Request for Information (RFI)
On
Frame Relay to MPLS Migration

RSVP Deadline: **May 16, 2005** e-mailed or postmarked by 5 p.m. (ET)
RFI Deadline: **May 31, 2005** e-mailed or postmarked by 5 p.m. (ET)
Publication Date**:** ***August 4, 2005***

I. Introduction

A. Purpose

This RFI (Request for Information) is proprietary to Network Computing and CMP Media, LLC. It is drafted and disseminated for the sole purpose of generating information on Frame Relay migration to an MPLS network for publication in Network Computing on August 4, 2005. Participating vendors must meet the minimum requirements for participation and agree that any information returned to Network Computing in response to this RFI may be published in print and electronic form on our Web site, www.networkcomputing.com.

B. Instructions

The following minimum requirements are essential to participate in the Frame Relay migration to MPLS review.

Please note: Services proposed in this RFI **MUST** be available at time of your response. No beta services, please. We reserve the right to examine a test unit (either in our lab or at a customer site) of any service proposed.

___ WAN services proposed must be available in all listed locations (through partnerships is OK).
___ MPLS-provisioned services must comprise at least part of the proposal.

If you do not meet the preceding criteria, your product does not meet the minimum qualifications for this review. Please RSVP by May 16 to Bruce Boardman (bboardman@nwc.com). Thank you for your consideration.

If you respond to the RFI, please note the dates in Section I.C to complete the RFI on time for inclusion in our Aug. 4 issue. We suggest you read through the entire RFI before answering questions. You can reference answers to other questions in the RFI using the section and question number. Please do not reference materials outside the RFI; incorporate them into your answers. This RFI will be the **only** source used to compare the participating services.

Essay-type questions include word-count limits. Any submission beyond the limit may be ignored.

Please answer all the questions in light of Sections II through V. These sections lay the foundation on which to base your answers, which will determine the winning bid and our Editor's Choice Award. If you have questions, please contact Bruce Boardman bboardman@nwc.com.

C. Effective Dates

RFI Issue Date: April 22, 2005
RSVP Deadline: May 16, 2005 e-mailed or postmarked by 5 p.m. (ET)
RFI Submission Deadline: May 31, 2005 e-mailed or postmarked by 5 p.m. (ET)
Publication Date: August 4, 2005

II. Business Overview

TACDOH Corp., worldwide purveyors of deep-fried delights, has an aging Frame Relay network linking its 100-plus sites. Employee productivity is a critical TACDOH competitive advantage and is fuel by a well-connected network and application infrastructure. In the past the current hub-and-spoke Frame Relay network served TACDOH's data needs well, but now an increasing rate of change and the need to leverage network dollars mandate a complete network redesign. TACDOH is searching for a new network strategy and design and is very interested in the flexibility and much-heralded cost savings of MPLS.

Change and growth are key elements the new network will have to support. Maintaining site connectivity and application support are crucial; in addition, the winning RFI will support the increasing changes forced onto the TACDOH network.

The network supports voice, video, SAP transactions and Lotus Notes. Voice includes IP trunking as well as telephony for call processing. Voice and Video conferencing is accomplished using Polycom units at each location and occasional video streaming for companywide broadcast events. SAP transactions are high-priority traffic, requiring reliable and consistent processing, while the Lotus Notes collaboration uses store-and-forward messaging and background replication. Additionally, TACDOH runs its own instant messaging server and supports employee access to the Internet. Internet traffic, however, is regionally filtered and monitored, in accordance with corporate policy.

Service levels are applied to two areas: network performance and service delivery. Network performance is defined as metrics like availability, jitter, error rate and throughput. Service delivery is focused on guarantees associated with the time it takes to install new sites, dispatches to customer premises, escalation of out-of-service conditions and so on. The winning service provider will explain in detail the types of service levels available and any associated quantifications, like percentage of uptime.

In addition to supporting and improving the service delivery and provisioning cost of its existing applications, TACDOH is seeking other ways to improve costs and service. To this end TACDOH is interested in other services available from each provider that may not be specified in this RFI, or considered part of TACDOH's initial conversion, but are recommended as a future network enhancements. Vision to outsource IT infrastructure services, cost-appropriate connectivity, redundancy, management, security and even extending network services to TACDOH customers are possible suggestions for fulfilling this partnership vision. Anything that better leverages TACDOH's network investment or core business will help the company choose a provider with which to partner.

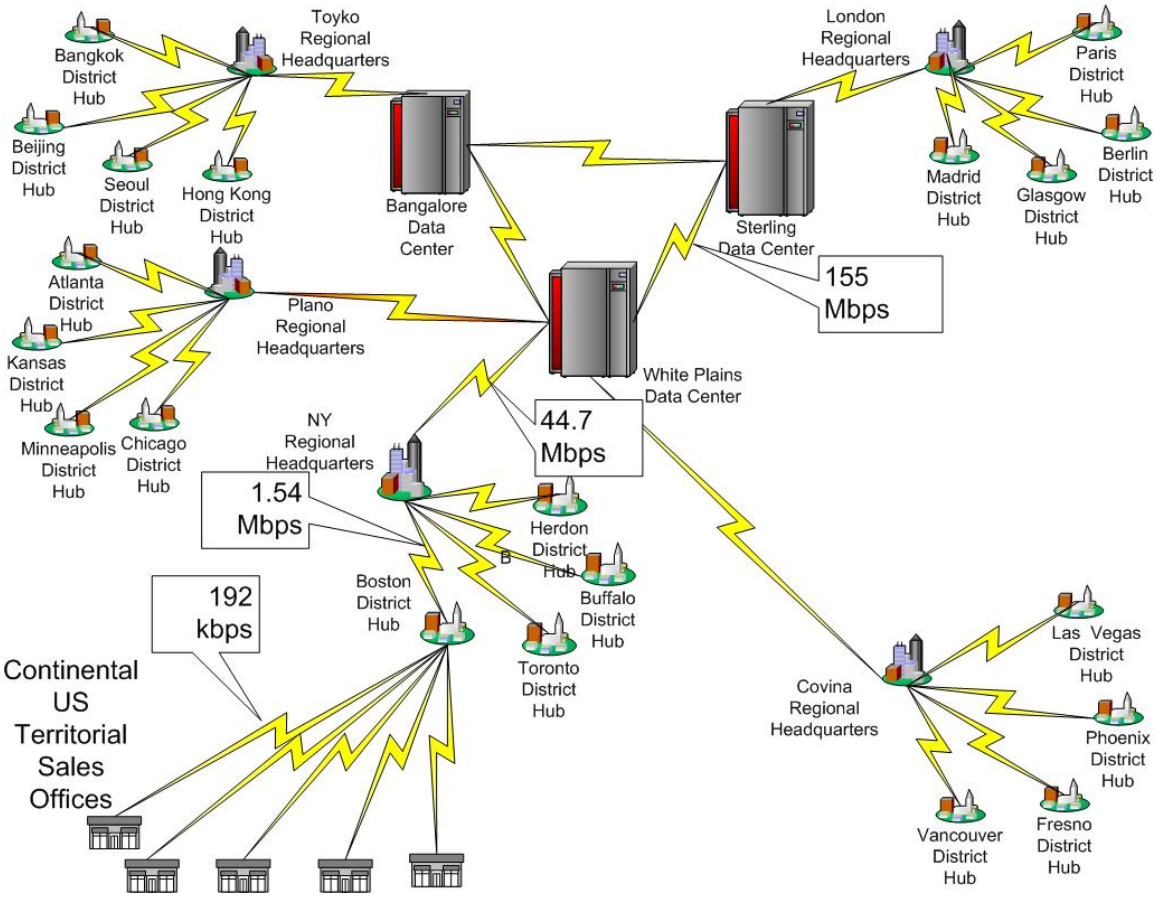
TACDOH is growing into new areas and requires a geographical coverage explanation from each service provider. The granularity should list world regions that are part of the service provider's native coverage and regions that will be covered using partners. In the case that more than a single partner relationship exists please list all available.

Finally, because TACDOH's network connectivity and services are so critical to the success of its enterprise, the financial health and technical infrastructure of each service provider is important. The most favored responses will demonstrate all of these areas, providing sales, customer references, financials and MPLS network connectivity in core and access network tiers.

III. Current Network

TACDOH currently has 128 sites, all linked with Frame Relay. Of these 114 sites are in the continental U.S., while the remaining 14 are located internationally. The top of this hierarchal network has **3 Data Centers**, connected to **5 Regional Headquarters**. Below and connected to the Regional Headquarters are **20 District Hubs**. At the lowest level connected to the District Hubs are the **100 Territory Sales Offices**.

Each data center is meshed with the other two other data centers, requiring two 155 Mbps connections for each. Each data center also has one or two downstream regional headquarters, each connected at 44.7 Mbps. Each regional headquarters has four district hubs, each connected at 1.54 Mbps. Each district hub has five 128 Kbps connections to the downstream territory sales offices.



As the traffic flows towards the data center it is aggregated.

A. Network hierarchy – Current total network sites equal 128 with the following breakdowns:

1. Connectivity

a) Data Centers – 3 - 155 Mbps OC3 connectivity with each data center connected to the other two.

b) Regional Headquarters – 44.7 Mbps T3/E3 connectivity to one data center and 2 district hubs

c) District Hubs – 1.54 Mbps T1/E1 connectivity to 1 regional headquarters upstream and 4 territory sales offices downstream

d) 100 Territory Sales Offices –192 kbps – All 100 sales offices are within the continental US and connected to US only District Hubs.

2. Distribution

a) Continental US = 114 total

1. Data Center = 1
2. Regional Head Quarters = 3
3. District Hubs = 10
4. Territorial Sales = 100

b) International = 11

1. Data Center = 2
2. Regional Head Quarters = 2
3. District Hubs = 10
4. Territorial Sales Offices = 0 (Internationally Territorial Sales offices are housed within District Hubs).

B. Applications supported on all circuits

1. Voice

a) IP Trunking
b) IP Telephony

2. Periodic Video Conferencing

3. Periodic Video Broadcasts

4. IBM Notes - including mail and database replication

5. SAP – Important real-time online transactions

6. Batch off hour data backup

C. Service Level Requirements

1. Technical Service levels

a) 99.99% uptime

1. Data Centers
2. Regional Headquarters
3. District Hubs

b) 99.95%

1. Territory Sales Offices

2. Service Delivery

a) New service turn-ups and service moves, especially as related to IP Telephony is critical.

b) Historical and anticipated change activity is as follows:

1. Personnel transfers requiring data and telephony – 500 annually
2. New sales offices – 10 annually for next 3 years
3. New District Hubs – 1 annually for next 3 years

D. Internet access

1. Centrally managed at each data center

2. Allowable protocols

a) HTTP
b) HTTPS
c) Instant Messaging

3. Browsing destinations controlled through categorization and filtering software

E. Network backup

1. Must be automated

a) Start and stop
b) usage sensitive in order to mitigate cost

2. Can include a mix of public and private network options with less important or delay/loss sensitive traffic routed on the public path.

3. Public directed traffic needs to be secured

IV. Objectives

- Billing must interface electronically to TACDOH accounting systems
- Break out usage and cost into territory, district, region and data center subsection based on a three year contract.
- Intelligently and cost effectively support the named TACDOH applications
- Provide 24/7/365 support for troubleshooting of circuit connectivity
- Provide network backup using public (Internet) and private options
- Provide self provisioning if available
- Replace current Frame Relay network with MPLS where possible
- Reporting of usage, availability and problems via role-based access control portal so as to allow TACDOH to limit access based on need to know and existing internal TACDOH directory.
- SOHO and Remote Access not part of this proposal

V. Selection Criteria

- Additional Service Costs
- Advanced Service Offerings
- Backbone Architecture
- CE Deployment Time/Costs
- Class of Service
- Contingency Services
- Geographical Coverage
- Global Network Strategy

- PoPs
- Price
- Summary of MPLS services
- Support for non-IP protocols
- Topology Service Offerings
- Traffic Classification

A. Monthly Cost and Geographical Coverage (assume a 3 yr contract)

Location Type	Location	Bandwidth and Reliability Requirements	Provider Network	Network Type – (MPLS, Frame, etc.)	Network Access Circuit Type (MPLS, Frame, etc.)	Network Backup Method	Monthly Cost	Explai if neec
Data Center	White Plains, NY USA	Voice = 50Mbps Video = 10Mbps SAP = 20Mbps Notes = 50Mbps Other = 25Mbps **Total = 155Mpbs**	AT&T VPN	MPLS-IP	MPLS POS[1]	Redundant link via second backbone node	$31722	Note 1
Data Center	Sterling, England	Voice = 50Mbps Video = 10Mbps SAP = 20Mbps Notes = 50Mbps Other = 25Mbps **Total = 155Mpbs**	AT&T VPN	MPLS-IP	MPLS ATM	Redundant link via second backbone node	$63539	See N
Data Center	Bangalore ,India	Voice = 50Mbps Video = 10Mbps SAP = 20Mbps Notes = 50Mbps Other = 25Mbps **Total = 155Mpbs**	AT&T VPN	MPLS-IP	MPLS ATM	Redundant link via second backbone node	$1.7M	See N
Regional Headquarters	New York, NY USA	Voice = 12Mbps Video = 3 Mbps SAP = 5 Mbps Notes = 12Mbps Other = 12Mbps **Total = 44.7Mbps**	AT&T VPN	MPLS-IP	MPLS POS	Redundant link via diverse PE router	$10,730	See N
Regional Headquarters	Plano, TX USA	Voice = 12Mbps Video = 3 Mbps SAP = 5 Mbps Notes = 12Mbps Other = 12Mbps **Total = 44.7Mbps**	AT&T VPN	MPLS-IP	MPLS POS	Redundant link via diverse PE router	$10,730	See N
Regional Headquarters	Covina, CA USA	Voice = 12Mbps Video = 3 Mbps SAP = 5 Mbps Notes = 12Mbps Other = 12Mbps **Total = 44.7Mbps**	AT&T VPN	MPLS-IP	MPLS POS	Redundant link via diverse PE router	$10,730	See N
Regional Headquarters	London, England	Voice = 12Mbps Video = 3 Mbps SAP = 5 Mbps Notes = 12Mbps Other = 12Mbps **Total = 44.7Mbps**	AT&T VPN	MPLS-IP	MPLS ATM	Redundant link via diverse PE router	$22323	See N

[1] POS = Packet-over-SONET

Regional Headquarters	Toyko, Japan	Voice = 12Mbps Video = 3 Mbps SAP = 5 Mbps Notes = 12Mbps Other = 12Mbps **Total = 44.7Mbps**	AT&T VPN	MPLS-IP	MPLS ATM	Redundant link via diverse PE router	$45705	See N
District Hub	Boston, MA USA	Voice = 512kbps Video = 128kbps SAP = 128kbps Notes = 512kpbs Other = 256kbps **Total = 1.54 Mbps**	AT&T VPN	MPLS-IP	MPLS PPP[2]	Redundant link via diverse PE router	$1027	See N
District Hub	Buffalo, NY USA	Voice = 512kbps Video = 128kbps SAP = 128kbps Notes = 512kpbs Other = 256kbps **Total = 1.54 Mbps**	AT&T VPN	MPLS-IP	MPLS PPP	Redundant link via diverse PE router	$1027	See N
District Hub	Herdon, VA USA	Voice = 512kbps Video = 128kbps SAP = 128kbps Notes = 512kpbs Other = 256kbps **Total = 1.54 Mbps**	AT&T VPN	MPLS-IP	MPLS PPP	Redundant link via diverse PE router	$1027	See N
District Hub	Toronto, Canada	Voice = 512kbps Video = 128kbps SAP = 128kbps Notes = 512kpbs Other = 256kbps **Total = 1.54 Mbps**	AT&T VPN	MPLS-IP	MPLS FR	Redundant link via diverse PE router	$40464	See N
District Hub	Atlanta, GA USA	Voice = 512kbps Video = 128kbps SAP = 128kbps Notes = 512kpbs Other = 256kbps **Total = 1.54 Mbps**	AT&T VPN	MPLS-IP	MPLS PPP	Redundant link via diverse PE router	$1027	See N
District Hub	Kansas City, MO USA	Voice = 512kbps Video = 128kbps SAP = 128kbps Notes = 512kpbs Other = 256kbps **Total = 1.54 Mbps**	AT&T VPN	MPLS-IP	MPLS PPP	Redundant link via diverse PE router	$1027	See N
District Hub	Minneapolis, MN USA	Voice = 512kbps Video = 128kbps SAP = 128kbps Notes = 512kpbs Other = 256kbps **Total = 1.54 Mbps**	AT&T VPN	MPLS-IP	MPLS PPP	Redundant link via diverse PE router	$1027	See N
District Hub	Chicago, IL USA	Voice = 512kbps Video = 128kbps SAP = 128kbps Notes = 512kpbs Other = 256kbps **Total = 1.54 Mbps**	AT&T VPN	MPLS-IP	MPLS PPP	Redundant link via diverse PE router	$1027	See N

[2] PPP = Point-to-point protocol

District Hub	Las Vegas, NV USA	Voice = 512kbps Video = 128kbps SAP = 128kbps Notes = 512kpbs Other = 256kbps **Total = 1.54 Mbps**	AT&T VPN	MPLS-IP	MPLS PPP	Redundant link via diverse PE router	$1027	See N
District Hub	Phoenix, AZ USA	Voice = 512kbps Video = 128kbps SAP = 128kbps Notes = 512kpbs Other = 256kbps **Total = 1.54 Mbps**	AT&T VPN	MPLS-IP	MPLS PPP	Redundant link via diverse PE router	$1027	See N
District Hub	Fresno, CA USA	Voice = 512kbps Video = 128kbps SAP = 128kbps Notes = 512kpbs Other = 256kbps **Total = 1.54 Mbps**	AT&T VPN	MPLS-IP	MPLS PPP	Redundant link via diverse PE router	$1027	See N
District Hub	Vancouver, Canada	Voice = 512kbps Video = 128kbps SAP = 128kbps Notes = 512kpbs Other = 256kbps **Total = 1.54 Mbps**	AT&T VPN	MPLS-IP	MPLS FR	Redundant link via diverse PE router	$4111	See N
District Hub	Bangkok, Thailand	Voice = 512kbps Video = 128kbps SAP = 128kbps Notes = 512kpbs Other = 256kbps **Total = 1.54 Mbps**	AT&T VPN	MPLS-IP	MPLS FR	Redundant link via diverse PE router	$155177	See N
District Hub	Seoul, South Korea	Voice = 512kbps Video = 128kbps SAP = 128kbps Notes = 512kpbs Other = 256kbps **Total = 1.54 Mbps**	AT&T VPN	MPLS-IP	MPLS FR	Redundant link via diverse PE router	$6554	See N
District Hub	Hong Kong, China	Voice = 512kbps Video = 128kbps SAP = 128kbps Notes = 512kpbs Other = 256kbps **Total = 1.54 Mbps**	AT&T VPN	MPLS-IP	MPLS FR	Redundant link via diverse PE router	$3885	See N
District Hub	Beijing, China	Voice = 512kbps Video = 128kbps SAP = 128kbps Notes = 512kpbs Other = 256kbps **Total = 1.54 Mbps**	AT&T VPN	MPLS-IP	MPLS FR	Redundant link via diverse PE router	$3885	See N
District Hub	Glasgow, Scotland	Voice = 512kbps Video = 128kbps SAP = 128kbps Notes = 512kpbs Other = 256kbps **Total = 1.54 Mbps**	AT&T VPN	MPLS-IP	MPLS FR	Redundant link via diverse PE router	$3249	See N

District Hub	Paris, France	Voice = 512kbps Video = 128kbps SAP = 128kbps Notes = 512kpbs Other = 256kbps **Total = 1.54 Mbps**	AT&T VPN	MPLS-IP	MPLS FR	Redundant link via diverse PE router	$3249	See N
District Hub	Madrid, Spain	Voice = 512kbps Video = 128kbps SAP = 128kbps Notes = 512kpbs Other = 256kbps **Total = 1.54 Mbps**	AT&T VPN	MPLS-IP	MPLS FR	Redundant link via diverse PE router	$3249	See N
District Hub	Berlin, Germany	Voice = 512kbps Video = 128kbps SAP = 128kbps Notes = 512kpbs Other = 256kbps **Total = 1.54 Mbps**	AT&T VPN	MPLS-IP	MPLS FR	Redundant link via diverse PE router	$3249	See N
100 Territory Sales Offices	Continental US	Voice = 64kbps Video = 32kbps SAP = 16kbps Notes = 64kpbs Other = 16kbps **Total = 192 kbps**	AT&T VPN	MPLS-IP	MPLS PPP	Redundant link via diverse PE router	$632 each	See N

Note 1: AT&T will provide an IP MPLS port to the customer. We will also provide a redundant port into a separate AT&T service node which will allow for load balancing and link and POP diversity to maintain high availability at the Data Center Site.

Note 2: AT&T will provide an IP MPLS port to the customer. We will also provide a redundant port into a separate AT&T MPLS Provider Edge router which will allow for load balancing, router and link diversity to maintain high availability at the Regional HQ Site.

Note 3: AT&T will provide an IP MPLS port to the customer. We will also provide a redundant port into a separate AT&T MPLS Provider Edge router which will allow for load balancing, router and link diversity to maintain high availability. Alternatively, we can provide an IPSEC/Broadband solution as the site will no longer act as a hub in the MPLS model.

B. MPLS Vendors Questions: General Guidance

The following questions explicitly address Network-Based MPLS service offerings utilizing the provider's **private** MPL backbone.

Question 1: MPLS Service Offerings

Please provide a high-level description of your current Network-based MPLS service offering, including details the technology and use of any strategic partners to deliver services.

Answer Guidance

Reason For Question

Understanding of the provider's Network-based MPLS service offering outlining the major features, functions or areas of support that differentiate the provider's service offering from competitors' offerings.

Mandatory Response Format:

Word count: Summary **not exceeding two pages** with executive overview and technical description.

1.0 **Executive Summary**

AT&T leads the industry with a seamless, consistent global deployment of an MPLS infrastructure that supports an extensive portfolio of MPLS services from every node. AT&T's MPLS IP infrastructure capabilities were built on the AT&T Global Network to provide enterprise customers with high reliability and performance. In the past few years, the company has developed innovative tools for customer end-to-end management that, to our knowledge, are unavailable from any other carrier.

AT&T also is an industry leader in the development and use of MPLS for the creation of VPN services and as a strategic platform for network convergence. AT&T Labs engineers are listed as co-authors of the industry-standard IETF specification RRFC2547bis, used worldwide by carriers to create IP VPNs.

AT&T was the first carrier to announce an MPLS VPN, in mid-1998. A scaleable service offering was debuted in early 1999 and the company has continually augmented its portfolio of MPLS-based services since then, culminating in its AT&T VPN service. AT&T has more than six years of experience in developing, implementing and managing MPLS VPNs, first on the its U.S. Frame Relay and ATM networks, then on its global network, and, most recently, on its massive U.S. IP network. AT&T has invested heavily in tooling and automation to support its MPLS-based services, creating an automated flow-through provisioning infrastructure that offers a technically rigorous performance monitoring infrastructure. AT&T's patented MPLS management tools automatically detect loss of connectivity within the VPN.

AT&T suggests that its AT&T VPN service will meet TACDOH's business requirements. AT&T VPN is a fully managed, globally consistent network-based solution that provides essential IP VPN networking, change and problem management, and security. AT&T VPN supports any-to-any mesh connectivity, making it easy to link remote or local employees, customers and trading partners in many locations around the globe, while possibly resulting in a reduction in investments in network equipment, systems and personnel.

A fully bundled service, AT&T VPN can include all the following elements in a single monthly recurring charge: Access, Transport, Managed Customer Premises Equipment (CPE) and Management. AT&T VPN is supported by 24_7 network operations and customer support. Global network management is provided from one point of contact and is available on AT&T's seamless global network in more than 60 countries.

1.1 Technical Details

The AT&T VPN architecture is based on the RFC 2547bis standard, and combines MPLS with technologies, such as Multi-Protocol BGP (MP-BGP) and Virtual Routing. The service provides any-to-any connectivity and customers can use private addressing. Data privacy and security are ensured by MPLS separation and AT&T's rigorous network security practices.

1.1.1 Technical Description of Packet Flows

Beginning at the Customer Edge (CE) and working towards the network core, CE routers connect to Provider Edge (PE) routers using EBGP or Static Routing and have a separate local routing table per connected customer VPN (called the customer VRF - Virtual Routing and Forwarding - table). The PE routers then distribute VPN routing information through MP-iBGP to other PE routers using "VPN-IPv4 addresses." PE routers exchange labels with the MPLS core.

Key to AT&T's VPN architecture is that PE routers do not need to know VPN routes and PE routers do not have to run BGP. AT&T's strategic direction for its core MPLS backbone is that BGP routes will be removed, making the network core extremely stable and invisible to outside entities.

1.1.2 Service Features

AT&T VPN is transport and access independent, and can provide secure any-to-any connectivity using MPLS technology. AT&T VPN is available in more than 60 countries via AT&T's seamless Global Network, using a wide range of connectivity/access types including broadband, 56K – OC48, wireless, and satellite. Inside wiring is included for domestic U.S. sites (up to 300 feet).

AT&T VPN supports an end-to-end Quality of Service specification by application type or network destination, allowing customers to prioritize applications based on service quality requirements. Enterprises may specify differentiated data classes of service transported over an MPLS-enabled network backbone and obtain performance reports for each class of service via AT&T's award-winning BusinessDirect® portal.

AT&T VPN Service also supports extended multiple IP VPN capabilities that allow customers to create their own communities of interest between customer sites, as well as port-based pricing (no PVC's) and simple VPN and Class-of-Service packages. AT&T VPN provides site-to-site service level agreement metrics by Class of Service and enhanced customer reporting available from AT&T's award winning BusinessDirect® portal. This portal is available 24X7 and provides secure, online access to the following functions:

- Electronic provisioning, new site, moves adds and deletes
- Custom interfacing with our e-bonding service to your accounting systems (billing interfaces to your system)
- Network statistics available for all site-to-site delivery ratios based on Class of Service
- VPN Snapshot – a topology map providing customers with a map of their network

Question 2: MPLS Backbone Architecture

Please provide a high-level description of overall Network-based MPLS backbone architecture covering the following topics:

- *Current use of provisioned VPNs (MPLS-based Layer 2 VPNs or BGP/MPLS VPNs "RFC2547bis" - L 3)*
- *Access and control plane*
- *Provider (P), Provider Edge (PE), Customer Edge (CE) technology*
- *Routing protocols between PE and CE*
- *Traffic engineering within the core (such as LDP, CR-LDP, RSVP-TE)*
- *Provider CE offering (Managed CE, non-managed CE or both)*
- *Identify any use of 3rd party infrastructure*

Answer Guidance
Reason For Question: Understanding of the provider's MPLS backbone architecture, outlining the functional areas (e.g., access plane, control plane and data forwarding plane) and how these differentiate the provider's backbone architecture from competitors. To, gain comprehensive perspective on how the provider network architecture can effectively meet their service requirement as relates to routing/communication across the provider MPLS backbone.
Mandatory Response Format:
Word count: Summary **not exceeding three pages** describing vendor's network base MPLS architecture.

2.0 AT&T MPLS Backbone Architecture

AT&T leads the industry with a seamless, consistent global deployment of an MPLS infrastructure that supports an extensive portfolio of an MPLS infrastructure, supporting an extensive portfolio of MPLS services from every node. Our MPLS architecture is built on the AT&T Global Network, with high reliability and performance, with tools for customer end-to-end management.

2.1 AT&T Current use of provisioned VPNs (MPLS-based Layer 2 VPNs or BGP/MPLS VPNs "RFC2547bis" - Layer 3)
AT&T is been the industry leader in the development and deployment of MPLS technology and VPNS. AT&T announced its first MPLS-based service in 1998 and has steadily added MPLS-based services to its portfolio since then. AT&T Labs engineers are listed as one of the co-authors of the industry-standard specification RFC2547bis, today's industry MPLS standard architecture used for IP VPNs.

In 2003 AT&T announced that MPLS was the strategic technology that would be used as a convergence platform for its networking infrastructure. In response, Broadband Publishing Corporation, in its Network Technology Report, described this announcement as "the strongest endorsement of MPLS to date, from the largest and most financially stable network operator in North America."[3] Broadband Publishing went on to predict that AT&T's endorsement of MPLS may be a harbinger of the future technology direction of the industry, as it was 10 years ago when AT&T announced its support of frame relay, now a widely deployed mainstream networking technology.

Since 1999 AT&T has continually rolled out new MPLS-based services. AT&T is also an innovator in the area of MPLS network management and has developed a number of patent-pending tools that can detect outages in MPLS-based VPNs as rapidly as a few seconds, thus providing network management visibility similar to that of traditional Layer 2 networks.

[3] Broadband Publishing, "Network Technology Report," ISSN 1542-6009, 2003, page 1.

As of April, 2005, AT&T has more than 60,000 customer MPLS VPN ports in service across its global network. AT&T is also developing Virtual Private Wire Service (VPWS) and Virtual Private LAN Service (VPLS) to support Ethernet WAN services.

AT&T's MPLS-based services are provided via the AT&T global network, a seamless AT&T-owned global network that is engineered to sustain high-level throughput while maintaining low latency. At Layer 3 this network is designed with regional autonomous systems in order to provide efficient intra-region routing and as well to maintain scalability.

Within the United States, MPLS-based services are deployed on Avici TSR routers, Cisco GSR routers and RPM blades within Cisco MGX switches, depending upon the size of the customer connection and service features requested. When managed CPE is provided, Cisco routers are deployed to support customer router feature requirements. The core of the US network is an OC192 backbone that provides reliability, low network congestion and consistent performance. Label switching functionality outside the United States is provided by router blades within Cisco MGX switches and Cisco GSR routers; global trunking ranges from E3-STM4. PE functionality is provided either by router blades within MGX switches or Cisco GSR routers.

AT&T's global architecture is based on a tiered structure comprised of three types of network nodes. All nodes use the same hardware and software platform and support all services. The distinction among the three node types relates to trunk capacity, placement within the network and geographic reach. AT&T's has standardized (globally) all equipment and architecture across the network.

The AT&T global network is designed to be highly reliable through the use of redundancy in the equipment and trunk configurations. All routers and switches are deployed in redundant configurations, including redundant processors and redundant power supplies. All nodes are connected to at least two others to allow for re-routing in the event of a facility failure. All service-affecting hardware elements are spared within the node. All backbone nodes are to be deployed within highly secure facilities. These facilities are to be served by two commercial power sources, as well as protected against commercial power failures with both battery backup and emergency generators.

The AT&T global network has been designed to be single-link and single-node survivable. Since the core network is engineered to carry all committed traffic in the event of any network trunk failure, sufficient capacity exists to reroute traffic to alternate facilities in the event that a single backbone facility fails.

There are three AT&T global network Node Types: 1) Type 1 (Large) is located in major metro areas with access to fiber, supports large number of customer ports, supports high bandwidth needs (>STM1) and is interconnected typically with STM4-STM16 trunks. Type 2 (Intermediate) nodes support 50-100 customer ports, customer connections up to STM1 and typically are interconnected with dual E3/DS3 trunks and can accommodate growth to STM1 trunking. Type 3 (Small) nodes support up to 50 customers, can accommodate customer connections up toE1 and typically are connected with dual E3/DS3 trunks. In all cases trunking has been deployed in diverse configurations with restorative properties such as SONET whenever possible.

In addition, the AT&T global network, both within the US and abroad, is protected by AT&T's unique Network Disaster Recovery program. This program consists of a fleet of pre-configured trailers and support personnel who are able to respond to a "smoking hole" disaster and rebuild a destroyed POP with a target restoration period of 24-168 hours, depending upon the location within the world. In 2004, this program, originally US only, was expanded to support global nodes to provide additional protection against a major disaster. A detailed document describing this program is available upon request.

2.2 Access and control plane

The access and control plane varies by the size and location of the TACDOH customer connection. The access solution includes:

- U.S. Access: AT&T VPN with MPLS IP network transport and MPLS PPP/POS access (POS for DS3 and above sites, PPP for T1 and below sites)

- Non U.S. Access: AT&T VPN with MPLS IP network transport and MPLS / ATM or FR access (ATM for DS3 and above sites, FR for T1 sites)

2.3 Provider (P), Provider Edge (PE), Customer Edge (CE) technology
P and PE technology varies by region. Within the United States, Avici TSRs and Cisco GSRs are used for the P core, while Cisco routers are used for the PE. Globally, Cisco GSRs and MGX switches are used for both the P core and the PE. Cisco routers are used for the CE.

2.4 Routing protocols between PE and CE
AT&T supports BGP and static routes between the PE and CE.

2.5 Traffic engineering within the core (such as LDP, CR-LDP, RSVP-TE)
AT&T presently uses LDP and OSPF within the core of its MPLS network. AT&T has built a robust network performance infrastructure that constantly probes for network performance between all endpoints and alerts the NOC when performance begins to degrade so proactive steps may be taken. AT&T has been testing MPLS FRR for quite some time and currently has plans to trial this feature in parts of the MPLS network towards the end of 2005. To date, AT&T has relied on a combination of mechanisms at L1 (such as SONET restoration facilities) or L3 (routing protocol tuning) which can typically detect and route around network failures transparent to end user traffic flows.

2.6 **Provider CE offering Managed CE, non-managed CE or both)**
AT&T can provide either unmanaged or managed CE if desired, fully managing the router and CSU device. AT&T also can provide a managed CSU only should the customer desire to control the router themselves. This proposal is based on managed CE.

2.7 Use of 3rd party infrastructure
Within the United States AT&T does not use third party infrastructures except for DSL and remote access technologies such as WiFi and Wired Ethernet, and the last mile access lines. All network services are transported across the AT&T global network.

Outside the United States, in addition to its own global POPs, AT&T has partnered with the two PTTs in China in order to use their MPLS POPs for deeper reach and service coverage within China. This make the two regulatory regions of China effectively appear to be two additional regions on the AT&T Global MPLS network. AT&T also is executing on a multi-pronged global access strategy to extend the reach of its global network using NNIs, MPLS interconnects, long private lines and satellite technology where appropriate. Additional 3rd party interconnects are being planned.

Question 3: Your MPLS Point of Presence

Please provide details about your POP geographical coverage across North America. Ensure you distinguish between "active" and "non active/planned".

Answer Guidance
Reason For Question: Understanding of Provider's MPLS reach-ability, point of presence and access connectivity types to TACDOH locations. Also, identify where the provider's backhaul paths might impact availability and service quality.
Mandatory Response Format: A topology map and a list identifying the access type connectivity, the city of the MPLS ready POPs and any future MPLS POP site. Include proposed access types (e.g., Frame-Relay, ATM, POS, DS-x, DSL, etc.) to customer premises (from PE to CE).

3.0 AT&T MPLS Points of Presence

AT&T has deployed a seamless, consistent global MPLS network, with a large number of nodes. Our MPLS capabilities are built on the AT&T global network, with high reliability and performance, with tools for customer end-to-end management.

AT&T MPLS services can be accessed from more than1000 Points of presence globally, of which approximately 600 are located in the US. AT&T has one of the largest networks within the United States, with more than 77,000 miles of AT&T-owned fiber facilities and ~600 POPS, in addition to over 200 POPs owned by AT&T Alascom, a wholly owned AT&T subsidiary. Exact details of POP locations are proprietary. However, AT&T can provide service to all TACDOH locations at the speeds requested. In general, all services are available at all POPs; AT&T does not distinguish between "active" and "planned." AT&T does not provide lists of service nodes.

The access solution proposed, to customer premises (from PE to CE) includes:

- U.S. Access: AT&T VPN with MPLS IP network transport and MPLS PPP/POS access (POS for DS3 and above sites, PPP for T1 and below sites)
- Non-U.S. Access: AT&T VPN with MPLS IP network transport and MPLS / ATM or FR access (ATM for DS3 and above sites, FR for T1 sites)

Figure 3.1 shows the global reach of AT&T VPN.

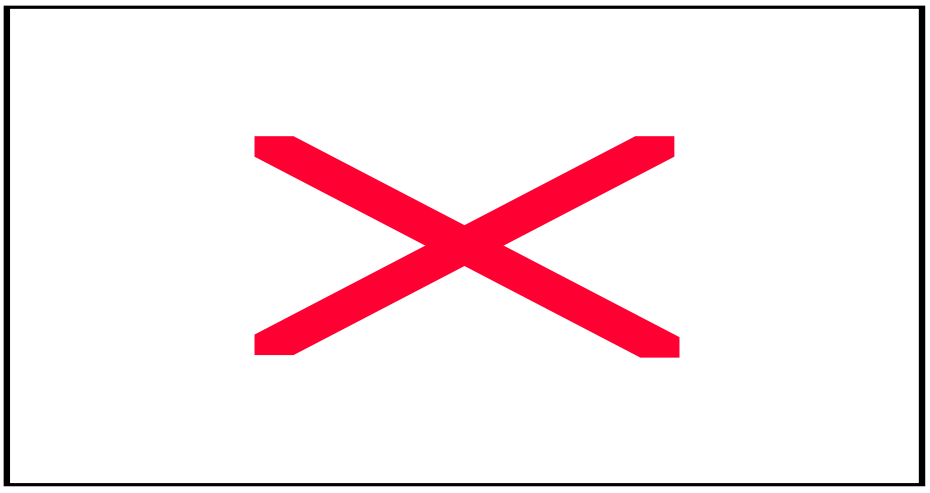


Figure 3.1

Question 4: MPLS Contingency/Backup Solution

Please provide details of your Network-based MPLS contingency solutions to ensure both service continuity a high availability.

Answer Guidance
Reason For Question: Understanding of provider's MPLS contingency solution for TACDOH business continuity and high availability service. The different high availability option should aid TACDOH in determining a cost effective solution for service availability at different locations (e.g., Business critical site would require a higher degree of contingency than a non critical site).
Mandatory Response Format:
Word count: Summary **not exceeding two pages** of provider's network base MPLS contingency solution, including but not limited to:

- Access Link Redundancy
- Component Redundancy
- Central Office (CO) diversity

4.0 AT&T VPN Resiliency Options

AT&T has deployed a seamless, consistent global MPLS infrastructure, supporting an industry leading portfolio of MPLS services from every node. Our MPLS capabilities are built on the AT&T Global Network, with a highly reliable and resilient network and access links.

AT&T VPN includes resiliency options to allow customers to create highly available VPNs. Resiliency options are intended to eliminate single points of failure in a customer's VPN and allow automatic service rollover functionality.

4.1. AT&T VPN Diversity Options
The AT&T VPN Diversity Options (DOs) help protect the customer's network in the event of a failure at an AT&T POP. DOs are an ordering option on most MPLS Ports. Customers may designate one or more AT&T VPN DO arrangements. Each AT&T VPN DO arrangement includes up to three mutually exclusive groups of MPLS Ports. The total number of MPLS Ports in each AT&T VPN DO arrangement may not exceed 1,000. Changing the assignment of an MPLS Port from one AT&T VPN DO arrangement to another is considered a disconnection of the existing DO MPLS Port assignment and a new assignment of the MPLS Port to the new AT&T VPN DO arrangement.

4.1.1. AT&T VPN Service Diversity DO Arrangements
In a Service Diversity DO arrangement, AT&T will provision each group of MPLS Ports to a different AT&T group of AT&T switches or routers. An MPLS Port may not be included in more than one Service Diversity DO arrangement.

4.1.2. AT&T VPN POP Diversity DO Arrangements
In a POP Diversity DO arrangement, AT&T will provision each group of MPLS Ports to a different AT&T POP or group of AT&T POPs. An MPLS port may not be included in more than one POP Diversity DO arrangement.

4.2 Network Resiliency
In the United States, the AT&T MPLS backbone consists of a core OC192/OC48 network constructed from the AT&T-owned physical infrastructure, using Avici TSR routers as backbone core routers. Avici routers are designed with highly redundant architectures and are designed to work within the DC Central office environment, so they have no power supplies but use DC indirectly. This eliminates the single points of failure of power supplies and required inverters. Multiple, diversely routed backbone trunks interconnect all city pairs and the network has been designed and is capacity-managed to be single-link and single-node survivable. Each backbone node is interconnected to at least two others with multiple-diversely routed physical facilities.

Backbone trunk restoration is performed by Layer 3. Edge devices (RPM blades or routers, depending upon size of customer connection) are interconnected to two backbone core routers for additional reliability.

Two types of edge devices are used to support customer connections: Cisco routers and RPM blades within Cisco MGX switches. For Cisco router edge devices, two types of redundancy are provided. First, the routers are deployed with redundant processors and redundant power supplies. Within the major U.S. nodes, a "hot spare" infrastructure has been deployed, consisting of fully loaded, powered up routers containing a full inventory of working cards of the same type used in the edge routers themselves. For RPM blades deployed within MGX switches, the power supplies, trunk cards, and port cards are redundant. Within the MGX switches themselves, processor, trunk and ATM cards are deployed in 1:1 redundant configurations, high-speed frame/ATM cards are deployed in 1:1 redundant configurations and low-speed frame connections are deployed in an 1:N redundant configuration.

All U.S. nodes are deployed within AT&T-owned and controlled POPs. These highly-reliable secure facilities are guarded and staffed 24x7 and are only accessible to authorized personnel. All nodes are protected by dual uninterruptible power sources, including battery backup and emergency diesel generators. In addition, a robust disaster recovery scheme is tested regularly to ensure that all components work in the event of a power failure.

Outside the United States, the MPLS core uses paired Cisco 12000 GSR routers as backbone routers. These devices use Cisco's latest GSR line cards (Engine 3) to support wire-speed trunking up to OC-48 speeds (an upgrade to the GSR can support OC-192 trunking). The GSRs are located at global core (Type 1) PoP locations. In addition, at each global core PoP location at least one high-speed GSR access router (MPLS PE router) is deployed to support STM-1/OC-3 and above access requirements.

Slower speed customer connections use RPM blades within Cisco MGX switches, deployed in the same locations. The MGX switch is connected to the core router via redundant ATM trunks, and from core router to core router, the connections are SONET over SDH. Outside the United States, protected facilities are obtained where available, and all nodes are connected to at least two other nodes via diversely routed facilities. The intelligence of the optical network makes it possible to restore service faster in the event of a failure. Switches can automatically reroute traffic after a failure because each switch has a comprehensive map of all available routes.

This multi-vendor, next-generation network features intelligent optical switches and multi-service platforms that are carrying new private-line, Internet, voice, data, and video traffic. The "intelligence" in the switches comes from innovative software that uses sophisticated real-time signaling and routing algorithms to make decisions without the need for manual intervention.

AT&T's global network nodes are housed in state-of-the-art, secure tele-house facilities, which are located in central business districts of major cities throughout the globe.

4.3 Access Resiliency

The AT&T Access Services portfolio provides reliable secure access to networking environments. Our access services are differentiated by worldwide availability, reliability metrics, end-to-end performance, and service flexibility options. AT&T offers a large breadth of capabilities worldwide. This enables AT&T to design a cohesive solution tailored to a customer's specific requirements, that considers how that customer may invest in and drive ROI from its access services for next generation networking.

AT&T also provides the ability to design, deploy, deliver and manage global access solutions that support a customer's networking environment needs. AT&T provides access between a customer's premises and the AT&T Point of Presence (POP) with owned (on-net) and LEC-leased access circuits. AT&T is the single point of contact for all access processes. AT&T also has an extensive portfolio of "high availability" access services. These options can supply

TACDOH with protected access facilities to ensure business continuity. AT&T also can provide access diversity with access service to two ports as two diverse circuits.

Question 5: Class of Service Offering

Please provide details of your class of service offerings that would enable TACDOH to differentiate services by category. TACDOH is interested in the following functional areas:

- *Number of class of services provided throughout the provider network.*
- *Recommended or restricted applications characteristics for each class*
- *Service level parameters related to each class covering:*
  Packet Loss
  One Way Delay (measured from CE-to-CE)
  Jitter OR other quality indicators (is this relevant?)

Please, fill in (Yes/No) the following table with the associated SLA parameter for each class of service.

Class of Service offerings	Delay	Packet Loss	Jitter (or other quality indicators)
Class 1			
Class 2			
Class 3			
Class 4			
Class 5 (if any)			

- *Do you offer the Committed Data Rate – CDR (contracted bandwidth) per circuit or per class of service?*
  - *If the CDR per circuit; please specify:*
    - ß *The minimum and maximum bandwidth CDR percentage limitation/allowed per circuit; please clarify if the technical reasons (if any)*
    - ß *If there is cost associated with the CDR per circuit*
  - *If the CDR per class of service; please specify:*
    - ß *The recommended CDR. percentage per class of service (if any)*
    - ß *The minimum and maximum bandwidth CDR percentage limitation/allowed per each class; ; please clarify if the technical reasons (if any)*
    - ß *If there is different cost associated with the CDRs per class.*

- *Bursting capabilities for each class (if any)*

- *Monitoring and reporting capability on QoS serviceability (if any)*

Answer Guidance
Reason For Question: Understanding of the provider's class of service (CoS) offering for TACDOH service differentiation categories. These classes will have some form of QoS/service level parameter that TACDOH will use to guarantee end-to-end quality of experience for its users. Also, TACDOH will utilize the contracted bandwidth allocation and bursting capability of each class for better capacity planning.
Mandatory Response Format:
Word count: Summary **not exceeding two pages**, outlining provider's network base MPLS class of service offerings.

5.0 AT&T Class of Service

AT&T leads the industry with a seamless, consistent global deployment of an MPLS infrastructure that supports an extensive portfolio of MPLS services from every node. Our MPLS Class of Service capabilities provide high reliability and performance, with tools for customer end-to-end management.

AT&T Class of Service is an architecture that provides improved and predictable network services. The AT&T Class of Service (CoS) offering is based on Modular QoS CLI (MQC) architecture which comprises of following techniques:

I. **Traffic Classification** is used to map traffic types to different classes of service. Traffic types are recognized by the ingress AT&T managed router using IP addresses, ports, protocols, IP Precedence/DSCP setting, or a combination.
II. **Policing and Marking** are the result of the above traffic classification when applied against an ingress COS profile. Packets exceeding the COS1 bandwidth allocation are strictly policed (traffic above the allocated bandwidth is discarded), while packets in any of the data classes (COS2 through COS4) are marked with an in-contract or out-of-contract DSCP settings.
III. **Scheduling and Congestion Management** are the methods used to service traffic across the WAN connection to and from AT&T's backbone network. An egress scheduling or queuing COS profile is selected to allocate the bandwidth needed for each class. If there is insufficient bandwidth to fully service a class, then out-of-contract packets may be discarded within the class to help relieve the congestion using the WRED algorithm. Discarded packets allow TCP applications to throttle back by closing their TCP windows.

The Class of Service feature applies to the Port the customer has purchased. For PPP ports, the customer gets the full port speed and the COS profile is applied to that port. For Frame Relay or ATM ports, the CDR is set to port speed and it is not a pricing element. Customers receive a port speed service, regardless of the Layer 2 access protocol. If however, they would like to also have legacy point-to-point PVCs terminating on the same port, than the CDR of the PVC to the MPLS VPN can be set to a value lower than the port speed; typically the Port speed less the legacy PVC.

AT&T CoS uses four priorities to classify traffic. Customers can use all four classes or a subset as defined by the list of predefined COS profiles. The table below describes the different classes, the corresponding priority, and the Diffserv Code Point (DSCP) markings[4]. The COS1 class is designed for real-time applications traffic, whereas the other three can be used for non-real-time applications traffic.

Class of Service	Traffic Priority	In-Contract Marking	Out-of-Contract Marking
COS1	URGENT (Real-Time)	DSCP EF	Dropped
COS2	HIGH (Critical Data)	DSCP AF31	DSCP AF32
COS3	MEDIUM (Business Data)	DSCP AF21	DSCP AF22
COS4	NORMAL (Standard Data)	DSCP DEFAULT	DSCP DEFAULT

Each of the three data classes (COS2 through COS4) has a specific amount of bandwidth allocation so that during congestion, all classes can transmit data. However, if any class does not use its entire

[4] Although DiffServ TOS markings can be backwards compatible to IP Precedence, the DSCP markings are not related to the legacy IP Precedence markings and are maintained independently. New and upgraded sites with COS will be implemented with the DSCP markings.

bandwidth allocation, packets of other classes can share the unused bandwidth. The two primary criteria for assigning data applications to the data classes are:

(1) Required bandwidth
(2) Delay sensitivity.

The Table below provides the Network edge to Network edge SLAs for each class of service within the U.S region. The Delay column represents a roundtrip delay. The Jitter and Packet Loss represent one-way statistics.

Class of Service offerings	Delay	Packet Loss	Jitter (or other quality indicators)
Class 1	39 ms Avg in US	0.1%	1ms
Class 2	39 ms Avg in US	0.1%	N/A
Class 3	39 ms Avg in US	0.1%	N/A
Class 4	39 ms Avg in US	0.1%	N/A
Class 5 (if any)	N/A	N/A	N/A

Table 3: SLAs

CE to CE SLAs can be provided and are dependent on access speeds and specific distances between the CE to account for propagation and serialization delays.

5.1 Monitoring and Reporting Capability

AT&T offers performance reports on its MPLS service. These performance reports are available through the AT&T BusinessDirect® portal and are based on data captured at five minute intervals. A summary port report enables customers to see the ingress traffic utilization, egress traffic utilization, packet discards and packet errors for each port based on an hourly average. Once there, they can select a specific location or site to see the details by hour in the data. Reports are available on a weekly basis and saved for four weeks. Reports are available in tabular and graphical form.

In addition to port reports, customers can get usage reports based on Class of Service. They can see the CoS profile that has been configured on the port, and then see tabular and graphical reports showing the usage by CoS relative to the bandwidth allocation for that class. Customers also can see the packet discards at egress by CoS, which would indicate the likely need for a profile change to increase in bandwidth to accommodate the offered load.

Question 6: Traffic Classification

Please provide details of how traffic is categorized and provides preference to TACDOH different service type TACDOH is specifically interested in the following (but not limited to) functional areas:

- *Traffic Classification/marking techniques on the CE router (example: marking by IP Address, TCP/UDP ports, URL, MIME, Citrix ICA, etc.)*
- *Honoring of customer LAN classification/marking (CoS marking IEEE Layer 2 802.1Q/P and Differentiated Service Code Point – DSCP, etc.) to provide End-to-End QoS.*
- *Traffic prioritization techniques for different traffic types. For example, real time, non-real time, etc.*
- *Traffic congestion avoidance techniques for different protocol type (TCP, UDP, SNA, etc.)*

Answer Guidance
Reason For Question: Understanding categorization; the provider may honor or re-mark TACDOH traffic categories with same level of precedence/prioritization as TACDOH application requires. Also, in time of traffic congestion at CE device, TACDOH needs to understand the congestion management/avoidance mechanism utilized by the provider to assure highest quality of user experience.
Mandatory Response Format:
Word count: Summary **not exceeding two pages,** outlining provider's network base MPLS class traffic classification.

6.0: AT&T Traffic Classification

AT&T leads the industry with a seamless, consistent global deployment of an MPLS infrastructure that supports an extensive portfolio of MPLS services from every node. Our traffic classification capabilities enable optimal performance.

This section provides guidance on selecting the appropriate CoS profile to implement given an enterprise specific group of applications traversing the WAN. The first step in this process is the non-trivial task of developing an inventory of applications traversing the WAN and the respective bandwidth consumption per application. With this information, applications can be classified more accurately and in a manner that assures the desired behavior of assuring all applications perform satisfactorily.

The following sections describe application characteristics as they relate to response time requirements as well as to other attributes that must be considered when classifying an application for CoS purposes. A discussion of data queuing and scheduling follows to provide a deeper understanding of why and when an application is mapped to a particular class. Last, some general axioms are presented to designate the proper CoS profile selection and application mapping.

The CE router would need to map any internal used classifications into the DSCP/ToS settings as laid out in the answer to Question 5 above. Traffic is assigned to a class on the customer router. The parameters used to classify application traffic on the customer router, include:

- Origin IP address
- Destination IP address
- Input interface
- TCP/UDP Port number
- Application protocol

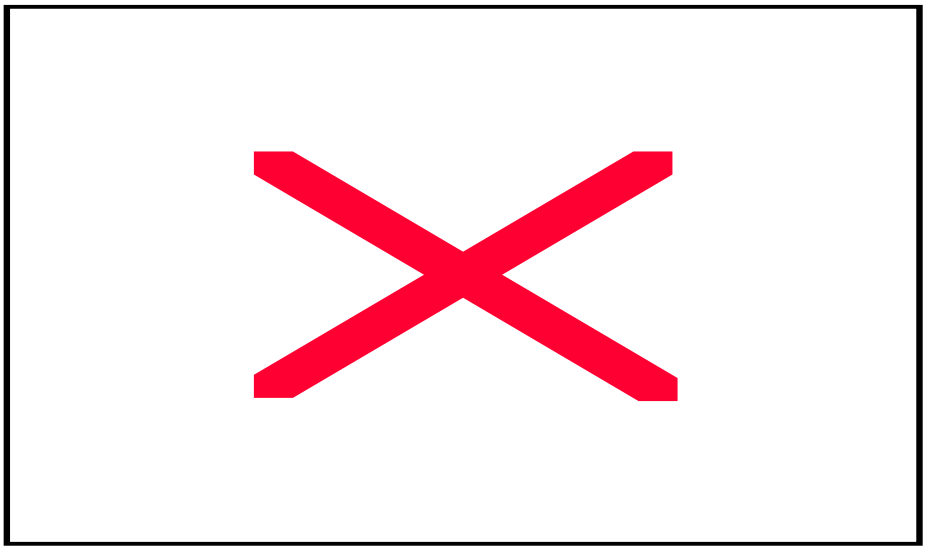
- Classification/setting of IP precedence bits/marking

Explicit prioritization is given to COS 1 using a Low Latency Queue (LLQ). In addition, WRED is used for congestion avoidance within Classes 2 and 3 to differentiate in and out of contract traffic.

6.1 Application Attributes

The primary differentiation provided by CoS features are differential queuing. The main impact of this differentiation is in network delay during congestion. An application with strict response time requirements needs the minimum queuing delay to meet those requirements, therefore we want to create a class (or CoS) hierarchy based on response time requirements. The Figure below illustrates response time requirements as a continuum of delay sensitive interactive applications to non-delay sensitive bulk data applications.[5] The applications listed in the figure are for illustrative purposes only and could be classified differently based on the specific enterprise environment.

While an application for one enterprise may need a 'Sub-Second' response time, another enterprise using the exact same software could consider the application response time requirement as 'Multi-Second' or 'Background' based on its implementation or criticality to the business mission. Further, user expectations for the response time of a particular application could differ from enterprise to enterprise. Each enterprise has a unique mixture of applications traversing the WAN that exhibit differing characteristics throughout the response time continuum. Therefore, each enterprise must be considered on a case-by-case basis when selecting the appropriate CoS profile and application mapping.



For TACDOH, we recommend the following mapping:

Application	Class
Voice	CoS 1
Video	CoS 2
SAP	CoS 2
Notes	CoS 3
Other	CoS 4

[5] In general, response time critical applications tend to consume less bandwidth, and non-critical applications tend to consume more bandwidth.

Question 7: Topology Service Offering

Please provide details of your meshing capability of your MPLS cloud. TACDOH is interested in the following (but not limited to) functional areas:

- *Any-to-Any connectivity for domestic and/or international locations;*
- *Technical limitation to create partial clouds (if required) to accommodate TACDOH current and future community of interest;*
- *Intra-connectivity between partial clouds for same provider*
- *Inter-connectivity between partial clouds between different providers.*

Answer Guidance
Reason For Question: Understanding of meshing capability of the provider cloud and how TACDOH can utilize this functionality to save on internal peering cost and connectivity to extranet partner via the Network-based MPLS cloud. Any-to-any connectivity from a single site to other TACDOH sites or partners should be a single connection to the MPLS cloud(s); forming fully meshed connectivity with single point to cloud concept. Also, Intra and Inter provider cloud connectivity allow TACDOH global reach-ability to communicate with different community of interest (Extranet Partners, Customer etc.).
Mandatory Response Format:
Word count: Summary **not exceeding two pages,** outlining provider network base MPLS topology service offering, including but not limited to the functional areas listed below. You should also include a diagram identifying your existing and future community of interest should accompany the vendor summary.

7.0 AT&T Topology Service Offering

AT&T has deployed a seamless, consistent global MPLS network, with a variety of interconnect options. Our MPLS capabilities are built on the AT&T global network, with high reliability and performance, with tools for customer end-to-end management.

7.1 AT&T Any-to-Any connectivity for domestic and/or international locations
AT&T VPN provides fully meshed connectivity between all TACDOH's locations within the United States and globally.

7.1.1 Technical limitation to create partial clouds (if required) to accommodate TACDOH current and future community of interest
AT&T currently meets the customers' community of interest by allowing customers to configure multiple VPNs from the same physical ports via PVCs or Frame Encapsulation over PL (private line) access. Each VPN can be constructed for its community of interest needs and the appropriate topology will be generated accordingly.

7.2 AT&T Intra-connectivity between partial clouds for same provider
As indicated above, AT&T can meet customers' needs of partial clouds within our network by using multiple VPNs to construct the necessary topologies.

7.3 AT&T Inter-connectivity between partial clouds between different providers
The need for AT&T to provide competitively priced and geographically desirable access for our customers to the Global MPLS-enabled IP network has necessitated that AT&T deploy Layer 1, Layer 2, and Layer 3 inter-working with a number of service providers around the world. Though AT&T will continue to deploy our own nodes globally there will be times when due to the regulatory environment, financial considerations, and need to fulfill client demands necessitate that AT&T pursue interconnect arrangements to expand our global network. As an example, AT&T recently established a Layer 3 (MPLS level) inter-working arrangement with two service providers in China which added 89 service nodes, significantly expanding our footprint and our ability to effectively serve our clients in China.

Question 8: Support for Non-IP Protocols

Please provide details of your support for legacy protocols.

Answer Guidance
Reason For Question: Understanding of provider support for legacy protocols (such as IPX, SNA, etc.) and applications over Network-Based MPLS service. The provider should describe their capability in supporting these protocols over the Network-Based MPLS including any use of encapsulation, tunneling or translation of these protocols to IP at CE device.
Mandatory Response Format:
Word count: One page summary outlining non-IP protocol support and how you transport it across your MPLS network

8.0 AT&T Supported Protocols

AT&T VPN supports the following customer protocols:

- IP Routing Protocols (LAN) – RIPv2, EIGRP, IGRP, BGP, OSPF
- IP Routing Protocols (WAN) – Static
- SNA encapsulated via Data Link Switching (DLSw)
- SNA via STUN
- NetBIOS supported with DLSw.
- IPX via Generic Routing Encapsulation (GRE) tunneling. Defined in IETF RFC 2784; it is IP tunneling over IP.
- Appletalk via GRE
- X.25 over TCP (individual case basis)
- Decnet Phase IV and Phase V via GRE (individual case basis)

SNA and IPX can be run at the same time.

8.1 Data Link Switching (DLSw)

To support SNA traffic via the MPLS network, we will use Data Link Switching encapsulation (DLSw). DLSw tunnels the SNA traffic in an IP packet; therefore the IP-only MPLS network can pass the data without any issues.

DLSw peers can be set up with redundancy. The DLSw configuration below outlines the standard for the primary backup scenario. Each DLSw peer is setup as primary (i.e., no backup peer statements). Because the source and destination MAC addresses are the same, the destination router keeps both DLSw paths in a cache and determines the feasibility of each based on its associated cost. Additionally DLSw timers have been set to optimize failover time between peers.

8.2 Novell IPX

Service Advertising Protocol (SAP) is a protocol that allows servers to advertise their services on a Netware internetwork. Servers broadcast their name, network address, and service type every 60 seconds by default, and this information is stored in the Netware Server Information table. Clients or workstations utilize the server's services by first logging on to the server and accessing the directories and files on the server. RIP (Routing Information Protocol) is used to advertise and route IPX packets across a network. RIP broadcasts the entire IPX route table every 30 seconds by default. Routers send periodic SAP and RIP broadcasts to keep all routers on the internetwork synchronized.

IPX routes and traffic are encapsulated in IP using generic routing encapsulation (GRE). GRE tunnels are configured on the CE routers forming a point-to-point tunnel. EIGRP for IPX is configured on the tunnel interfaces to keep the RIP and SAP broadcast traffic down to a minimum but RIP and SAP are configured on the LAN interfaces to dynamically discover the IPX networks and SAPs.

Question 9: Advanced Services Offerings

Please provide details of your advanced service offerings to support services. TACDOH is interested in the following (but not limited to) functional areas:

- *IP Multicast support (e.g., Multicast VPN, IP Multicast over P2MP MPLS TE, etc.);*
- *IP Voice call processing functionality (Voice over IP Gateway, IP Telephony call processing, on-net and off-net);*
- *IP Video bridging functionality (point-to-point and point-to-multi-point);*
- *Internet Access Service;*
- *Broadband Access Service (e.g., connectivity for TACDOH small locations and Corp. Remote Access Users) to customer Network-Based MPLS cloud*
- *Traffic encryption between all or selective TACDOH locations; please outline the technology used.*
- *Provider's future plan to add additional class of service to the current service offering (if any).*

Answer Guidance
Reason For Question: Understanding of provider's MPLS advanced service offerings to support services such as Voice call processing, Video bridging, Multicast, Internet Access, etc. Additional service offerings by the provider may need to be examined by TACDOH for strategic and cost effective plan/architect new Network-based MPLS to accommodates voice network, video network, streaming applications, disseminate corporate communication, remote user access, Internet accesses, etc.
Mandatory Response Format:
Word count: Summary **not exceeding three pages,** outlining provider network base MPLS advance service offering, including but not limited to the advance services listed below. Diagrams identifying how you support these advance service on your MPLS network should accompany the vendor summary.

9.0 AT&T Advanced Service Offerings

AT&T leads the industry with a seamless, consistent global deployment of an MPLS infrastructure that supports an extensive portfolio of MPLS services from every node. Our MPLS capabilities are built on the AT&T Global Network, with high reliability and performance, with tools for customer end-to-end management. Our MPLS advanced service offerings provide customers with the flexibility to add seamless options that fully integrate in the customer's network with the consistency and performance customer applications require.

9.1 IP Multicast Support

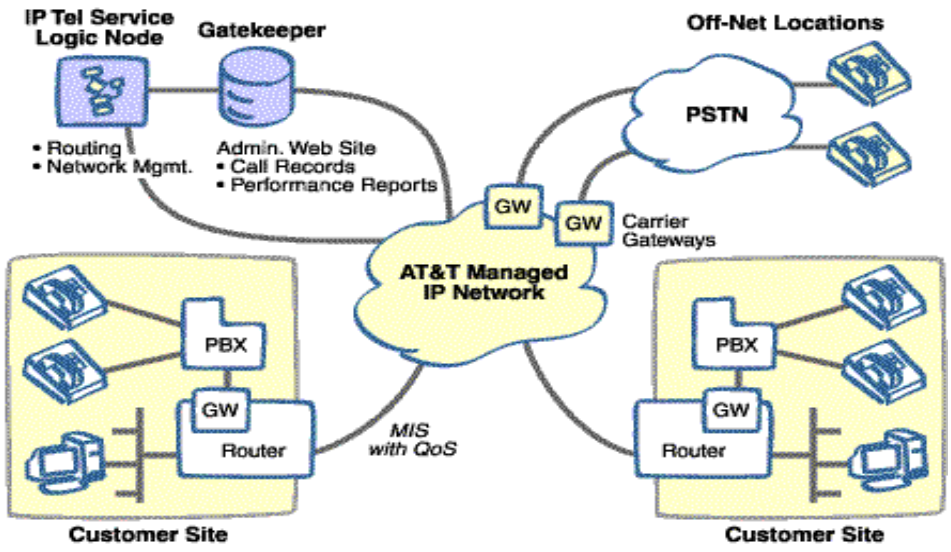
Multicast Enabled VPN (M-VPN) provides a one-to-many and many-to-many multicast transport service within the AT&T network for enterprise VPN networks. In M-VPN, packet replication is performed in the core network, freeing the customer's network servers and/or routers to focus on performing other important enterprise communication tasks and avoids the potential for access links to clog with duplicate copies of the same packet being sent to different remote locations. M-VPN provides an efficient IP multicast transport service to support the deployment of multicast applications by customers.

AT&T's Multicast Virtual Private Network solution is based on IETF specification "Multicast in MPLS/BGP VPN." The multicast peering protocols supported across the Provider Edge-Customer Edge interfaces (CE-PE) are Protocol Independent Multicast Sparse Mode and Protocol Independent Multicast Source Specific Mode. Both modes can be dynamically enabled automatically for each multicast-enabled CE-PE connection. AT&T supports Protocol Independent Multicast (PIM) protocol on CE-PE interfaces used to establish the PIM neighbor relationship with CE routers. It is also used to create VPN specific multicast forwarding entries and discovers Multicast VPN specific RP information (if applicable). The unicast routing information required by PIM on PE-CE interfaces is provided by static routing or eBGP.

9.2 IP Voice Call Processing Functionality
AT&T Voice DNA[SM] provides a complete IP communications solution that includes network-based IP telephony with advanced features, Any Distance calling plans, and a full suite of management services and tools. AT&T Voice DNA[SM] is a single-provider nationwide solution, consolidating local, IntraLATA, and long distance service over AT&T's world-class network, with AT&T TDM Local back-up.

AT&T Voice DNA[SM] can be considered a migration path to true convergence (Voice/Data Integration) because it provides a converged voice/data environment for better network management and simpler access arrangements, as well as addresses the availability of enhanced applications via IP applications interface (e.g., IP Centrex). AT&T Voice DNA[SM] offers interoperability with PBX, IP PBX or IP Centrex; simplified management with one point of contact for local, LD and data; real-time control with an IP PBX and IP Centrex application; and corporate dial plan supporting both local and LD dialing plans. AT&T's provides customers with the ability to add the service on a site-by-site basis and offers 99.99% network SLAs. The IP Local capability leverages AT&T's High-Speed IP Backbone Network, not the public Internet, for voice and data transmission, with an availability target of 99.99%. The service is competitively priced with consistent and predictable monthly costs.

The diagram below illustrates AT&T IP voice call processing.



9.3 IP Video Bridging Functionality
AT&T Videoconference Services offers support for IP Video multipoint conferencing, using the AT&T MPLS backbone. The service offers support for multiple customer ePVCs on AT&T VPN services and provides either multipoint or point-to-point calls for customers and gateway together -- placing ISDN and IP customers on the same call through the video bridge. Calls are either fully assisted or self-serve. Self-serve is available through the AT&T Video Meeting Center customer service web portal.

9.4 Internet Access Services
AT&T Business DSL Internet Service allows broadband access over conventional telephone lines at speeds several times higher than standard 56K or 33.6 analog modems, providing flexible solutions for small office/home office (SOHO), remote branch offices, and telecommuters.

AT&T VPN provides high-speed, managed dedicated Internet access for businesses. AT&T monitors the network 24 hours a day, seven days a week, and maintains the communications link between the customer and the AT&T network. The service provides flexible access options for corporate sites that need access to the Internet or host Web sites on the Internet. Its Unilink feature allows access to the public Internet to connect via a logical channel (LC). Unilink also enables customers to divide VPN

connections into LCs that define individual VPNs within the overall VPN. This capability lets customers separate traffic by divisions, organizations, and/or agencies within their VPN, further defining the VPN to meet their requirements.

AT&T VPN provides a high-performance analog Internet service with access speed up 56Kbps for dial, V.92, ISDN and up to 11 Mbps for WiFi, and wired Ethernet for traveling users worldwide.

AT&T Managed Security Service Network-based provides simple or sophisticated security policies for outbound and bi-directional Internet access and e-commerce applications. It is available for AT&T customers including AT&T VPN services.

9.5 Broadband Access

AT&T offers an extensive broadband service footprint providing economical, high bandwidth access for the AT&T VPN services portfolio. It offers more than 7,000 points of presence in the U.S., managed broadband access in Canada and nine European countries. AT&T expects to continue its aggressive track record in expanding the global broadband footprint.

9.6 Traffic encryption between all or selective TACDOH locations

AT&T supports the use of end-to-end hardware-based encryption through the use of IP Secure (IPSEC) tunnels on Cisco Routers, which use digital certificates for authentication and support advanced routing protocols within the tunnel. Encrypted tunnels can be implemented to address each sites individual need or support the complete network. Customers may choose level of encryption based on site requirements and local legal mandates. Remote access via encrypted IP SEC tunnels is also available.

Encryption enables trading partners and extranet members to securely connect over third party connections to the customers MPLS VPN via AT&T's remote access Virtual Interface Gateway (VIG). All connections that access leverage third party transport are firewalled via a centrally configured inspection hardware based firewall. AT&T's Premise and Network based VPN platforms allow customer to choose different methods of access (Dial, WFI, Broadband, or dedicated), multiple levels of security, and completely granular level of security for each access method to your MPLS VPN. (This customization of end-user security can be configured down to the port level in many designs.) The use of varied access methods and varied encryption methods may allow customers to reduce their total overall network costs while providing robust security solutions.

Many customers also choose to configure their network with a high availability configuration, which may include multiple links or dynamic encrypted tunnels used over a public Internet connection for back or bandwidth on demand.

9.7 Additional features

9.7.1MPLS Tools/Monitoring

AT&T deploys the core network solution that best fits a customer's business objectives. The company keeps its customers updated on the health and status of their network with AT&T developed and/or deployed tools accessible via our award-winning AT&T BusinessDirect® web portal. This web portal provides customers access to alerts, collaboration tools, and shortcuts to their favorite links. It can be personalized for particular roles or responsibilities with built-in help sites and online tutorials. AT&T BusinessDirect® portal also provides a single portal to access multiple service tools for proactive route monitoring, network modeling, real-time flow-thru provisioning, predictive performance management and application monitoring.

9.7.2 Route Monitoring Tools

MPLS uses Multiprotocol – internal Border Gateway Protocol (MP-iBGP) to exchange customer specific routing information. Traffic separation occurs without tunneling or encryption, because it is built directly into the network itself.

AT&T's VPNMon tool pro-actively monitors customer VPN reachability across the AT&T backbone network (edge-to-edge). It detects MPLS VPN-affecting impairments; route distribution impairments within a VPN associated with MP-iBGP sessions between PEs and VPN- RRs (Route Reflectors); VPN-RRs; and changes in the PE-CE link-to-VRF (Virtual Routing and Forwarding) relationship.

9.8 Remote Access

AT&T's flexible access options and the variety of access arrangements the company offers, enable optimal support for remote users, smaller offices and global locations. AT&T network-based VPN interoperates with the AT&T global remote access VPN solution and can provide a single solution for remote access from an end-user's personal computer, or LAN to corporate LANs, intranets, and extranet(s), as well as to the public Internet. Customers can connect to these 'private' networks via access options such as, AT&T Dial (Analog or ISDN), Extended Access Analog or WiFi, AT&T DSL, AT&T Global Managed Internet Service or Third Party access. They can have customer-managed authentication with Secure ID, RADIUS, or Safeword. They also can have dual access that provides access to the network-based VPN and Internet, with support for either registered or unregistered IP addresses, along with IPsec and L2TP support for dial users. No specialized CPE is required and the capability is available worldwide.

Question 10: Price Model and Additional Service Cost

Please provide details of cost components for MPLS service offerings. TACDOH is interested in the following (but not limited to) functional areas:

- *IP Multicast support*
- *IP Voice routing/processing functionality*
- *IP Video bridging functionality*
- *Internet access service*
- *Broadband access service*
- *Adding a new class of service*
- *Traffic Encryption*

Further, describe which services are within the standard price model or enhanced price model (requiring additional cost/customization).

Answer Guidance
Reason For Question: Understanding of cost component associated for additional MPLS service offerings. TACDOH will utilize this as an initial guide to do a cost/benefit analysis to determine the feasibility of additional MPLS services instead of keeping their existing service (voice, video etc.).
Mandatory Response Format:
Word Count: Summary **not exceeding three pages**, outlining provider pricing model for additional MPLS service offering with supporting executive spreadsheets (if required).

10.0 AT&T Price Structure

AT&T has deployed a seamless, consistent global MPLS infrastructure, supporting an industry leading portfolio of competitively priced MPLS services from every node. Our MPLS capabilities are built on the AT&T Global Network, with high reliability resiliency network and access link options.

The AT&T VPN service is structured to support a hierarchy of services from basic transport to application level delivery. The basic AT&T MPLS VPN service recurring monthly charge structure consists of:

1) Local access into an AT&T network access point.
2) A MPLS port charge base on port speed
3) A tiered Class of Service package structure with:
    - Multimedia High (4 classes with a high percentage of Real time traffic)
    - Multimedia Low (4 classes with a low percentage of Real time traffic)
    - Critical Data (3 classes)
    - Business Data (2 classes)

Change charges apply when changing class of service packages on a customer port or upgrading physical access port speeds. There is no charge for Class of service profile changes within the same package.

10.1 IP Multicast Support
AT&T supports a fully integrated, network-based multicast capability as an add-on to the AT&T VPN service. Customers may choose to activate multicast functionality on a port by port basis, allowing a customer's MPLS ports to run both unicast and multicast traffic through a single physical connection and class of service configuration. Charge structure for multicast service is a monthly charge per activated port, and is based on the VPN port speed.

10.2 IP Voice/ Processing functionality
AT&T offers four options for VoIP services over its managed AT&T VPN service: PBX interface packages, on-net calling, U.S. off net calling packages, and International calling.

VoIP PBX Interface Feature Packages: The VoIP PBX Interface Feature Packages include the Service Component bundle necessary to enable a VoIP Site for On-Net calling. The VoIP Feature Packages vary by the number of concurrent calls permitted, the PBX type, and the probable PBX protocols. There also is an option to provide the service through customer-owned CPE.

AT&T Off-Net VoIP Feature Packages: Off-Net VoIP Feature Packages may be ordered for any VoIP Site inside or outside the US from which a customer expects to place calls to Off-Net termination points in the US. These Feature Packages are defined by the maximum number of minutes of calls to US Off-Net termination points ("U.S. Calls") included in the Feature Package for the particular VoIP Site. Customer must also have a VoIP PBX Interface Feature Package in place concurrently with Off-Net Feature Package.

AT&T Off-Net Feature Packages include all US Calls for no additional charge if a customer does not exceed the global aggregate number of minutes permitted under the Off-Net Feature Packages purchased by the customer for all sites. On a monthly basis, all Off-Net calling minutes permitted in all Off-Net Feature Packages ordered for all customer sites globally will be aggregated and compared to the total minutes of U.S. calls for all sites. If there is a usage overage, AT&T will charge a customer a per-minute rate set forth in the Schedule of Charges for the net excess minutes, prorated across the sites that were "over" their maximum number of minutes. A customer will also incur normal PSTN charges for any calls from a VoIP Site that uses the PSTN.

AT&T VoIP Off-Net Non-US calls. Customers can also make calls originating from VoIP Sites inside or, where permitted, from VoIP Sites outside the US to Off-Net termination points located outside the US ("Non-US Calls"). Customer may call Off-Net termination points in any country in the world with telephone service, even if the Service is not available in the country. No matter where in the world an AT&T VPN Off-Net call originates, the gateways where all such calls hop-off onto the public switched telephone network are currently in a limited number of locations in the US and elsewhere in the world, with appropriate interconnection arrangements for US or international PSTN termination. Customer Site will be billed per minute charges for Non-US Calls based upon the country/region being called, and these charges do not vary based on where the call originates. Per minute charges for Non-US Calls apply even where the Non-US Off-Net termination point called is in the same country as the VoIP Site where the call originates.

10.3 Charges for VoIP offerings
1) Per VoIP site one-time installation charges if a site visit is required to install the VoIP card in the router.
2) Monthly Recurring Charges Feature Package Charges.
3) Monthly non-recurring charges such as:
· Charges for US call minutes used by Customer in excess of the global aggregate Off-Net minutes purchased.
· Charges for Non-U.S. calls (even where the non-U.S. Off-Net termination point is in the same country as the originating VoIP site), determined according to the call termination point.
· Charges for US call overage and for Non-U.S. calls are billed in six tenths (6/10) of a second increments; however, there is a 30-second per-call minimum billed for Non-U.S. calls.

10.4 IP Video Bridging Functionality
AT&T is positioned ideally in the market to provide videoconferencing capabilities to enterprises through the integration of the existing videoconferencing and management services with the MPLS network offering. This videoconferencing service model, and thus the customer experience, provided over the MPLS network is identical to that delivered over ISDN today. The model is proven and has been adopted widely throughout the ISDN videoconferencing user base.

AT&T will be providing access from a customer's existing VPN directly into the AT&T Video Operations Center, preserving all the security of the VPN while saving the Customer the cost of ISDN transport. The

set-up cost of the ePVC into the AT&T Video Operations Center has not been determined at this time. The base rates for a videoconference will thus be reduced, by making use of the customer's existing VPN for the video transport. In the ISDN transport model the cost components for a typical dial-out call would be the cost of the bridge port and the ISDN transport for each endpoint. In the IP transport model there is no per minute cost for transport any longer. Thus, a typical 4-endpoint call at 384K speed for 1 hour, using all IP-enabled endpoints, would have significant cost savings at list rates, by converting to the AT&T IP Video offer. This would be a recurring savings with each call.

10.5 Internet Access Service
AT&T's Unilink option allows a customer to order a separate Internet logical channel supported on a single MPLS port in addition to any private VPN logical channels. These multiple logical channels can be used for accessing one or more VPNs, one or more MPLS PVCs, or access into the internet. Each logical channel is associated with a specific amount of bandwidth on the MPLS port to allow proper bandwidth allocation across different resources. A monthly charge is assessed on a per logical channel basis.

10.6 Broadband Access Options
Broadband access can delivered to AT&T VPN through a number of varied technologies.

MPLS DSL Access Connection includes an MPLS port that allows a customer site to connect to the AT&T Network using ATM or Frame Relay protocol, bundled with a DSL access line between the Port and the Customer Site. AT&T also provides and installs an AT&T DSL Modem (either a DSL DSU or a DSL Router) at the customer site, with default configuration settings, including up to 100 feet of inside wiring from the LEC minimum point of entry (not to exceed two hours of inside wiring work).

An IP MPLS port allows a customer site to connect to the AT&T Network using Internet Protocol. Two types of IP MPLS ports are available: IP MPLS ports supporting PPP IP format and IP MPLS Ports supporting Frame Encapsulation IP format. Subrate ports are also supported for DS3 speeds at 5M, 10M, 15M, 20M, 25M, and 30M. For OC3 speeds at 50M, 75M, and 100M and for OC12 speeds at 200M, 300M and 400M.

Remote Access: The AT&T Network Based IP VPN Remote Access services introduce a standard set of capabilities to access data and IP Network Based VPNs. This offer will provide remote access/SOHO capabilities on AT&T's MPLS network. Customers using remote access can connect to these private 'networks using any of the following options:

- AT&T Dial (Analog or ISDN)
- Extended Access Analog or WIFI
- AT&T DSL
- AT&T Managed Internet Service/Global Managed Internet Service access.
- Third Party Access (Access circuit is not ordered or managed by AT&T) broadband or ISP dedicated.

10.7 Adding a New Class of Service
AT&T has a robust and flexible class of service management capability, allowing customers to easily tune class of service on their MPLS ports to support differing application profiles. Class of Service profiles, like other customer specific IP VPN configuration changes, can be managed through the AT&T BusinessDirect® Portal. Once the IP Class of Service changes has been submitted, the changes will flow through automatically into customer VPN. This provides customers a 'Class of Service on Demand' capability, used with the introduction of new applications into the network, or changes required during specific times during the year.

There are two types of changes for class of service management, a request of a class of service profile that changes the number of class of services supported on a specific MPLS port, or requesting a change in class of service profile, which changes the amount bandwidth allotted to each existing class of service on the MPLS port.

- Changing Class of service profiles – This allows customers to tune the amount of bandwidth each class of service is allotted on a MPLS port, within the Class of the Service package that was initially ordered.

This is considered a configuration change and does not alter any of the customer's monthly network charges.

- Adding additional classes of service – Classes of service may be added to a MPLS port by changing the class of service package that is applied to the port. Each package establishes the number of classes that are supported on a port. The packages, either Multimedia High or Low, Critical, or Business data, will have a monthly class of service charge associated with it.

10.8 Traffic Encryption

Traffic encryption will be supported on the AT&T VPN CE router with IPsec tunneling either to the AT&T MPLS network or to an alternate network for network diversity. Pricing will involve a monthly recurring charge and setup charge.

Question 11: CE Deployment Time/Cost

Please provide details of how vendor would approach an MPLS deployment for an organization the size of TACDOH. TACDOH is interested in the following (but not limited to) status areas:

- *Change Bandwidth (CDR) associated for specific Class of Service*
- *Change the status of classes of services (e.g., upgrade from one class to three classes)*
- *Change the status of an application in class of service; Add a new application to a class of service or remove it from particular class of service (e.g., in case of additional marking required on the CE device)*
- *Change the current status of CE from partial cloud to Any-to-Any connectivity or visa-versa*

Answer Guidance
Reason For Question: Understanding of cost component and business downtime associated with change order request for Network-Based MPLS service offering.
Mandatory Response Format:
Word Count: Summary **not exceeding two pages** describing the implementation duration, service upgrade/downgrade (if any) and the cost associated to provide these services per CE.

11.0 AT&T CE Deployment Time/Cost

11.1 Change Bandwidth CDR for Specific Class of Service
Class of Service Feature for Multi Protocol Label Switching Connectivity
CoS is a feature of AT&T VPN that allows Customers to classify application traffic into different levels of service. Customer traffic is differentiated at the CPE router into classes of service with a maximum of 4 classes:

COS1: Designed for voice and broadcast video transmissions.
COS2: Designed to carry premium business applications with strict requirements in terms of end-to-end delay and end-to-end packet delivery.
COS3: Designed to carry standard business applications with strict requirements in terms of packet delivery and delay constraints.
COS4: Designed to carry general business applications without strict requirements in terms of packet delivery and delay constraints.

The CPE uses this classification to differentiate the traffic and to prioritize the applications before transmission through the network. The objective is to provide critical applications with service before less critical applications and to help optimize access link utilization. In the case of access congestion, high priority application traffic takes precedence.

11.2 Change the CoS Status
To implement or change the class of service feature, a customer completes a matrix where they indicate which application traffic should be associated with which class, and what bandwidth requirement is needed for each class. This matrix can be built with assistance from AT&T designated personnel. All AT&T VPN customer traffic must have a CoS classification. If customers do not request a specific CoS, the AT&T VPN traffic will be classified by AT&T as CoS3. If customers specify CoS differentiation at a site but an application is not mapped, then that traffic for the unmapped application will be classified as CoS4.

Customers may use the following parameters to classify traffic: origin IP address, destination IP address, input interface, port number and application protocol.

The CoS feature is designed to provide a minimum bandwidth to every class of service, while providing a strict priority to CoS 1 and 2 Class of Service reports are provided optionally for all classes (CoS 1-4) and cover:

1) Router Traffic Usage by CoS.

2) Router Traffic Behavior by CoS.
3) Site to Site performance/latency reports by CoS (for qualifying pairs).

The percentage of bandwidth associated with each CoS represents the amount of data in bits per second of the Managed Access Connection capacity committed for transporting data in that CoS per customer site. For Classes of Service 2-4 in single VPN solutions, bursting may be allowed up to the total bandwidth of the MAC. When customer connects multiple VPNs sharing the same Managed Access Connection, the bandwidth for each VPN using the MAC, including burst (if any), must be allocated such that the sum of all CoS percentages for all VPNs does not exceed the Managed Access Connection bandwidth. The bandwidth allocated to each VPN using the MAC cannot be shared.

Adds and changes to Class of Service Mappings. Changes to Class of Service and application mappings to CE configurations are done through requests through the BusinessDirect® customer portal. In the case a service engineer is involved, the changes will occur within 24 hours.

11.3 Changes in Status of Applications
Changes in class of service percentages or application mappings involve a one-time charge on a port basis, additions or deletions of specific classes of services will trigger a billing event, changing the Class of Service traffic package that is applied to a specific port.

11.4 Changes in the current status of CE from partial cloud to any to any connectivity or vice versa.
AT&T currently meets the customers' community of interest by allowing customers to configure multiple VPNs from the same physical ports to form the community of interest VPN.

AT&T is planning to offer Modular VPN and Route Group feature sets in the near future to address more specific community of interest requirements.

AT&T is developing a proprietary routing functionality that will provide a scalable way to implement route group, for customers who require logical level community of interest restriction on their routing.

Our Modular VPN feature will allow customers to create hybrid VPN topology, to have multiple partial mesh VPNs to be connected either via partial mesh or any-to-any VPN topologies.

Question 12: Global Network Strategy

TACDOH is interested in how the vendor can deliver global MPLS service. Please address the following functional areas:

- *MPLS Interoperability with other providers (e.g., Inter AS MPLS VPN); full cloud visibility with class of service.*
- *Inter-providers connectivity (e.g., DiffServ Gateway); partial cloud connectivity with class of service mapping.*

Answer Guidance
Reason For Question: Understanding of the provider's peering capability with another provider and how TACDOH can utilize this functionality to save on internal peering cost and connectivity to extranet partner between different providers MPLS cloud. This will allow TACDOH to understand the global connectivity reach and how the selected providers will honor TACDOH class of service marking and prioritization across two separate providers' management plane/domain.
Mandatory Response Format:
Word count: Summary **not exceeding two pages**, outlining provider's network base MPLS global strategy.

12.0 Global Network Strategy

AT&T leads the industry with a seamless, consistent global deployment of an MPLS infrastructure that supports an extensive portfolio of MPLS services from every node. Our MPLS architecture is built on the AT&T Global Network, with high reliability and performance, with tools for customer end-to-end management.

12.1 AT&T MPLS Interoperability with other providers

AT&T provides restricted MPLS level interoperability, depending on geographical and economical situations. We currently have implemented in certain countries and plan to extend to a few more. The current implementations maintain AT&T's four CoS feature integrity end-to-end for the customer, including across the Inter-AS boundary. Full cloud visibility is supported.

12.2 AT&T Inter-provider connectivity

AT&T offers Layer 1, Layer 2, and Layer 3 inter-providers connectivity. However, we are not using the third party DiffServ gateway service. Since DiffServ is a Layer 3 capability that rides over the lower transport mechanisms, for Layer 1 or Layer 2 inter-provider implementations, it is transparent. Regarding Layer 3 inter-provider service, AT&T works with partners to align our CoS policy and treatment, so necessary CoS mapping will be implemented.