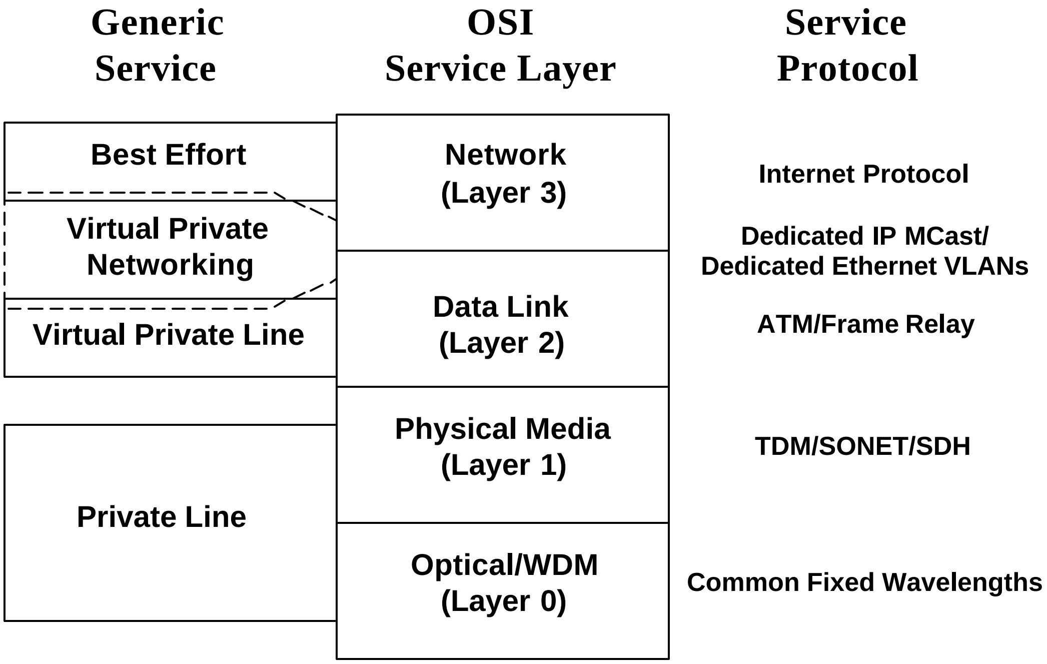

Figure 1 Generic Data Communications Service Models

The connection type definition is based on whether the service is connection oriented or non-connection (connectionless) oriented. The bandwidth types are fixed, burstable with a committed information rate, or variable based on core bandwidth availability. The service level refers to the OSI model and what level of the data communications stack the customers' equipment operates at in order to use the service. The infrastructure level also refers to the OSI model of data communications layers and what layer that service operates at. Availability refers to the relative "up-time" that the customer access has. Reliability refers to how many errors or dropped data packets/frames will occur within the data communications bandwidth. Stability refers to the latency variance between data packets/frames of variable size that will be transiting the infrastructure of the data communications service. How hard the data communications segregation and the type of segregation between any one customer and others is considered the security of the service. The level of variability of the routing of customer data communications traffic through the infrastructure is the autonomy of the service. Operations/network management is often "out of band" or "in band" with the revenue bearing traffic. "Out of band" may be included with the lower level signaling of the data communications infrastructure, but is not part of the data traffic used for customer service data traffic. The customer cost structure is based on the relative cost of the services to the customer. The service provider margins are a relative relationship of the profitability of the different services relative to each other; not including any value added services that are also provided.

Recently, there has been a lot of effort to provide all of the different data communications services over a singe common shared bandwidth infrastructure at a higher level than traditional fixed, segregated, bandwidth TDM/SONET/SDH. Efforts have been made to sell variable rate Virtual Private Line services to replace true Private Line services. These efforts have had mixed results, sometimes at the loss of customer satisfaction. In order to keep the customers, sometimes the more expensive fixed rate Virtual Private Line service was provided at the lower variable rate prices, at a financial loss to the service provider. Without an understanding of the distinctions between the generic service models, this is an easy mistake to make.

A Source of Confusion

It must be noted that very often the different services are confused with having distinctly different infrastructures. While it is recognized that each service can have different service specific systems, there is a vast difference between the services and the infrastructures that they are provided over. More often, all of the services are provided over a lower common denominator type of infrastructure that is used to provide a service distinct from the other services. The real understanding of the distinction between a service and the infrastructure is recognizing that a service is what is billed for, not the infrastructure. For example, almost all services use the same infrastructure of point to point inter-machine trunks to provide the basic bandwidth that is billed for as "Private Line".

There has been a lot of data communications technology developers that have stated that they were developing "TDM circuit emulation" over some other type of service infrastructure. What they were actually developing is the ability to provide "Private Line" or "Virtual Private Line" services over non-traditional types of infrastructures. It is hoped that this paper will help relieve some of that confusion.

Another level of confusion is the part that different data communications layers play in the services, as well as where within the process the various functions are labeled as belonging to one Layer or the other. As part of this paper, the Open System Interconnect (OSI) model of layers within data communications is used to explain the distinctions between the services. There is a distinction between how the Information Technology (IT) community and the Telecommunications service providers view the application of the different layers. The Telecom community often refers to the out of band network management overhead as Layer 2 (Data Link) because if provides a management data link between various network elements. From the IT viewpoint, that overhead is a sublayer of Layer 1 (Physical Media). This paper will provide a view based on the IT understanding of data communications services. The OSI model does not take into account the development of Optical or Wave length Division Multiplexing (WDM) technology. This paper will refer to the Optical or WDM level as Layer 0.

The various service models are provided at different Layers within the OSI model. The service provider provisions and supports these services an infrastructure at the specific Layer or the one below that which the service is provided at. For example, Frame Relay is a Layer 2 service, but the infrastructure creates a logical segregation specific to each customer that is more closely related to a Virtual Layer 1.

Content Services vs. Communications Services

Data communications services are a specific segment of the services provided by diverse group of communications service provider companies. Content and other value added services might use the same infrastructure as specific data communications services, but are a separate segment of services provided by that same diverse set of companies. Being able to determine what is actually billed separates these service segments.

In many cases, content services are confused with the data communications services or data communications infrastructures. Services such as Voice and other valued added services are actually content services instead of direct data communications services. Data communications is specific to computers or other electronic systems. In the case of Voice service traffic, the Voice content is vocal human communications that have been converted to a digital electronic signal before it is communicated as the content of a stream of data.

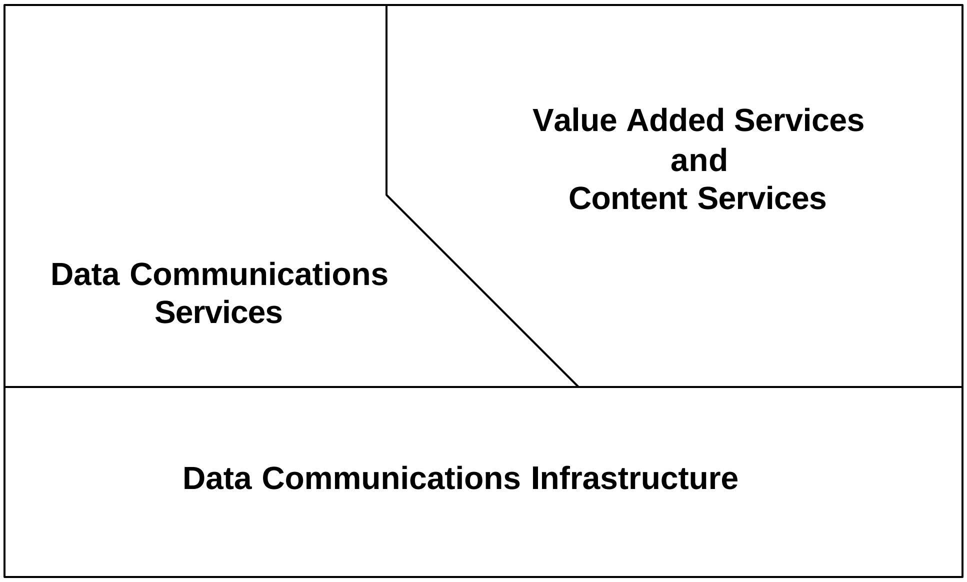

Figure 2 Relationship of Data Comm & Value Added Services to Data Communications

There is confusion about the role that data communications infrastructure plays to not only data communications services but also other, value added and content services. In the case of value added and content services, much of the same infrastructure is used, that is also used for billable data communications services. The distinction is that the customers of the values added and content services often do not directly pay for data communications services as part of the value added and content services. If any billable data communications services are used to provide connectivity for the value added and content services, it is often treated as a separate billable service. Sometimes the use of the data communications infrastructure is not billed for at all.

In the same manor that various different upper Layer protocols can function and use a common Layer 1 infrastructure, content services can be implemented over multiple types of generic data communications infrastructures. Voice can be treated as a direct digital encoded signal, or it can be packetized into various data communications protocols. As a direct digital encoded signal it is carried directly in a Private Line inter-machine trunk. As a packetized data stream it can be carried over Frame Relay or ATM in Virtual Private Line virtual circuits, or as Voice over IP (VoI) in the Best Effort or Virtual Private Network service infrastructure.

In the case of local voice services, the customer is actually paying for a circuit on demand communications service. Over the same service, the customer may want to run computer data in the form of a dial up link to another computer, or the voice conversations that are normally associated with the service. In both cases, the customer is paying a fixed rate for connectivity to a circuit switch over which a circuit is established on demand as established by the "off hook" dial codes sent to the circuit switch. When the circuit crosses between "local" and "long distance" the customer pays additional usage charges for the communications service. In all case, while the service is called "voice", voice is actually a content of the service that gives it added value.

Dial up Internet service is also a content value service. Based on connectivity access to a common best effort communications service, the value of dial up Internet services is the "content" that is provided over the Internet, not the use of Internet Protocol to communicate between computer systems. Internet access provides a Best Effort data communications service to Internet content service providers.

In addition to the Internet communications itself, content vendors with Internet accessible systems are able to provide fee-based access to content. For example, in this way, an Internet video download service is able to use the customers' access to the Internet as a communications infrastructure, while the customers pay for it as data communications services over the Internet/TDM infrastructure. This is a good example of the hierarchy and layering relationship of content services, communications services, and infrastructure.

Private Line

Private Line is the most basic of the four services and is the most commonly data communications sold service in the telephony service provider industry. Access to many of the other services, particularly the value added content services such as traditional voice, is though Private Line data communications services. Private line is also the oldest data communications service model.

PL Connection Type

Private Line (PL) services are specifically only point to point. This service is distinctly connection oriented at what the IT community thinks of as the Physical Media Layer (Layer 1). Optical services (Layer 0) are also specifically connection-oriented point to point. This means that the customers can use any type of Data Link (Layer 2) and above protocols that they desire and that is appropriate such as SDLC, HDLC, LAPB, Ethernet, etc.

PL Bandwidth Types

PL is also distinguished by having a hierarchy of specific fixed bandwidths based on the hierarchy of Time Domain Multiplexed (TDM) infrastructure payloads (T0/DS0, T1/DS1, T3/DS3, OC3/STM1, OC12/STM4, etc). Except for the emerging use of 802.3 Ethernet, the Layer 1 signal encoding used by the custome r is also normally based on the Telecommunications encoding types, (B8ZS, etc or SONET/SDH). The bandwidth and signal encoding used for Optical services have not been fully determined at the time that this is written. At present, it is most likely that the Optical services to customers will also be based on some form of the existing Telecommunications industry encoding standards such as SONET or SDH. All PL services are multiplexed based on physical time domain payloads or discrete physical wavelengths.

PL Service Level

The PL service interface is normally at the Physical Media Level (OSI Level 1). Customers' data equipment can normally utilize any Data Link Level (OSI Level 2) protocol that their applications require, including all of those that are used for the other services. This service is unique in this aspect.

PL Infrastructure Level

Service providers use the most basic infrastructure to provide PL services. Service provisioning, and operations support is done at the specific Layer of the billed service. For Layer 1, the TDM infrastructure is used directly to provide the service. Provisioning is done with TDM based provisioning and grooming systems. Operations support, which includes fault/maintenance protection as well as performance monitoring, is done at that same level using the same infrastructure equipment. With Layer 0, Optical services use the optical fiber or wavelengths for provisioning and operations support. New direct optical switching technology is planned to provide additional provisioning and operations capability.

PL Availability

The availability to the customer of Private Line service connectivity is the highest of all of the service models. Full redundancy with fast fault restoration and maintenance switching is the hallmark of the inter-machine trunk infrastructure that Private Line services are directly provisioned over. With the exception of the sometimes single threaded local access loops, PL customers normally have better than 99.99% availability of their circuit connectivity. For customers that require even higher availability, redundant local loop circuits with physical route diversity can be provisioned. This can give a total availability of as much as +99.999%

PL Reliability

PL is the most reliable as far as data errors and delivery is concerned. Often the service level reliability is measured with a Bit Error Rate (BER) in average errored bits per bandwidth bit rate. This is often so low that it is expressed as a negative exponential number such as 10^{-10} or better. For example a BER of 10^{-10} is an average of no more than one bit error for every for 10,000,000,000 bits. At the data communications level this translates to about a data loss of about 0.000001% at an average of 400 bytes per packet/frame.

PL Stability

PL also provides the most stable data communications service. Once a customer hands off the data to a service provider, the data packets/frames transit the infrastructure with bit to bit level of latency variance. This bit level of stability is measured in pecoseconds per bit. This translates into a latency variance of "0" at the data packet/frame level.

PL Security

PL provides the greatest level of security for the customers' data. Each customer's traffic is specifically segregated from each other customer's traffic at the physical facility level. This is equivalent to the customer leasing a physical infrastructure facility, like a specific copper or fiber pair. Within the telecommunications Layer 1 signaling there is an "out of band" overhead that encapsulates the customers’ data signals and provides a hard logical segregation of data communications signals/traffic. Unless there is a provisioning error that links one customer to another, PL provides a physical segregation level of data protection.

PL Routing Autonomy

Within the infrastructure used to provide PL services, the circuits are hard provisioned with little routing autonomy within service layer. Once the circuit is provisioned from one point to another only a fault or maintenance occurrence will change route that provisioned for the service, and often that is fixed by a pre-planned or direct physical layer infrastructure alternative, such as a "switch to protect" over a SONET ring.

PL Operations/Network Management

Operations/network management of the PL service infrastructure is "out of band" from the customers' data communications traffic. Separate, fixed bandwidth facilities are provided at the Layer 1 signaling level, and out side of the circuits provisioned for the customers, to provide the service providers with the ability to operate, maintain, and repair the infrastructure. These facilities range in bandwidth from a few kilobits per second for Tx and DSx services, to several hundred megabits per second for SONET/SDH systems. At the service edge, this overhead originates on the customers equipment interfaces and is then used by the service providers. In addition, fixed bandwidth inter-machine trunks are provisioned over the transmission infrastructure to provide additional Data Communications Network (DCN) facilities. The "out of band" and DCN facilities are generally not accessible by the customers. The consumer protocol, Ethernet is undergoing a change that will give customers limited access to some of the service overhead functionality which will require the service providers to block access to what is not required by the customers.

PL Customer Cost Structure

The facilities used for PL are used for all other services as basic inter-machine trunks to provide the scalable bandwidth for those services. PL does not however have the additional systems which are used to provide the other services, with the additional capital, facilities, operations, and back office costs. Without those additional costs, PL can be a service that has high margins for a data communications service. PL also continues to be less of a commodity service, which keeps the pricing for the service at a higher level. In addition to the base bandwidth rating costs, PL circuits also incur distances charges on the bandwidth. Even with the higher cost per bandwidth and distance, PL continues to be an extensively used service.

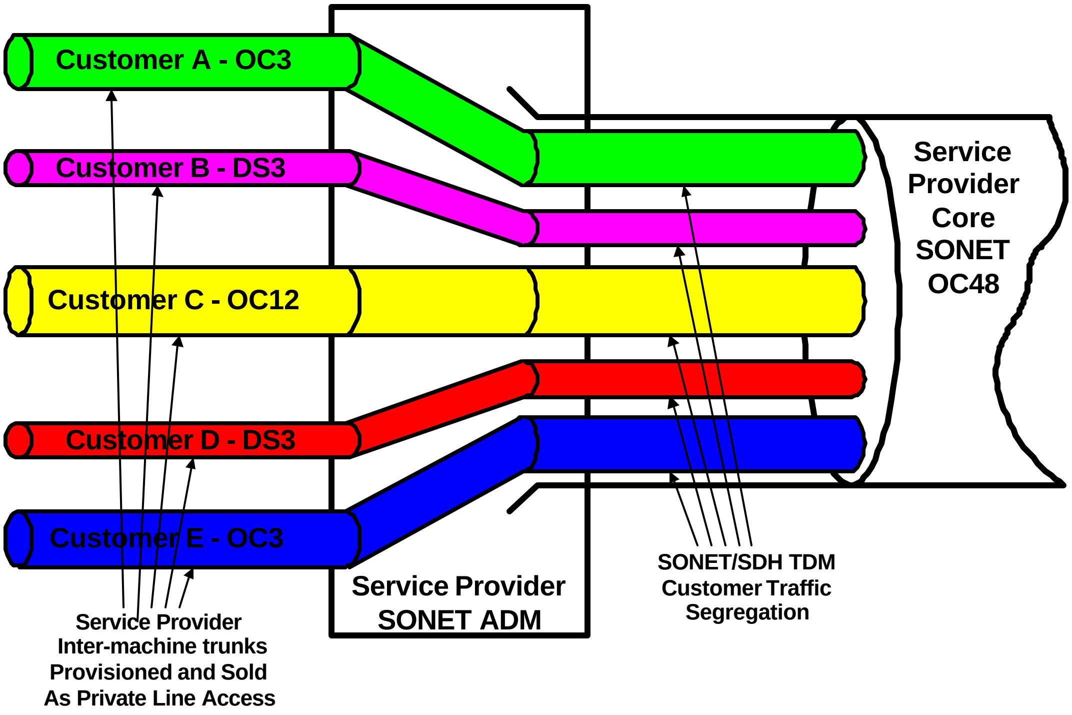
Customer A - OC3
Customer B - DS3
Customer C - OC12
Customer D - DS3
Customer E - OC3
Service Provider Core SONET OC48
Service Provider SONET ADM
SONET/SDH TDM Customer Traffic Segregation
Service Provider Inter-machine trunks Provisioned and Sold As Private Line Access

Figure 3 Private Line Service Model

PL Service Provider Margins

Private Line services have the highest margins of any data communications only service. Only two functions are normally part of the billable service, bandwidth and distance.

Private Line Service Summary

Private Line is a fixed bandwidth, point to point, connection oriented, Layer 1 service over physical Layer 1 facilities. It provides the most reliable, stable, and secure data communications available. Private Line Services segregates each customer’s traffic within fixed physical and fixed time domain leased facilities. The aggregated time domain facilities are multiplexed into a larger transmission core bandwidth to share the high bandwidth transmission facilities. PL is a costly yet extensively used service with high margins the service provider.

Virtual Private Line

Virtual Private Line (VPL) type services are based on providing Layer 2 connectivity over a virtual Layer 1 facility. The most common Layer 2 protocols used to provide these services are ATM and Frame Relay. While the Protocols are very different, the services provided have certain commonalties. The specific services are provided through the use of service gateways that link the customers' access to the service specific infrastructure. ATM is a fixed 53 byte "cell" based protocol and Frame Relay is a variable size "frame" based protocol.

VPL Connection Type

VPL provides data communications between multiple customer sites over a common infrastructure. Each site communicates to each other site by connection oriented, point to point, Permanent Virtual Circuits (PVCs). Multiple PVCs can be provisioned from each site, which gives VPL the ability to provide point to multi-point services. While the service provider uses a connectionless protocol architecture to provide the virtual layer 1 switching, the service itself is connection oriented.

VPL Bandwidth Types

There are several different bandwidth definitions for VPL services. Fixed bandwidth services are available using Constant Bit Rates (CBR) over ATM. There are also Variable Bit Rate (VBR) and Available Bit Rates (ABR) available over ATM. The links between the customer and the service gateway are normally over existing fixed bandwidth TDM infrastructure. Frame Relay (FR) normally has a fixed Committed Information Rate (CIR) that is a portion of the bandwidth available over the fixed bandwidth link between the customer and the service gateway. Frames rates that exceed the CIR are tagged as "drop enabled". When the bandwidth utilization within the infrastructure becomes close to being congested, the "drop enabled" frames are dropped. There are customers that obtain 0 CIR FR services and use them for low priority, non-time critical applications that provide data reliability within the applications themselves. Other customers use FR with applications that allow for tunable bandwidth usage to make use of only the CIR bandwidths. Access from the customer site to the VPL service gateway is often fixed TDM links between the customer and the service gateways that are provisioned and supported as fixed bandwidth PL in metro and local service domains. For almost all of these, the access service bandwidth is often greater than the service bandwidth purchased by the customer. The actual service bandwidth purchased is the CBR or CIR bandwidths.

VPL Service Level

The VPL service interface level is at the Data Link Layer (OSI Layer 2). Only services for specific protocols, ATM and Frame Relay are currently provided. These protocols provide Permanent Virtual Circuits (PVC) for the customers' connection oriented links over the service, between the service gateway ports. Only customers' applications that operate over ATM or Frame Relay can make use of this service.

VPL Infrastructure Level

While the service is Layer 2, the infrastructure is a combination of fixed TDM PL links and Virtual Layer 1 Switching. The term Virtual Layer 1 Switching is used because the service infrastructure encapsulates the customers' Layer 2 protocol in the manner of a Layer 1 protocol and provides the multiple site gateways to multiple site gateways communications. Within the service infrastructure, the service bandwidth is statistically multiplexed and is shared by multiple customers. With the exception of a "drop enable" tag on FR frames, the customer cell and frames are delivered unmodified over the infrastructure. Often the virtual switching infrastructure is thought of, and presented as a "cloud". That cloud is actually L2 or L3 switches that are interconnected by a mesh of point to point links over the same inter-machine trunk infrastructure that is used for Private Line services.

VPL Availability

Availability of VPL service connectivity is based more on the access gateway port than the transmission infrastructure. The service gateway that encapsulates the customer traffic into the virtual Layer 1 switching infrastructure often becomes a single point of failure. By providing redundant, diverse routed links between the gateway systems improves the availability of the customers' virtual circuit connectivity and provisioning these redundant links over bandwidth protected inter-machined trunks, link fault tolerance is not solely dependant on the gateway systems or the gateway systems' software. Because of the single point of failure the service connectivity is often no better than 99.95%.

VPL Reliability

There are several different levels of reliability for VPL services. Most often these are related to the Quality Of Service (QOS) rating of the ATM service definition. The base reliability standard of ATM has a cell loss of 10^{-8}. With lower level QOS services, there may be a higher cell loss. Frame Relay does not have the same base reliability standard, but often has a history of about 10^{-4} frame loss.

VPL Stability

Within the service ATM cell delivery latency variance is generally very small. Because of the fixed cell format of the protocol, the maximum latency variance of ATM over a non-congested infrastructure is the bandwidth rate bits time of a cell at each transmission interface. Each switching point in the service infrastructure increases the latency variance. Over a congested infrastructure, the latency variance is directly related to the service QOS. The higher QOS has a lower latency variance, while the lower QOS has a higher latency variance dependant on the congestion buffer sizing in the infrastructure switches.

Frame Relay has a much higher latency variance. The latency variance can be as little as a few milliseconds, or a great as a hundred milliseconds, depending on the congestion of the service infrastructure and the distance between service gateway customer ports. This makes application performance over Frame Relay somewhat non-deterministic. This is much more severe for the bandwidth that is over CIR. Applications can be tuned so that only the CIR bandwidth is used, and the latency variance consistently compensated for, so that it appears that the overall latency is consistent.

VPL Security

The encapsulation of the customers' protocol data cell/frames provides a lower layer software/protocol logical segregation between any one customer's data traffic and any others'. The PL links between the customers' sites and the gateways have the standard PL security. These combine to provide to provide a very high level of data security, although it may not be as high as true PL.

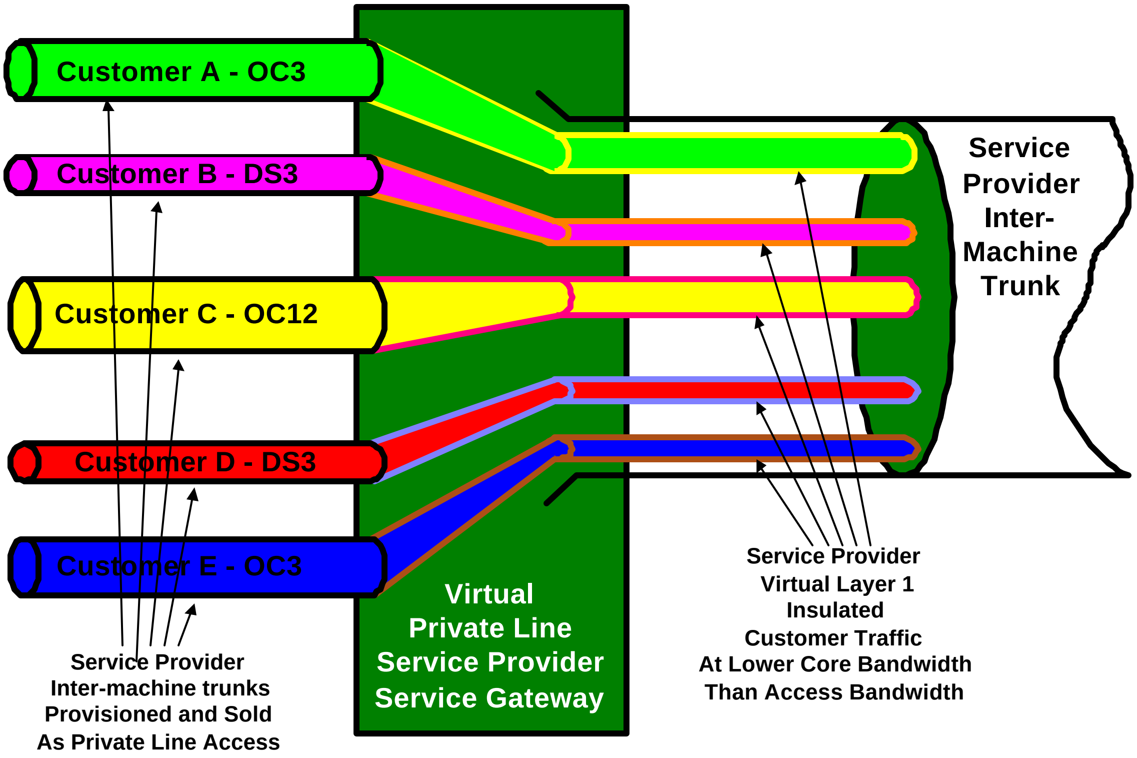
Customer A - OC3
Customer B - DS3
Customer C - OC12
Customer D - DS3
Customer E - OC3
Service Provider Inter-machine trunks Provisioned and Sold As Private Line Access
Virtual Private Line Service Provider Service Gateway
Service Provider Virtual Layer 1 Insulated Customer Traffic At Lower Core Bandwidth Than Access Bandwidth
Service Provider Inter-Machine Trunk

Figure 4 Virtual Private Line Service Model

VPL Routing Autonomy

The circuits between the customers' sites and the gateway ports are provisioned as standard PL local loop services. Within the service infrastructure "cloud" the customers' data traffic routing is only loosely provisioned. The implementation architecture of the "cloud" and the gross traffic management between gateway sites is the only determination of how the traffic is routed. Often fault and operations route switching is often done with a certain amount of autonomy within the service infrastructure.

VPL Operations/Network Management

Operations/network management is considered to be out of band to the customers' traffic. The PL local loop links between the customers' sites and the gateway sites is managed as standard PL services. Within the VPL service infrastructure "cloud", segregated facilities are provided within the virtual Layer 1 domain of the service. The only time that the service provider has direct access to the customer data itself is at the gateway where it is encapsulated and such things as the "drop enabled" tags are assigned. The customers do not have access to the service provider operations/network management facilities or systems.

VPL Service Provider Margins

The margins on VPL services are normally moderately high. Margins for service providers are based on several factors. Most notable of these is that the customer purchase access bandwidth in addition to any guaranteed bandwidth across the service. Any access bandwidth traffic over and above the guaranteed bandwidth is normally treated as preemptable traffic. In addition to filling in between the data traffic busting of the guaranteed bandwidth traffic, this traffic can make use of the service bandwidth that is normally reserved for fault protection in PL services.

VPL Customer Cost Structure

VPL is not a commodity service. There are three specific components common to the cost of VPL to the customers. The first is the cost of the PL local loops between the customers' sites and the gateway sites. Only the distances between the customers' sites and the gateway sites incur distance charges in addition to the bandwidth rates. The next is the cost of the VPL service itself. The next is the cost of the guaranteed service bandwidth (CBR or CIR) across the service infrastructure. In addition to these costs there are other costs that are based on the bandwidth and bandwidth type, the number of multiple communications points, and any QOS ratings of the services provided. The real savings to the customer is that within the service infrastructure, the customer does not normally pay distance charges. Within the business requirements of the customers VPL services often are vary cost effective.

Virtual Private Line Service Summary

Virtual Private Line is a point to multi-point, connection oriented, Layer 2 service at fixed and burstable best effort bandwidths over Physical and virtual Layer 1 facilities. It provides secure data communions that is moderately reliable and moderately stable. The local access only distance charges provides a major savings to the customer. The statistical multiplexing and access service bandwidth to core bandwidth ratio also provides an opportunity for additional billable functionality to service provider, creating moderately high margins. Unlike Private Line, Virtual Private Line allows transmission core bandwidth to be shared at the data level, instead of the physical time domain level. Unlike Virtual Private Network, which will be discussed later, Virtual Private Line does not modify or directly use the customers’ data packets/frames for routing or performance monitoring.

Best Effort Services

Best Effort data communications are shared Layer 3 (IP) services that are most generally associated with the public Internet. There are other, dedicated data communications service infrastructures that qualify as Best Effort. Although 0 CIR FR and ABR ATM can also be considered as best effort as far as data reliability is concerned, there are other characteristics that distinguish Best Effort services from other services. Best effort services are considered the lowest cost, which is reflected in the low reliability and poor stability of the data over the service infrastructure. The protocol that currently used to provide the service interface is Internet Protocol (IP). The terms "IP Services", or "Internet Services" are often used synonymously within the context of Best Effort Services.

BE Connection Type

Best Effort services are connectionless in that each data packet is handled independent of other data packets within the service infrastructure. The independent addressing of each data packet based on a common registry of addresses provides that connectionless communications ability. Whatever connection orientation is provided by the Layer 2 protocol in each link between the service infrastructure elements, that connection functionality is specific to that link only and not the service as a whole.

BE Bandwidth Types

Within the service, bandwidth is based on the overall infrastructure bandwidth availability only. In most cases there is no way to provide any kind of fixed bandwidth services.

For the most part, there is major difference between the bandwidth in the access to the service and the amount of bandwidth available within the infrastructure of the service. This higher amount of access bandwidth to core bandwidth can be referred to as "statistical gain". This gain is dependent on the "bursty" nature of the customer's data traffic. The high instantaneous bursts of traffic are buffered and used to "fill in" the "gaps" between traffic bursts to provide an overall bandwidth usage average that is lower than the peek access bandwidth.

There are some efforts to provide a minimal level of QOS that would provide better access to the available bandwidth for certain customer requirements and create virtual "fixed" bandwidth services. These are most generally associated with dedicated infrastructure for a specific group of customers. The access infrastructure bandwidth most often defines the "available" bandwidth that the customer sees. The bandwidth that the customer is able to actually able to use is based on the service infrastructure.

There are attempts to provide a shared bandwidth access infrastructure with access port bandwidths that have a certain amount of Guaranteed Bandwidth Access (GBA) and Burst-able Bandwidth Access (BBA). GBA is the base subscription bandwidth that is supportable within the access network. BBA is an attempt to provide burst-ability for data traffic at a limited amount of bandwidth for a limited amount of time. It is assumed that there is a certain amount of overall bursty-ness to the customer's traffic in which they do not use all of their GBA bandwidth, which gets filled in with the BBA bandwidth. The GBA and BBA bandwidths are more often not based on the traditional bandwidth granularity of traditional PL or VPL services. The average of the total bandwidth used by the customer has to remain within the overall supportable subscription bandwidth of the access infrastructure or excessive data loss starts to occur.

BE Service Level

Best Effort services are normally based on Internet Protocol (IP) which is a Network Level (OSI Level 3) protocol. IP, originally developed for the Department of Defense was made available to schools and universities as part of a government financed dedicated communications network, National Science Foundation Network (NFSNet). IP expanded in use outside of the NFSNet because of its low cost and ability to provide communications between a wide variety of computers. A wide diversity of applications that can operate over IP can make use of this service have also been developed over the years. With the development of the original WEB content service applications, Best Effort services stated to be commercialized, and provided as a general service to almost all levels of businesses and home users. Many content and other value added services applications are designed to operate specifically over Best Effort services.

BE Infrastructure Level

This service has an infrastructure that operates at the same level as the service. The infrastructure for Best Effort services is made up of IP Network Layer Routers or Routing Switches. IP is a Layer 3 protocol that is used for both the service and the infrastructure. The customers' enterprise network boundary routers are connected to service provider routers generally by means of access PL service links. The routers, customers' and service providers', operate basically in a peer to peer relationship at Layer 3 (IP). These provide the individual connectionless packet routing within the service infrastructure and between the customers' infrastructure and the service providers' infrastructure. Fixed bandwidth inter-machine trunks similar to PL or VPL circuits provide the data communications traffic pathways between all of the Routers. The service data traffic statistically multiplexed within the shared service bandwidth at Layer 3 (IP).

BE Availability

There are several components to the availability of Best Service and service bandwidth. The components are access infrastructure/access bandwidth, core infrastructure, and core bandwidth.

The standard access infrastructure for individual customers can be dedicated PL circuits or dial-up circuits through an ISP modem pool. The PL circuits have the full 99.99% availability of standard PL services. With PL access the customer has access bandwidth available all the time, whether it is used or not.

The dial-up service availability is based on the ratio of the number of customers the ISP has to the number of modem ports that the ISP has implemented. This ratio is also adjustable relative to the ratio of business dial-up customers to residential dial-up customers. For the most part, dial-up customers can get access to bandwidth generally 95% of the time that they attempt a dial-up session. Also dial-up customers' access will terminate when the service is not in use. For the most part actual bandwidth availability is less than 10%.

There are other access infrastructures that Best Effort services are provided over, such as Cable Modem and DSL. With Cable Modem, the time availability is very high, around 99.9%; the bandwidth availability will vary somewhat unpredictably for individual customers. The unpredictability is because what the access is always available, the infrastructure has a fixed bandwidth that is shared by multiple users. As more customers attempt to use that fixed bandwidth, the less is available for each individual customer. DSL is sometimes used as an "inexpensive" VPL access service for linkage to Best Effort services. DSL often also has an overall shared fixed infrastructure bandwidth

The core infrastructure is made up data switches or routers that are more often designed, built, and implemented based on a data centric paradigm instead of telephony centric paradigm. There has historically been a major difference in the attitude toward equipment and protocol reliability between these two paradigms. The telephony centric paradigm views reliability as paramount and part of the reduction of operational costs as well as the delivery of customer service level agreement requirements. The data centric paradigm often takes it for granted and sometimes actually requires a certain amount of "failure" within the network. This means that the data centric paradigm does not put as much emphasis on service availability as does the telephony paradigm. This translates into infrastructure architectures and implementations that have a relatively high amount of equipment and inter-link outages. Also when these outages occur, the restoration functionality of the best effort protocols are very much slower than the restoration functionality of a telephony centric paradigm, such as Private Line. Also because the best effort service architecture tends to be common between multiple service providers and countries, there are additional protocols that are involved with restoration of services between these as well. All of this translates into an availability that is greatly affected by equipment and link failures. This is very unpredictable, but can sometimes prevent service availability between sections in the core of the infrastructure for minutes, hours, or even days. While the overall infrastructure is operational, often customers are affected by these outages in ways that they have come to accept as part of the service.

Core infrastructure bandwidth, in addition to being effected by equipment and link outages, is also affected by "bandwidth engineering" within the service. Because the service uses restoration protocols that can attempt to force more service bandwidth on to links that are inadequate, specific engineering has to go into designing the links between the service equipment. In addition to providing for restoration bandwidth, often links are prioritized to distribute the service traffic to prevent "bottle-necks" within the infrastructure. When the bandwidth engineering is inadequate, then situations will occur where the customers' applications time out as if the service were not available at all. This is also a situation that the customers of Best Effort services have come to accept.

BE Reliability

Best Effort services are considered to be the least reliable of all of the data communications services provided. Data loss, at best, is right at as 10^{-2}, or 1% of the offered data traffic. Often, due to congestion within the Best Effort service infrastructure, data loss is 5% or higher. Most of the congestion data loss is at the access to core service interface, in the "statistical gain" component of the service access. Sometimes, when there is a fault within the core infrastructure, congestion can lead to additional data loss.

Most customers run applications that will retransmit data information that has been lost within the service infrastructure. This gives the applications the appearance of reliability at the cost of performance. The retransmission of the data also lends to a higher attempted usage of available bandwidth, until the applications can make use of "flow control" functionality based on the amounts of data that is being lost. The "flow control" functionality further degrades the applications' performance over the Best Effort services. The combination of data loss, retransmission, and flow control are a major component to customers' perception of the poor performance of Best Effort services.

BE Stability

Data stability within best effort services is very poor. The service systems are designed to buffer and queue up the data before it is sent on to the next location within the infrastructure. Often within each of the service systems there are several buffers and "store and forward" queues. Each of these buffer and queue functions adds variance to the latency of the data packets through the infrastructure. This latency variance can be as little as a few milliseconds to several hundred milliseconds. This makes it difficult if not impossible to pre-determine the latency of traffic for various applications across a loaded infrastructure. The non-deterministic nature of data delivery within this service creates a requirement within the customer applications to compensate for data latency variance by buffering the received data. The buffering and variance compensation degrades the performance of the applications that are run over Best Effort services.

BE Security

Within the Best Effort service there is very little security. Datagram and content encryption functionality is common and often included as part of the applications that are used over the Best Effort services. Firewalls are often put into place between customer data networks and the Best Effort service network to prevent unwanted intrusion, disruption of internal systems and other problems cause by outside "hackers". For the purposes of Federal wiretap requirements, all of the traffic of all of the customers must be examined in order to capture any one customer's traffic. Constant, spurious surveillance of all data traffic is common within service provider systems. Any type of real security for the data traffic must come from strong encryption of the datagrams within the customers' traffic before they are put on the service provider network.

BE Routing Autonomy

Best Effort services currently use a protocol that is fully autonomous in the way that data traffic is routed over the infrastructure. Internet Protocol (IP) is the most commonly used service protocol for this service. Along with the IP datagram packets as defined by the IP protocol standard from the Internet Engineering Task Force (IETF), other, routing protocols, such as Open Shortest Path First (OSPF), Routing Internet Protocol (RIP), and Internal System to Internal System (ISIS). These routing protocols autonomously tell the routers what path route for each of the customers' data packets to take, in order to reach the desired destinations.

BE Operations/Network Management

Operations and network management is in-band with the customers' data traffic. A data packet format protocol was specifically defined within the IP domain to carry operations and management messages to and from the infrastructure elements. This data packet protocol is called Simple Network Management Protocol (SNMP). SNMP packets are carried as part of the service bearing traffic with destinations to the Service Provider SNMP Network Management systems. In situations where there is congestion or faults in the network, the SNMP management messages are effected just as much as the customers' traffic. The availability issues that affect the customers' traffic also affect the network management traffic, making the network management of the Best Effort infrastructure somewhat less than 100% reliable or deterministic.

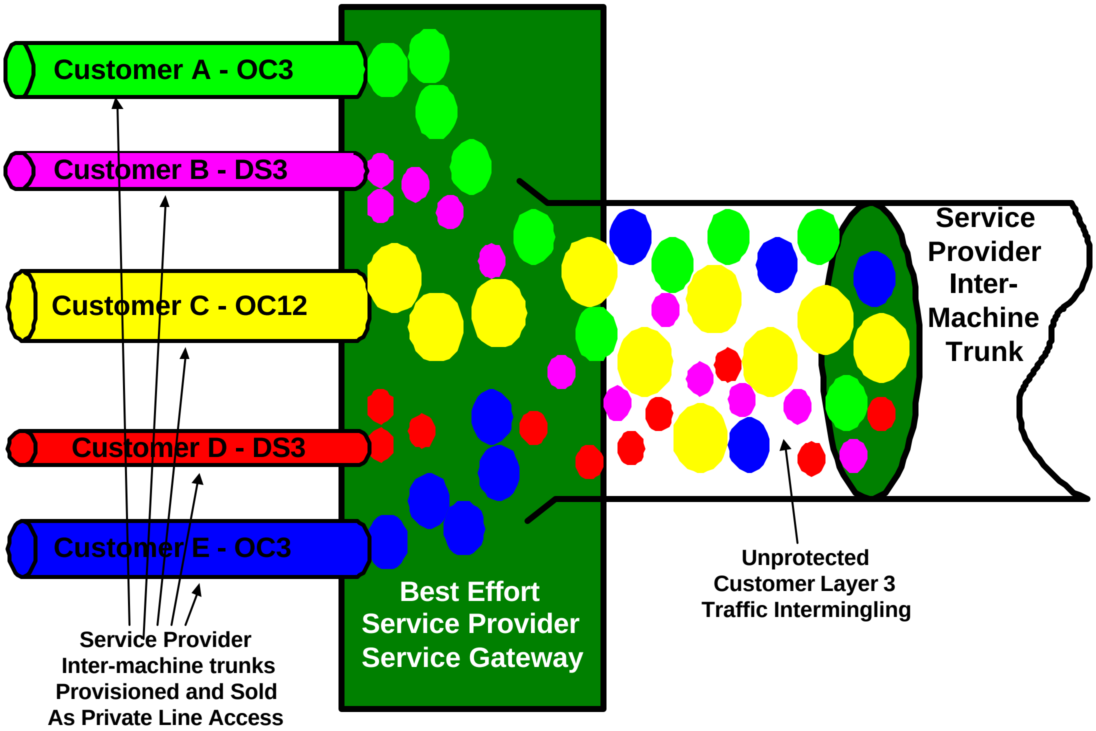
Customer A - OC3
Customer B - DS3
Customer C - OC12
Customer D - DS3
Customer E - OC3
Service Provider Inter-machine trunks Provisioned and Sold As Private Line Access
Best Effort Service Provider Service Gateway
Service Provider Inter-Machine Trunk
Unprotected Customer Layer 3 Traffic Intermingling

Figure 5 Best Effort Service Model

BE Customer Cost Structure

The cost of Best Effort services are very commodity drive and are often "flat rate" based on the basic access bandwidth. The cost per bandwidth is the least of any of the services. More often the cost of access to the Best Effort services costs more than the service does. Because of this, the Best Effort bandwidth has very little, if any margin within the service itself. Only through offering other services over the Best Effort service do service providers generate enough revenue over the costs of providing the service to be profitable.

BE Service Provider Margins

Margins on the Best Effort data communications service itself are the lowest in the industry. Some BE services are only charged at flat rate, regardless of usage. In some cases, only the access bandwidth is charged for, regardless of the customer application connection distance. Funding for capital and operations costs of providing BE data communications services are often subsidized by content and value added services that are provided over the BE communications service.

Best Effort Service Summary

Best Effort is a point to multi-point, non-connection oriented, Layer 3 service at fixed and burstable bandwidths over different Layer facilities depending on the service. Best effort tends to be un-secure data communications that is the least reliable and least stable of all of the services. The loss of data, data retransmission, and data latency variance compound to degrade the performance of applications that are used over Best Effort services, creating the perception that the service as a whole has very poor performance. Best effort bandwidth services are very commodity priced and have the least margin of all of the data communications services. It does, however, provide a facility to provide other value-added services to a wide variety of customers.

Virtual Private Networks

Virtual Private Networks (VPNs) are services over special cases of Best Effort service infrastructure networks. The VPN service attempts to add a certain amount of customer traffic insulation and Quality Of Service (QOS) within a common best effort Layer 2 (Ethernet) or Layer 3 (IP) infrastructure. The insulation of the customers' traffic is through the use of soft logical traffic direction (VLANs) within the Layer 2 VPN service and dedicated multi-cast addressing (MPLS) with traffic direction or datagram encryption within the Layer 3 VPN service. The apparent better than "best effort quality" of Ethernet (Layer 2 VPN) is because of the very reliable physical layer (PHY) that is standardized for Ethernet. The apparent better than "best effort quality" of IP (Layer 3 VPN) is most often based on having a dedicated infrastructure (non-Internet) that is bandwidth engineered to prevent congestion, reduce data loss, and reduce latency variance (Data Jitter). In some cases customers' will create their own VPN functionality within Best Effort services using their own datagram encryption to provide isolation security.

VPN Connection Type

VPN service connectivity is semi-connection oriented. The protocols that are used to provide VPN services are actually non-connection oriented. The use of soft traffic direction gives the service gateway devices the ability to direct the traffic to and from specific ports on the service gateways. The customers' data traffic is not encapsulated in a different protocol or another layer of the same protocol like it is with VPL services. Also the customers' traffic intermingles indiscriminately within the autonomous routing of the data traffic within the service infrastructure. Layer 2 (Ethernet) VPNs use dedicated service gateway systems located on the customer site to provide Ethernet connectivity to the customer's data switches. Layer 3 (IP) VPNs often uses reliable PL links to link the customer sites to the service gateway sites, or the service can use Ethernet VPN services to provide that connectivity.

VPN Bandwidth Types

The bandwidths available for VPN services are a complex as those of the Best Effort services. Many times the same access infrastructure that is used for Best Effort services is also used for VPN services. There is also an attempt to provide the same type of burstable GBA/BBA bandwidth as with the Best Effort services.

VPN Service Level

VPN services are most often provided through the use of Internet Protocol (IP) which is a Network Level (OSI Level 3) protocol. Even though Level 2 protocols such as Ethernet or MPLS are used for the customer interface, the service requires that the customer use IP. This is sometimes a cause of confusion because of the marketing label that is given to the specific service provider's implementation of the service.

VPN Infrastructure Level

Ethernet (Layer 2) VPN service uses Ethernet Switches that are inter-connected by a dedicated fiber infrastructure to connect the customer sites to other service gateway sites and to each other. This dedicated fiber infrastructure functions to by-pass the Incumbent Local Exchange Carrier (ILEC) copper and fiber access infrastructure, thus avoiding a major cost of providing competitive data communications services to customers. IP (Layer 3) VPN services are based on IP dedicated IP routers that are inter-connected over dedicated inter-machine trunks, provisioned over the same infrastructure as PL. The local access infrastructure can and often uses the ILEC access infrastructure. In some cases dedicated ILEC by-pass infrastructure is used.

VPN Availability

The availability of VPN services is very dependent on the type of VPN service. Where the VPN service is actually a data encryption over dial up Best Effort services, then the availability of the VPN is limited to that of the dial up Best Effort services. Where the VPN is provided over dedicated infrastructure, then the availability is relative to the availability of the access type/infrastructure, the core infrastructure implementation, and the congestion that the engineered bandwidth allows on the core infrastructure. The complexity of the components to the VPN availability normally prevents any stringent service level agreements from being made by the service providers. Under normal circumstances, VPN availability over dedicated infrastructure is slightly better than it is for Best Effort services.

VPN Reliability

Most often there are no data delivery/reliability service level agreements given to VPN customers. Data reliability is very dependent on the infrastructure that the service is implemented over. Even in the best case, over dedicated infrastructure, VPN data loss can be as low as 1%. Over specially engineered infrastructures, the data loss may be less. Operating as data encryption over Best Effort services, the data reliability is no better than what is delivered over the Best Effort service infrastructure.

VPN Stability

VPN data stability is very dependent on the infrastructure implementation that is run over. Where the VPNs are run as encrypted data over the Best Effort network infrastructure, data stability is no better than that of the Best Effort service. In addition to the latency variance of the Best Effort service infrastructure, the encryption/decryption processing of the data causes additional latency variance. All of this latency variance translates to perceived application performance problems just like the Best Effort services.

Sometimes dedicated infrastructures, that are engineered and provisioned to be non-congested networks, are used for VPN services. On these dedicated infrastructures, data stability is better than it is with the Best Effort services. There is also a priority queuing functionality within the some VPN service implementations that allow some service types to have a slightly lower latency variance than other service types. This is often referred to as a QOS or a "Diff-Serve" function.

VPN Security

While customers do not commonly have access to other customers' traffic, all of the customer data traffic is available to the service provider. For the purposes of Federal wiretap requirements, all of the traffic of all of the customers must be examined in order to capture any one customer's traffic. Any type of real security for the data traffic must come from strong encryption of the datagrams within the customers' traffic before they are put on the service provider network.

VPN Routing Autonomy

Service traffic routing is done autonomously over the Best Effort infrastructure that it is implemented over. Some of the dedicated infrastructure implementations have manually configured static routes to do traffic shaping. Other implementations have route prioritization mapped to switched Layer 2 networks that tend to provide a certain amount of limiting of the normal autonomous routing done on the Best Effort infrastructure.

VPN Operations/Network Management

Operations/Network management of VPN service infrastructure is the same as the Best Effort network infrastructure it is implemented over. Most VPN services use SNMP as the primary operations and network management protocol. Also, like the Best Effort services, the service providers' operations/network management traffic is in-band with the customers' revenue bearing traffic.

VPN Customer Cost Structure

The cost of VPN services for customers' is somewhere between the Best Effort services and the Virtual Private Line services. VPNs provide customers with a slightly more secure version of Best Effort services without the costs of Private Line or Virtual Private Line services. The cost of capital equipment to support VPN services, in most cases, is the same as the Best Effort services, since they are using the type of infrastructure. For data encrypted VPNs, often it is only a software investment instead of a hardware investment. For better performance or for support of data encryption from multiple users, dedicated hardware systems can be implemented that will support relatively high bandwidth VPN services. These encryption systems add to the cost of the services from the customer's point of view.

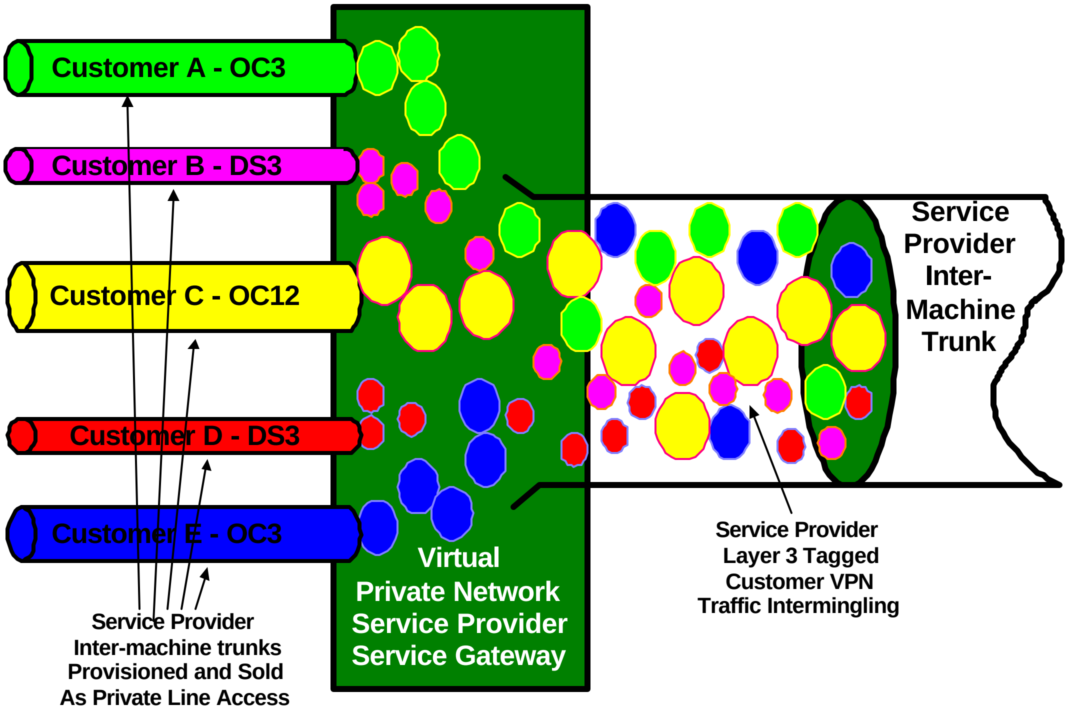
Customer A - OC3
Customer B - DS3
Customer C - OC12
Customer D - DS3
Customer E - OC3
Service Provider Inter-machine trunks Provisioned and Sold As Private Line Access
Virtual Private Network Service Provider Service Gateway
Service Provider Inter-Machine Trunk
Service Provider Layer 3 Tagged Customer VPN Traffic Intermingling

Figure 6 Virtual Private Network Service Model

VPN Service Provider Margins

VPN services have moderate to moderately low margins. VPN services have higher margins than the Best Effort services because of the additional value created by the security and virtual connection functionality. VPN services use the same infrastructure as BE services so the cost of providing the service is only slightly higher than BE services. VPN services should not require subsidy from content or other value-added services to be profitable.

Virtual Private Network Service Summary

Virtual Private Networks are a special class of services that are point to multi-point, non-connection oriented over Layer 2 or Layer 3 facilities. In many ways VPNs are simply more secure versions of Best Effort services with slightly better reliability and data stability. Unlike Private Line, and like Virtual Private Line, Virtual Private Networking allows transmission core bandwidth to be shared at the data level, instead of the multiplexed physical time domain level. Unlike Virtual Private Line services, however, Virtual Private Network Services do modify or directly use the customers' data packets/frames for routing or performance monitoring. VPNs are not considered as commodity services, which gives them slightly higher margins than simple Best Effort, although the costs and complexities are higher. VPNs also gives the opportunity to provide some specific valued added services to specific customers.

Existing Service Infrastructure Stack

Like the OSI Model the infrastructure layers under the various service are layered on top of each other. The existing infrastructure for all of the existing services has been in place for some time. The basic Layer 1 infrastructure under all of the existing services is the TDM/SONET/SDH inter-machine trunks. Above the Layer 1 inter-machine trunks, is the Layer 2 (ATM & PPP) and Layer 3 (IP) infrastructures of the other services, Virtual Private Line and Best Effort. Above the Layer 3 infrastructure for Best Effort services is the Virtual Private Line (MPLS & data encryption) functionality.

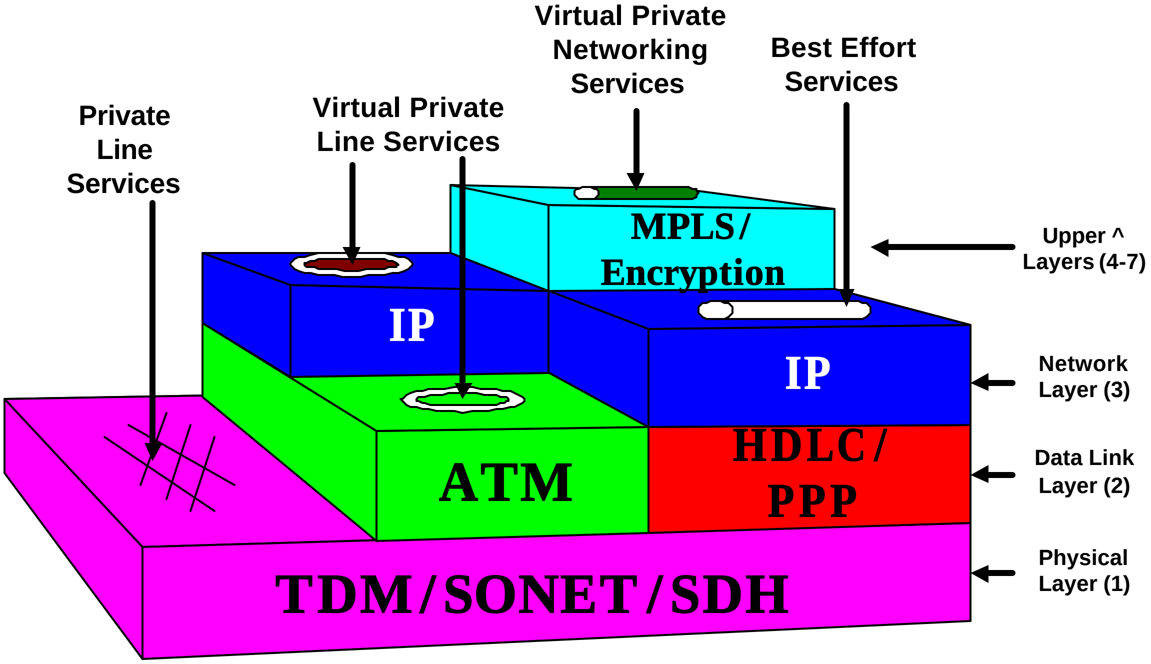

Figure 7 Existing Services Models Infrastructure Stack

The fixed bandwidth and other features of the TDM infrastructure used for PL services gives the ability of the designers and implementers of the other service infrastructures to design architectures against the known functionality of the TDM infrastructure. Without deterministic and predictable availability, reliability and bit level latency the stability of the protocols used for the other service infrastructures would be even less predictable and dependable than they currently are. The fixed, deterministic nature, of the Layer 1 TDM infrastructure is taken for granted so much by the individuals designing, implementing, and supporting the other service infrastructures and protocols that many of the protocol standards do not even mention specific Layer 1 operations functionality requirements. Only some limited bandwidth and physical media functionality is mentioned by the ATM and PPP standards. This is a common characteristic of the protocols normally recognized for use in Wide Area Networks (WANs) which are used the existing VPL, BE, and VPN services.

Best Effort and VPN services today use Internet Protocol (IP) which functions at the Network Layer (OSI Layer 3). The service protocols and the customer protocols are the same. The standards authority for IP is the Internet Engineering Task Force (IETF). The

IETF has a very large library of protocol standards called Request for Comment (RFC) documents. These documents define the inter-operability of each function, sub-layer and addressing assignment relating to IP and the Transmission Layer (OSI Layer 4) protocols of User Datagram Protocol (UDP) and Transmission Control Protocol (TCP). The Data Link Layer (OSI Layer 2) protocol which has been defined as normal use for IP is Point to Point Protocol (PPP). PPP does not specify Physical Layer (OSI Layer 1) functionality other than the use of the existing TDM/SONET/SDH network infrastructure. The IETF has also defined the use of Multi-Protocol Label Switching, a form of a Data Link Layer (OSI Layer 2) protocol. MPLS does not specify a Physical Layer (OSI Layer 1) function, so is still dependant on the existing TDM/SONET/SDH network infrastructure.

Virtual Private Line services provide transport for the customers' ATM and Frame Relay (FR) protocol data traffic. ATM and FR are both Data Link Layer (OSI Layer 2) protocols. In the case of FR, the customers' traffic is encapsulated into another, unrelated protocol. Sometimes the encapsulation protocol is actually a Network Layer (OSI Layer 3) protocol (IP), a protocol that functions at a higher layer than the customers' service protocol. In some cases the encapsulation protocol is ATM. For the ATM services, most often ATM is used for the encapsulation protocol. The customers' ATM data traffic is completely encapsulated into the payload bytes of the service providers' ATM traffic. The Physical Layer (OSI Layer 1) transport function of ATM is specified as the TDM/SONET/SDH infrastructure. Even in cases where ATM is used under IP, the Layer 1 transport remains the TDM/SONET/SDH network.

An interesting observation about the services infrastructure stack is that the more ubiquitous Best Effort service has the most complex implementation infrastructure. The more customer specific service of Private Line has the most generic infrastructure. This is an inverse function of complexity and common ubiquitous access.

Future Infrastructures and Services Within the Service Models

In spite of efforts to create new service models, or migrate some existing service models to other service model infrastructures, the ultimate judge of the viability of the service models are the data communications customers. In spite of the expansion of very low cost Best Effort services in the past few years, high cost Private Line has remained a viable, high margin, service model. Based on this, it is unlikely that a major change can be made to the existing service models themselves. What can be done is change the customer interface, and possibly change the specific infrastructure under specific service models based on the new interface.

Because of the lower capital costs to the customer for the data communications support systems, Ethernet has become dominant as the enterprise Local Area Network (LAN) infrastructure. The specification of Layer 1 functionality is very different between the traditional protocols used for data communications services, and the protocols normally considered to be used only for LAN implementations. When the IEEE 802.3 working group developed the optical based Physical Layer (PHY) specifications for 1000BaseLX (Gigabit Ethernet, GbE) the distinctions between the LAN and WAN infrastructures have diminished. GbE was considered by its designers to be an extended campus enterprise protocol. Since it was formally ratified, GbE has been used to implement metropolitan data communications services infrastructures. While this does not change the nature of the Generic Data Communications Service Models; it does create additional confusion about the distinctions between services and infrastructures.

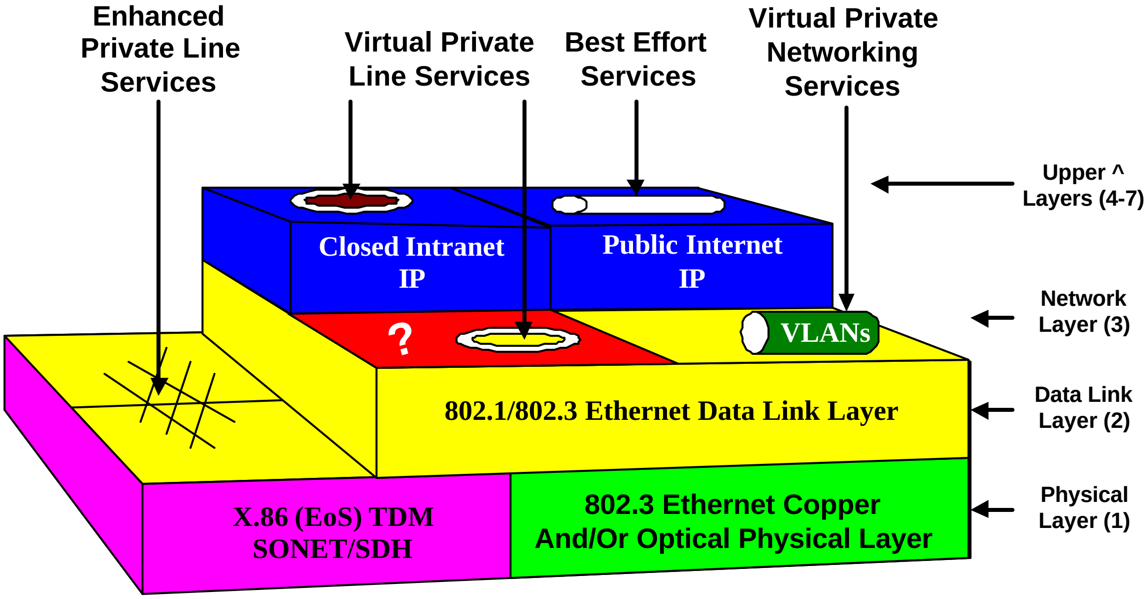
Enhanced Private Line Services
Virtual Private Line Services
Best Effort Services
Virtual Private Networking Services
Upper ^ Layers (4-7)
Closed Intranet IP
Public Internet IP
Network Layer (3)
?
VLANs
802.1/802.3 Ethernet Data Link Layer
Data Link Layer (2)
X.86 (EoS) TDM SONET/SDH
802.3 Ethernet Copper And/Or Optical Physical Layer
Physical Layer (1)

Figure 8 Possible Future Services Infrastructure Stack For Ethernet Based Services

With the development of 10000BaseWX (10Gigabit Ethernet WAN PHY, 10GbEWAN) Ethernet, which has previously considered to be a LAN only protocol has implemented data communications services specific functionality. This makes Ethernet into a Wide Area Network (WAN) protocol, in addition to being a LAN protocol.

While Ethernet is considered to be the most widely deployed LAN protocol in the world; most people are not aware that 98% of the document that defines 802.3 Ethernet is actually dealing with providing a very reliable physical media layer (Layer 1) functionality. With Ethernet able to be implemented as WAN based infrastructure, and with a specifically defined reliable Layer 1 functionality, the traditional TDM/SONET/SDH common infrastructure may no longer be the only common service infrastructure deployed globally.

Like all services, data reliability is based on the underlying layers of infrastructure and the bandwidth management within the service. With services over Ethernet infrastructure, the defined Physical Layer reliability provides for added data service reliability. In the case of Ethernet VPN services, the data loss should be about 10^{-5} or less, because of the dedicated fiber optic infrastructure it operates over. Ethernet infrastructure supported IP service VPNs will also tend to have better stability than other infrastructure technologies because Ethernet, as an infrastructure technology, has lower latency variance than any of the other technologies that might be used.

What does not change with Ethernet as the service infrastructure is the generic models of the data communications services provided, or the customer service interface. The traditional Private Line services still function the same as over the traditional network infrastructure. For high bandwidth services, Private Line becomes individually provisioned wavelengths over an optical service network. For lower bandwidths, Ethernet will map directly into the existing TDM infrastructure payloads for transport over the traditional SONET/SDH infrastructure. Just as with the other services using the traditional TDM SONET/SDH network to provide inter-machine trunks as circuit links between the various service gateway systems the Ethernet infrastructure will provide inter-machine trunks to act as circuit links between the various service gateways.

One distinction is that Ethernet has a function that is used to insulate the data communications traffic for specific groups of users within Virtual Local Area Networks (VLANs). This is much the same as the traditional VPN service functionality. The distinction with using Ethernet as a VPN infrastructure is the limitation on the number of VLANs that can be implemented in any one system or domain. This creates a scaling limitation for Ethernet VPNs. This scaling limit can be overcome by providing IP services or IP VPNs over the Ethernet infrastructure and doing IP routing between different Ethernet VPN infrastructure domains. A few customers can be provided direct Ethernet VPN services, but their numbers will be limited. The distance between the specific customer sites will also be limited to a common VPN domain infrastructure within a metropolitan service area.

Virtual Private Line service using Ethernet as the service protocol is still in question. At present, because of the flat network switching functionality defined for Ethernet, the ability to use Ethernet as a direct VPL service infrastructure is limited. There are efforts by vendors to develop the technology that will provide for Ethernet Interface VPL services. Frame Relay, which often uses IP as a Virtual Layer 1 infrastructure, can still use the IP Network Layer infrastructure over an Ethernet Data Link Layer infrastructure.

Generic Data Communications Services Summation

Data communications services are a specific segment of the services provided by diverse group of communications service provider companies. Within that segment, based on a comparison of their characteristics, these services can be separated into four distinct generic models.

Private Line Service Model

Private Line is a fixed bandwidth, point to point, connection oriented, Layer 1 service over physical Layer 1 facilities. Private Line Services segregates each customer's traffic within fixed physical and fixed time domain leased facilities. The aggregated time domain facilities are multiplexed into a larger transmission core bandwidth to share the high bandwidth transmission facilities. It provides the most reliable, stable, and secure data communications available. PL is a costly yet extensively used service with high margins the service provider.

Virtual Private Line Service Model

Virtual Private Line is a point to multi-point, connection oriented, Layer 2 service at fixed and burstable best effort bandwidths over Physical and virtual Layer 1 facilities. It provides secure data communions that are moderately reliable and moderately stable. Unlike Private Line, Virtual Private Line allows transmission core bandwidth to be shared at the data level, instead of the multiplexed physical time domain level. Unlike Virtual Private Network Services, Virtual Private Line does not modify or directly use the customers' data packets/frames for routing or performance monitoring. The local access only distance charges provides a major savings to the customer. The statistical multiplexing and access service bandwidth to core bandwidth ratio also provides an opportunity for additional billable functionality to service provider, creating moderately high margins.

Best Effort Service Model

Best Effort is a point to multi-point, non-connection oriented, Layer 3 service at fixed and burstable bandwidths over different Layer facilities depending on the service. Best effort tends to be un-secure data communications that is the least reliable and least stable of all of the services. The loss of data, data retransmission, and data latency variance compound to degrade the performance of applications that are used over Best Effort services, creating the perception that the service as a whole has very poor performance. Best effort bandwidth services are very commodity priced and have the least margin of all of the data communications services. It does, however, provide a facility to provide other value-added services to a wide variety of customers.

Virtual Private Network Service Model

Virtual Private Networks are a special class of services that are point to multi-point, non-connection oriented over Layer 2 or Layer 3 facilities. In many ways VPNs are simply more secure versions of Best Effort services with slightly better reliability and data stability. Like Virtual Private Line, Virtual Private Network Services allows transmission core bandwidth to be shared at the data level, instead of the multiplexed physical time domain level. Unlike Virtual Private Line Services, Virtual Private Network Services do modify or directly use the customers' data packets/frames for routing or performance monitoring. VPNs are not considered as commodity services, which gives them slightly higher margins than simple Best Effort although the costs and complexities are higher. VPNs also gives the opportunity to provide some specific valued added services to specific customers.

Generic Data Communications Services Model Comparisons

In this presentation, there are 12 characteristics that used to compare these service models. The following table provides a comparison of the service models based on those characteristics:

Service Criteria	Private Line	Virtual Private Line	Best Effort	Virtual Private Network
Connection Type	Connection Oriented	Connection Oriented	Connectionless Oriented	Connectionless Oriented
Bandwidth Type	Fixed	Fixed and Bustable	Burstable	Burstable
Service Level	Level 1	Level 2	Level 3	Level 3 *

Infrastructure Level	Level 1	Virtual Level 1	Level 3	Level 3 Virtual Level 3*
Availability	High	Moderate	Low to High	Moderate to High
Reliability	High	Moderate	Low	Moderate
Stability	High	Moderate	Low	Low
Security/ Segregation	High/ Fixed Time Domain	High/ Full Encapsulation	Low/ No Segregation	Moderate/ Header Modification/ Encryption
Routing Autonomy	Fixed	Fixed PVC Self Autonomous	Self Autonomous	Self Autonomous
Operations/ Network Management	Out of band	Out of band to customer revenue traffic **	In band to customer revenue traffic	In band to customer revenue traffic
Customer Cost Structure	High with distance chgs	High without distance charges	Low, No distance chgs	Moderate, No distance chgs
Service Provider Margin	High	High Moderate	Low	Low Moderate

Notes on Generic Data Communications Services Models Table
* Virtual Private Network IP service over IP MPLS or Ethernet VLAN infrastructure
** Virtual Private Line operations/network management is out of band to the encapsulated customer data traffic, in band to the protocol that is used as the encapsulation infrastructure.

These Generic Service Models and Future New Technology

As new data communications technologies become available, new services specific to those technologies may be created. The generic service models that are defined here can most likely be applied to those new technology services as well. The understanding that data communications services should not be confused with the data communications infrastructure is important to understanding the specifics of the data communications services. The same data communications infrastructure that is used for data communications services is also used for content and other value added services. In spite of all of the differences between the different service models, there are basic infrastructure functions that are common to all of them. There is also a basic infrastructure that provides the reliable physical layer transport for all services, data communications and value added. At present that reliable infrastructure is the TDM based SONET/SDH transmission network. In the future the lowest level of common service infrastructure may be an automatic switched optical network technology. The reliable functionality of that level of common transport infrastructure will not change regardless of new communications technologies that develop over the years.