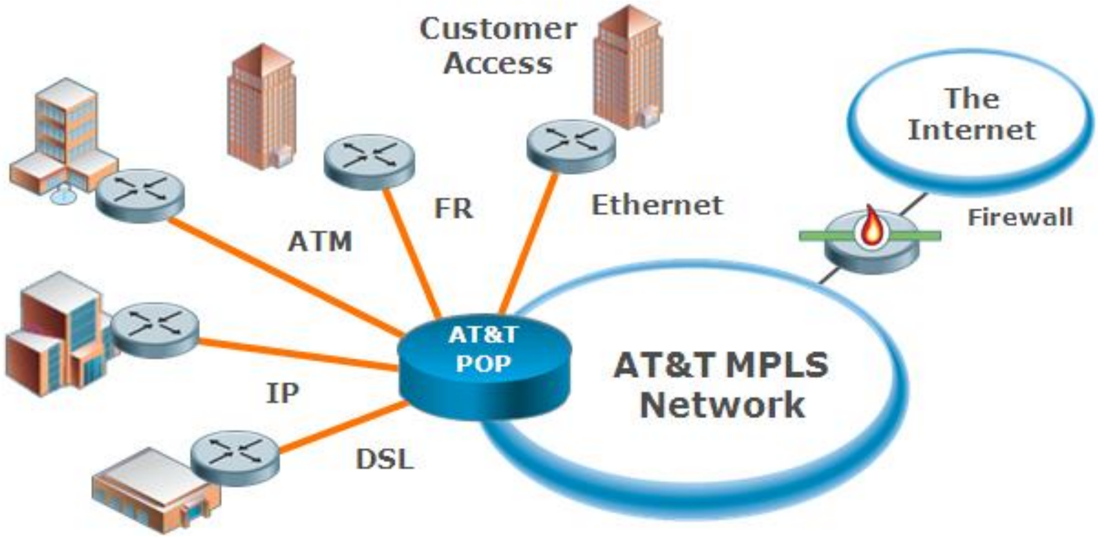
AT&T Virtual Private Network (AVPN) Service

I. Service Overview

II. Service Components, standard and options



I. Service Overview

AT&T Virtual Private Network (AVPN) is a network-based IP VPN solution that is enabled by Multiprotocol Label Switching (MPLS). AVPN is the evolutionary successor to the IP services which began with IPeFR/ATM. AVPN service enables Customers to build an application aware, network-based MPLS virtual private network to link locations and efficiently transmit applications such as voice, data, and video over a single connection.

Customers have the option of choosing the access method to AVPN which best meets their requirements. ATM, Dedicated Private Line and Frame Relay may all be used to connect to an MPLS port. DSL and Ethernet (where available) may also be used. . In addition to a range of port types, AVPN also supports a variety of router ownership and management options.

AVPN uses MPLS standards and brings efficient, secure, and scalable way to support critical IP applications. AT&T can say that our MPLS implementation is fully compliant with RFC3031 (MPLS ARCHITECTURE), but more accurately, we are compliant with RFC2547bis, now been replaced by IETF standard RFC4364. RFC4364 describes a method by which a Service Provider with an IP backbone may provide VPNs (Virtual Private Networks) for its customers (MPLS). ***AT&T Labs is the co-author of both the acknowledged MPLS VPN industry-standard RFC2547bis and its replacement RFC4364.*** Additionally, AT&T's MPLS network is fully compliant with RFC 3032 (MPLS LABEL STACK ENCODING), RFC 3036 (LDP SPECIFICATIONS), RFC 2702 (REQUIREMENTS FOR TE OVER MPLS).

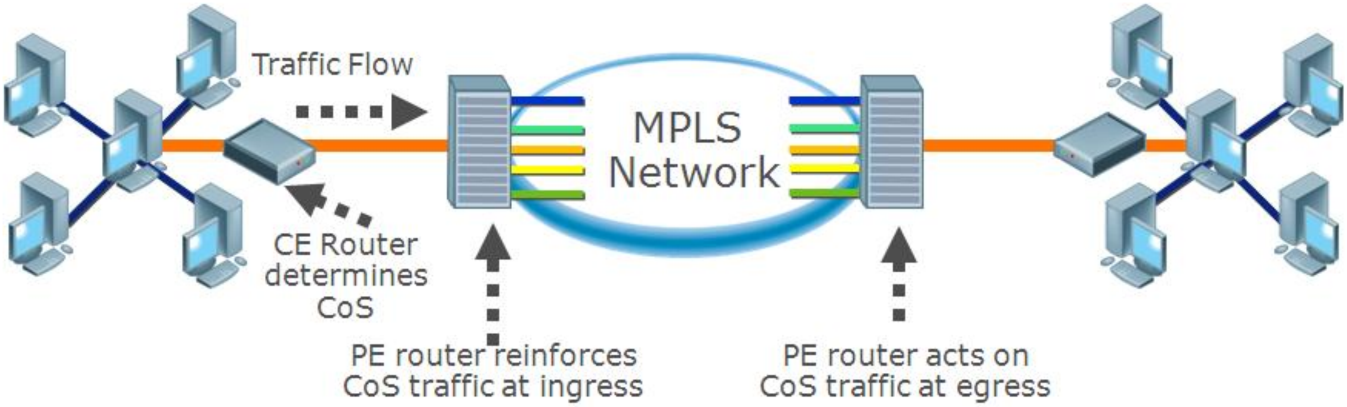
Customers looking for simplified fully-meshed communications and those with a need for distributed communications now have a simple solution that provides the best of both worlds—the flexibility of IP access and the inherent security and reliability of Frame Relay / ATM.

II. Service Components, standard and options

To use AVPN at Customer Sites located in the US, Customer must obtain access between each Customer Site and an AT&T POP, using clear channel digital dedicated access facilities obtained by Customer from AT&T or from another provider, or using another access arrangement compatible with AVPN.

The two primary benefits of AVPN are:

- **Any-to-Any connectivity** – All Customer AVPN sites that are part of the same VPN can communicate with each other regardless of the types of AVPN Ports at the different Customer Sites.
- **Prioritization of traffic** – Customers can choose from six different network-based class of service (CoS) to prioritize traffic. They are **CoS1** (for real-time applications like VoIP), **CoS2** (for critical data applications), **CoS2V** is a specifically intended to support video applications, **CoS3** (for business data applications), and **CoS4** (for standard data applications), with the default being CoS4 if a CoS is not defined, **COS5** is a 'scavenger' class intended to support non-critical applications.


Traffic Flow
MPLS Network
CE Router determines CoS
PE router reinforces CoS traffic at ingress
PE router acts on CoS traffic at egress

AVPN Standard Components

The required/standard AVPN Service Components are WAN Access between Customer Edge Router (CER) and Provider Edge router (PER) and MPLS Ports. Each MPLS port includes a logical channel connection to the customer's VPN.

The CER may be provided and managed by the customer, provided and managed by AT&T or under Premium Services, provided by AT&T and managed by the customer.

AVPN with AT&T-owned and Managed Router has the following router options (as of June 2011):

Basic:	Cisco IOS 1841 or Cisco IOS 2801
Small:	Cisco IOS 2811
Medium:	Cisco IOS 2821
Large:	Cisco IOS 3825
XLarge:	Cisco IOS 3845
XLarge+:	Cisco IOS 7206
XX Large:	Cisco IOS 7304

AT&T Virtual Private Network (AVPN) Service

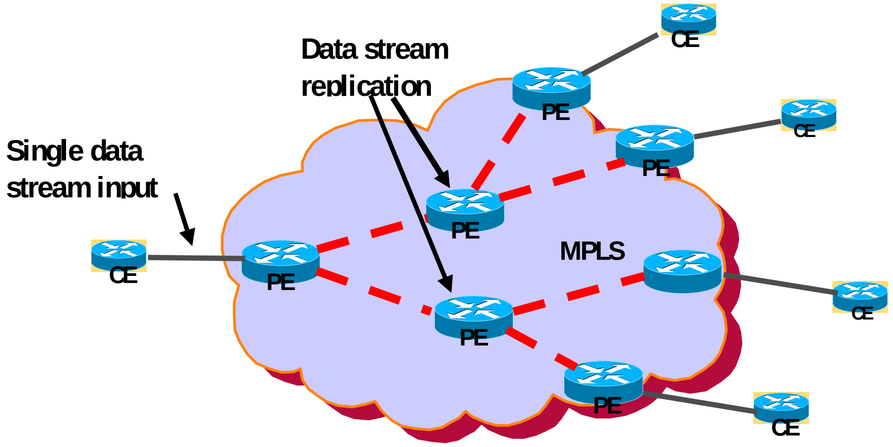
AVPN Optional Components

AT&T offers a variety of options that can enhance AT&T VPN, the most commons ones are:

- **Class of Service** (4CoS & 6CoS) - allows customers to prioritize their traffic based upon the type of traffic or application and their performance requirements. The CoS Profile defines the bandwidth allocation for each CoS, as indicated in the **CoS Profile Bandwidth Allocation Table.**

CoS Package	Classes of Service Supported
Multimedia High	CoS1, CoS2V, CoS2, CoS3, CoS4, CoS5
Multimedia Standard	CoS1, CoS2V, CoS2, CoS3, CoS4, CoS5
Critical Data	CoS2, CoS3, CoS4, CoS5
Business Data	CoS3, CoS4
Standard Data (None specified, or Default)	CoS4

- **Multicast** - Allows a Customer to send data from one MPLS Port to multiple Customer MPLS Ports (instead of sending individual unicast packets to each destination) within a Multicast enabled VPN.



- **Unilink** - Allows customers to order up to twelve (12) multiple Logical Channels on a single MPLS port. These multiple Logical Channels can be used for one or more VPNs.
- **MPLS Port Service Diversity (SDO)** - assigns multiple ports onto different switches in the same central office.
- **MPLS Port PoP Diversity (PDO)** - puts multiple ports into different central offices (usually different cities).
- **IPv4/IPv6 Dual Stack** - Fundamentally: a new packet header with a larger address space. Strategically: an enabler of new network-based capabilities that previously had been difficult or impossible with IPv4. IPv6 provides: Larger address space, New fields, Standard packet header options