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.

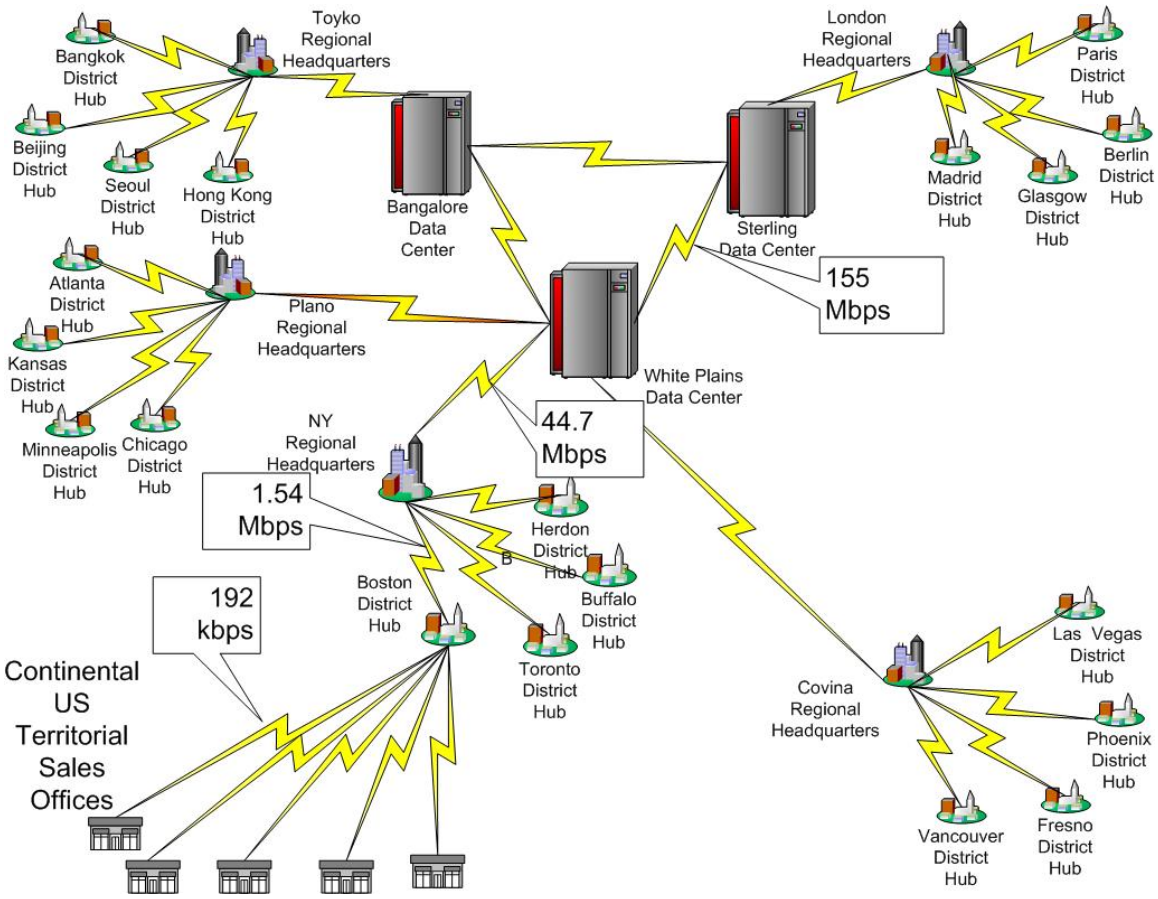
TacDoh is growing into new areas and requires a geographical coverage explanation from each service provider. The granularity should list world regions that are part of the service provider's native coverage and regions that will be covered using partners. In the case that more than a single partner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

Qwest provides a formatted customer billing file.

- Break out usage and cost into territory, district, region and data center subsection based on a three year contract.

Addressed in attached Monthly Pricing Sheet

- Intelligently and cost effectively support the named TacDoh applications

Addressed in Body of response.

- Provide 24/7/365 support for troubleshooting of circuit connectivity

Addressed in Body of response.

- Provide network backup using public (Internet) and private options

Located in Question 5 and Monthly Pricing

- Provide self provisioning if available

See description of Q.Control - Question 5

- Replace current Frame Relay network with MPLS where possible

Addressed in Body of response.

- 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.

Located in Question 5 and Monthly Pricing

- 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)

See attached Excel document.

B. MPLS Vendors Questions: General Guidance

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

Question 1: MPLS Service Offerings

Please provide a high-level description of your current Network-based MPLS service offering, including details of 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.

Executive Overview:

The Qwest Network based MPLS service offering is built on a nationwide OC-192 core IP/MPLS network. The Qwest network is a single Global AS with approximately 94 major POPs that are interconnected with OC-192 wavelengths. The smaller regional POPs are connected via SONET circuits ranging from OC3 to OC48. Most of the network was built within the last 5 years, starting from the optical layer to the Layer 3 network elements. This has given us the luxury of not having to accommodate legacy architectures in our MPLS network. Qwest was an early adopter of MPLS Fast ReRoute technology to provide sub-second failure recovery in the core IP/MPLS network, and has had this technology operational since 2001. The transport elements of this core network are built on Qwest's own fiber facilities, giving Qwest access to abundant amount of optical transport capacity. Internationally, Qwest has MPLS PE routers deployed in Tokyo, Hong Kong, Singapore and Sydney over Qwest owned transport facilities, Qwest is able to deliver a global network solution through network interconnections with partnership arrangements. These network interconnections occur at the TDM (transport/Private Line) layer, ATM, FR, IP and MPLS layers, allowing Qwest to support all of these network options for customers with international locations.

MPLS Service Technical Description:

Qwest initially deployed RSVP (Resource Reservation Protocol) in 2001 – RSVP is a signaling (control plane) protocol that allows MPLS Label Switched Paths (LSP's) to be signaled across the network. Qwest has spent six months maturing the RSVP network implementation. Initially, this MPLS deployment did not result in commercially available MPLS services, such Fast-ReRoute "protected" LSP's were used primarily for carrying VoIP traffic between the Qwest Class 4 switches and to augment traditional TDM interconnections between such Class 4 Voice switches with "IP trunks". Once ready for production, Qwest began to actually carry forwarding (data plane) traffic across such RSVP signaled, Fast-ReRoute protected LSPs. Qwest is currently carrying approximately 2.3 Billion MOUs (Minutes of Use) of such VoIP traffic across its MPLS backbone -- transparently to users of its Long Distance Voice service.

Qwest deployed an RFC2547bis Layer 3 VPN service using LDP signaling with MP-BGP for VPN-v4 route distribution in early 2002, and announced commercial availability of MPLS L3 VPN services in late 2002. The first generation of the commercially available Qwest MPLS VPN service was offered on "shared" Provider Edge (PE) routers – i.e. PE routers that were serving the needs of MPLS as well as Internet customers. Such routers were connected to the Internet and shared their data and control planes with the Internet.

The second generation of the commercially available MPLS service from Qwest made use of "Private" PE routers – such routers are not connected to the Internet, and are "invisible" to the Internet. These Private PE routers are exclusively serving MPLS VPN

customers, and do not connect customers to the Internet directly. This service has been available since late 2003 and is referred to as Qwest iQ Networking™.

Qwest iQ Networking Executive Overview:
Qwest iQ Networking makes it possible for Enterprise customers to more easily build an integrated network that includes various access and network technologies, with options to overlay Managed services, Security services and VoIP service on top of the Enterprise Network. Internal systems, processes and workflows have been built from the ground up in support of Qwest iQ Networking, resulting in a seamless service experience for the customer at all stages of their engagement with Qwest, regardless of the technology/service choices the customer makes.

Qwest iQ Networking is a strategic initiative that shifts focus from the traditional approach to building products that are oriented around particular technologies (e.g. ATM, MPLS, FR, etc.) and servicing customers with a silo-based approach centered around each technology. Although Qwest has made huge investments in ensuring that its network is state-of-art, we recognize that our ability to differentiate ourselves from the competition is not just based on having the most technically superior network, but more importantly, in our ability to make it easier for the customer to build and operate their networks. Qwest recognizes that Enterprise customers want to the have flexibility of construct building networks utilizing the best technology options that are available to them that match their demands for price and quality – for example, using protected TDM access for key locations where bandwidth guarantees are critical, Ethernet access where traffic demands can be seasonal, DSL access where cost is the most important factor, and ATM/FR access to support legacy needs..

Key Differentiators:

- The Network based MPLS service is built upon an OC-192 national backbone that is also Qwest owned (i.e. Qwest is a facilities based network operator).
- Since 2001, Qwest has employed MPLS Fast-ReRoute deployed in the core network that guarantees sub-second failure recovery.
- Private PE routers that are deployed exclusively for MPLS VPN services provide for a complete separation of traffic from the Internet.
- Industry leading Service Level Agreements (SLA) defined by Core backbone optimization and sustained performance for reliability, redundancy, minimal latency and jitter, as evidenced by the 2.3 Billion minutes of voice traffic it is carrying per month. There is not a better test that can be designed to validate the quality of the Qwest IP/MPLS backbone, which is being tested every minute of every day with such massive amounts of critical, real-time, delay and jitter sensitive VoIP traffic flowing across the Qwest IP/MPLS nationwide backbone.
- International presence with Qwest owned facilities and partnership arrangements for global reach and coverage.
- Qwest iQ Networking, Qwest's approach to deliver a service experience to its customers that transcends traditional technology boundaries for the small, medium, and large private and public-sector customer.

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

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" - Layer 3)*

Qwest currently provides Layer 3 VPN employing BGP/MPLS VPNs "RFC2547bis",on our MPLS backbone. The modus operandi at Qwest is to deploy new technologies and protocols for internal use only and to allow such early implementations to mature, before building commercial offerings on such platforms. This is evidenced by the fact that MPLS was deployed initially for over a year for its FRR capability (internal use only) before a commercial MPLS L3 VPN service was built on the same infrastructure. Similarly, the commercial rollout of VoIP benefited from over 4 years of operational maturity, during which Qwest was using the IP/MPLS backbone to replace TDM trunks between its Class 4 switches. Qwest is currently testing and evaluating the use of MPLS L2 VPNs for carrying ATM/FR traffic between its ATM switches and plans to commercially make available a Layer 2 VPN service in the near future, benefiting from the operational maturity of such technology within the Qwest network.

- *Access and control plane*

For the control plane, Qwest employs iBGP to establish peering between the BGP Route Reflectors and the Private PE's for creating Virtual Routing and Forwarding tables and for exchanging customer network routes. This control plane is separate from, and is independent of the "Internet" BGP routing, i.e. these Route Reflectors are only serving the Private PE routers that are its RR-clients for the exclusive purpose of VPN-v4 Route Distribution (not Internet routes). From a data plane perspective, all Private PE routers are dual connected into the core IP/MPLS backbone and are dedicated for VPN customers only, and do not carry any Internet traffic, in fact they are incapable of receiving or sending any traffic to the Internet, since they have no control plane (routing) visibility to the Internet.

- *Provider (P), Provider Edge (PE), Customer Edge (CE) technology*

Qwest combines Juniper M160 Provider core routers with Juniper M40 Provider Edge routers for a total MPLS solution. TacDoh has the discretion to use any CE router that meets their specific needs. Qwest can provide recommendations of CPE make and models after assessing the specific requirements, and also offers a managed service option for such CPE.

- *Routing protocols between PE and CE*

Qwest supports static or eBGP routing between the PE and CE.

- *Traffic engineering within the core (such as LDP, CR-LDP, RSVP-TE)*

Qwest uses RSVP-TE for optimal load distribution for very specific requirements (on an exception basis). Traffic Engineered LSP's are more of an exception in the Qwest backbone rather than the rule, and are typically used in specific cases as a short-term solution for traffic management. In general, Qwest's traffic management philosophy relies on "right-sizing" the network to handle the traffic offered to it by planning and making available capacity much before it is actually needed. Every

Qwest TeraPOP is connected via multiple backbone circuits to a minimum of two (in most cases three) other TeraPOPs over diverse physical facilities. Usage reports are gathered for all such backbone circuits (defined as those circuits that interconnect core backbone devices) and reviewed weekly. Any individual backbone circuit with 95th percentile utilization greater than 40 percent or peak utilization greater 60% (over a given sampling period) is flagged for upgrade. In addition to simply monitoring circuit utilization under normal operating conditions, traffic flows on the backbone are regularly modeled for potential failures (due to fiber cuts/hardware failures, etc.). This modeling helps predict traffic utilization patterns due to abnormal network conditions. Using such modeling data we are able to identify those backbone circuits that must be upgraded to conform to the planning threshold of 40 percent utilization even under failure conditions. Although Qwest's primary approach is to make adequate capacity available for normal as well as abnormal network conditions, Qwest is also evaluating the use of Bandwidth-reserved LSP's across the core network for certain traffic types –- the current network architecture with physical separation between those network elements at the edge of the network serving different services (VPN, Internet, VOIP) lends itself naturally for such an architecture.

Summary:
Qwest's design goal for the backbone is 100 percent packet delivery. The network uses Multiprotocol Label Switching (MPLS) fast re-route for redundancy and trunk fail-over in the network. Qwest's network boasts a sub-100-ms routing recovery time in the event of a network outage, as opposed to the 15 - 30 seconds on traditional SONET healed networks that rely on standard IGP (Interior Gateway Protocols) for failure recovery. This ensures that network availability for sensitive applications such as VoIP and Video don't suffer if there is a link/node failure in the network. There are over 2,200 Access POPs to bring customer traffic onto the network and 94 IP Router locations (Including TeraPOP's, IP AccessPOP's, Layer 3 Facilities and CyberCenters). Qwest provides tools for customers to view the performance of the Qwest IP/MPLS network. Performance statistics for the core IP/MPLS backbone are publicly posted, and may be viewed at http://stat.qwest.net (The Agilent Firehunter tool is used to gather and report these statistics; it is not based on a proprietary Qwest tool).

Qwest continues to rank highly among its competitors in network reliability, resiliency and latency/jitter measurements with one of the largest and best-performing IP networks in the world, the Qwest network features over 114 Gbps of aggregate peering capacity. The network ensures low latency/jitter with one of the most aggressive performance metrics guarantees in the industry—50 millisecond (ms) average round-trip network delay SLA within the US and 95 ms average round-trip delay between the Qwest network and other leading networks in the industry. Some of the features of Qwest iQ Networking service are:

- 100% network availability guarantee
- 50ms Latency
- 99.50% packet delivery guarantee
- 10-minute outage notification via e-mail
- <2ms Jitter
- Around-the-clock support with 24-hour customer service
- Full range of available access bandwidths: DS-0, NxDS0, DS-1, NxDS-1, DS-3, OC-3, OC-12 and OC-48, and access options including ATM, FR, Dedicated access (PPP/HDLC) (current) and Ethernet, DSL (future).

- *Provider CE offering (Managed CE, non-managed CE or both)*

To manage all TacDoh's CE Qwest offers Integrated Management, a complete, fully integrated product suite that provides TacDoh comprehensive out-tasking of part, or

all, of your data network. TacDoh can focus on specific internal business and IT management needs, while Qwest manages your data network. With Qwest Integrated Management, you get all the inherent out-tasking advantages, such as lower network costs and minimized personnel complications, as well as continuously updated technology and polices. TacDoh can rest assured that Qwest is effectively and efficiently managing the TacDoh data network.

Features

You can choose from the following service options:

- **Integrated Management–Select**
  - – Network inventory and topology map
  - – In-band 24/7 monitoring of customer devices and Qwest data transport
  - – Fault management to isolate and correct any troubles
  - – Configuration management services, including: design, provisioning, backup, comparison and restoration
  - – Online reports documenting network performance
  - – Web-based portal for access to the ticketing system, reports, inventory and topology map
- **Integrated Management–Comprehensive**
  - Includes all of the features of Integrated Management–Select, plus:
  - – 24/7 monitoring of non-Qwest transport
  - – Total customer agency for resolving issues with non-Qwest transport and customer premises equipment (CPE)
- **Integrated Management– IPsec Tunnel Management**
  - Includes all of the features of Integrated Management–Comprehensive, plus:
  - – Configuration of site-to-site virtual private network (VPN) connectivity

Qwest also has resell arrangements with equipment vendors (e.g. Cisco , Juniper, Tasman, etc.) to make procurement easy for the customer.

- *Identify any use of 3rd party infrastructure*

Within the U.S. Qwest's backbone network does not rely on any 3rd party infrastructure. The Qwest Wavelength and SONET networks are built on Qwest owned fiber facilities. The IP/MPLS backbone in turn is built on Qwest owned Wavelength and SONET networks, so that there is no reliance on a 3rd party to plan for and upgrade network capacity as needed. In addition to this domestic network that is fully Qwest owned (starting from the fiber to the transport to the IP/MPLS layer), Qwest's network also extends into Tokyo, Singapore, Hong Kong and Sydney. Outside of these cities in Asia and the domestic U.S. Qwest relies on network interconnections with its international partners to deliver service outside the continental US.

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).

Per Section B, Question 1, Qwest offers a suite of IP/MPLS based products referred to as Qwest iQ Networking™.

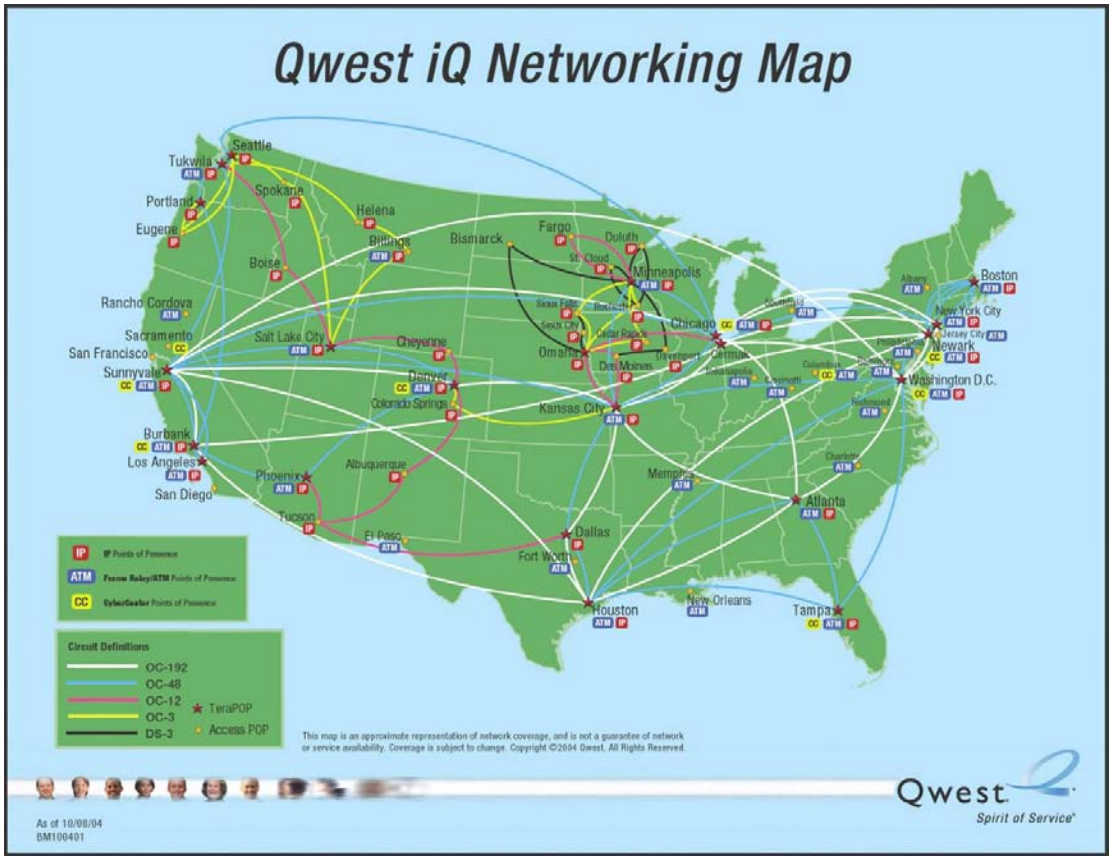
Qwest iQ Networking accommodates the need for constructing modular wide area networking solutions. TacDoh will be able to implement solutions tailored to their specific business requirements. Many of TacDoh's networking hard cost investments are protected since TacDoh can use existing customer premises equipment (CPE) and Layer 2 access environments such as Asynchronous Transfer Mode (ATM) and Frame Relay. Qwest iQ Networking encourages and fully supports the convergence of Layer 2 access technologies to connect into the Qwest IP/MPLS network backbone. Qwest iQ Networking will accommodate TacDoh's need for an easy to design multi-node, any-to-any intranets or extranets solution that extend secure connectivity to remote TacDoh locations, trusted vendors, suppliers and customers.

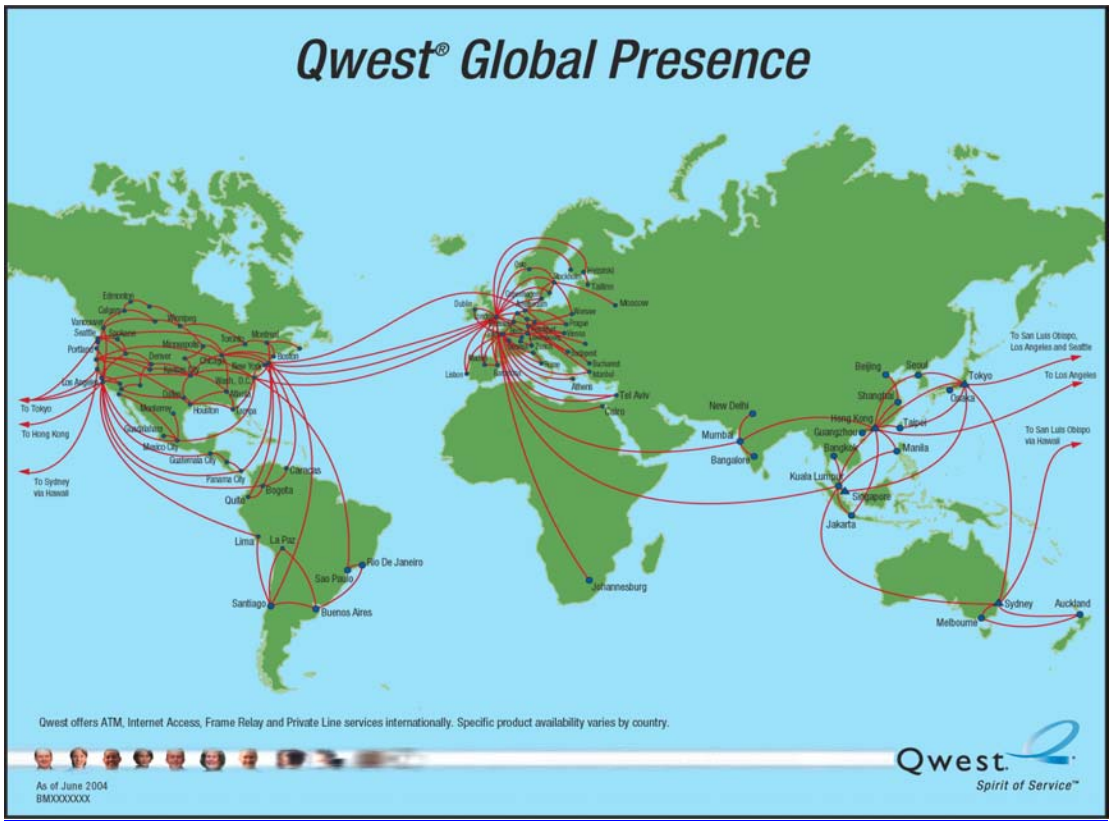
US IP Backbone

Locations of the Qwest IP POPs (termed "TeraPOPs") are provided on the attached domestic IP map. Qwest's TeraPoP facilities are used to expand Qwest's MPLS PE networking convergence footprint. Additionally, Qwest has four on-net Pacific Rim/Asia TeraPOPs (Tokyo, Hong Kong, Singapore and Sydney), as well as partnerships throughout Europe and the rest of the world to provide Global IP connectivity.

The logical layout of the TeraPOPs includes two or three Core Routers (Juniper M160s) providing redundancy. Each POP is multi-homed to other POPs to provide diversity in the event one path should fail. Additionally, each Edge Router (which connects to the customer) is multi-homed to two Core Routers, providing redundancy to the edge for customer traffic.

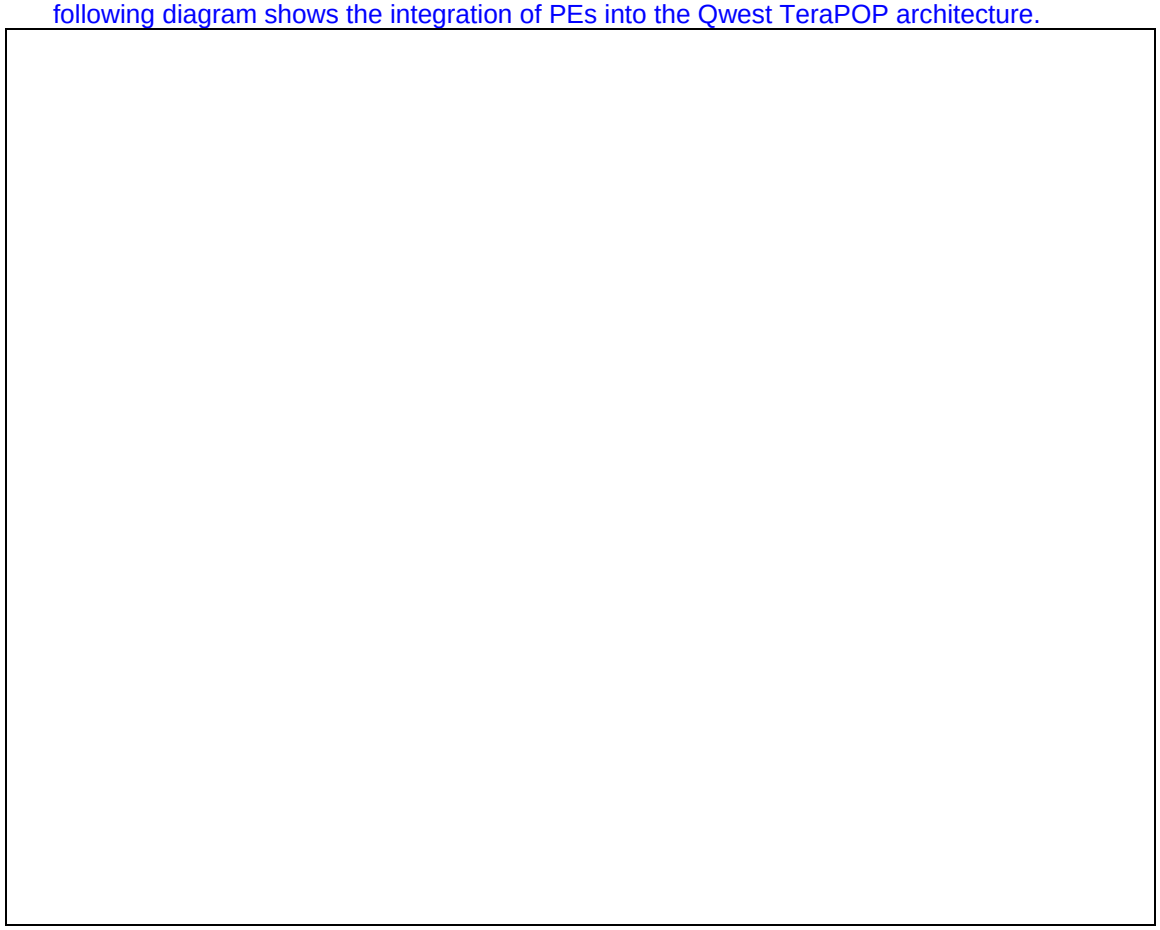
IP TeraPOPs are located in Atlanta, Boston, Burbank, Chicago (2), Dallas, Washington DC (2), Newark NJ, Houston, New York City, Kansas City, Los Angeles, Sunnyvale, Tampa, Denver, Omaha, Minneapolis, Phoenix, Salt Lake City, Portland, Seattle, Tukwila, Spokane, Eugene, Boise, Helena, Billings, Cheyenne, Tucson, Albuquerque, Colorado Springs, Bismarck, Fargo, Duluth, Rochester, St. Cloud, Sioux Falls, Sioux City, Des Moines, Cedar Rapids, and Davenport. In addition to these IP TeraPOPs, Qwest has 9 CyberCenters (Hosting Centers), and approximately 30 Collocation sites across the U.S, for a total of 94 IP enabled POPs. Such "IP enabled" POPs are those POPs where a Layer 3/IP termination is possible into a Router. Beyond these 94 IP enabled POPs, Qwest has 2,200 transport access nodes where customer loops can be interconnected into the Qwest national transport backbone for TDM services.





US and Asian Provider Edge Physical Topology and Locations

In the US, Qwest MPLS VPN Edge (Provider Edge or PE) routers are deployed at 11 locations. As customer growth and demand increase, additional locations will be added. In all US locations, PEs are deployed in pairs for redundancy. In the initial deployment, each PE has an OC12 connection to a separate Qwest ATM switch, as well as dual OC48 uplinks to different TeraPOP Core Routers. The OC12 connections support both ATM and Frame Relay access. Private Line Access ("Dedicated IP Access") from DS0 to OC48 speeds is provided by TDM or SONET connections to the same PEs. The following diagram shows the integration of PEs into the Qwest TeraPOP architecture.



Currently, PEs are deployed in these 11 domestic cities: Atlanta, Burbank, Chicago, Washington DC, Houston, New York City, Kansas City, Sunnyvale, Tampa, Denver, Seattle, Tucson (8/05) Additionally, PEs are now in place in Hong Kong, Tokyo, and Singapore. The customer locations need not directly overlap with these PE's. Qwest's national transport backbone has an excess of 2,200 transport nodes that the customer access can be terminated to and then backhauled over the SONET protected Qwest transport network to the closes MPLS PE. Qwest continually evaluates demands that may drive expansion plans beyond these 11 domestic sites, and has plans to expand this footprint as driven by capacity demand.

iQ networking Port Types

To facilitate access and customize the TacDoh network solution, TacDoh will select individual site locations to utilize a standard set of features from Qwest iQ Networking's Port Type Portfolio. The Port Type Portfolio is comprised of Internet Port, Private Port, and Enhanced Port. Each port type offers a variety of WAN topology control and a range of port speeds, including 56 Kbps to 2.4 Gbps. Different MPLS networking features are included within each Port type bundle. This product approach by Qwest offers TacDoh the ease of configuration to select the correct port bundle and avoid the confusion of paying for incremental features in a traditional Network Service Provider's a la carte model of pricing for feature. . As TacDoh' requires expanded levels of feature functionality, TacDoh can switch to another port classification.

- **Internet Port** – Provides customer locations with connectivity to the Internet from 94 IP POPs nationwide.
- **Private Port** – Provides WAN connectivity between customer locations. Customers have the options to allocate traffic to point-to-point Layer 2 connections or Layer 3 MPLS.
- **Enhanced Port** – Provides all of the functionality of both an Internet Port and a Private Port in a consolidated communications solution, over a single access loop.

TacDoh can mix and match port types within Qwest iQ Networking. For each Qwest iQ Networking port, Qwest provides associated local loop access. Customer-provided access is permitted with domestic ports. Certain access types may not be available for all iQ Networking Port types.

Types of Qwest iQ Networking access types are as follows:

- **Dedicated IP Access** – Special access local loop connection from customer premises to Qwest IP POP.
- **Dedicated ATM Access** – Special access local loop connection from customer premises to Qwest Communications Corp. (QCC) ATM POP, terminating on Lucent® 500/550 architecture and then interconnected to Cisco/Juniper Qwest iQ Networking infrastructure via a virtual connection.
- **Dedicated Frame Access** – Special access local loop connection from customer premises to QCC Frame Relay POP, terminating on Lucent 500/550 and then interconnected to Cisco/Juniper Qwest iQ Networking infrastructure via a virtual connection.
- **ATM Partner Access** – Local loop connection from customer premises to local exchange carrier (LEC) ATM POP that is interconnected to QCC ATM POP via a user network interface (UNI), and then interconnected to Cisco/Juniper Qwest iQ Networking infrastructure via a virtual connection. ATM Partner Access currently includes in-region Qwest Corporation (QC) connectivity in 14 local access and transport areas (LATAs). In the future, additional ATM Partner Access options are expected.
- **Frame Partner Access** – Frame Partner Access is a Local loop connection from the TacDoh sales office to LEC's Frame Relay POP that is interconnected to Qwest's Frame Relay network via a NNI. Once on the Qwest frame network the user can now access Qwest's IP private and or public MPLS based service. In addition to offering frame relay within our 14 state LEC territory, Qwest has established NNIs with Verizon, Bell South and SBC giving Qwest a highly dense nationwide frame relay footprint.
- **Secure Remote Access** – Remote Access dial service with secure IPSec client used for broadband connections or dial up service provider connections.
- **Ethernet Access** – Local loop connection from customer premises to Qwest IP POP, terminating on Ethernet interconnection switch and then interconnected to Cisco/Juniper Qwest iQ Networking infrastructure.

- **Coming late 05 early 06**
  - ß National WiFi
  - ß National DSL

NOTE: *Enhanced Port connectivity with Dedicated IP Access is not currently available. These options are anticipated with future releases of Qwest iQ Networking.*
** Qwest Local Access (the loop) is a separate service.*

Question 4: MPLS Contingency/Backup Solution

Please provide details of your Network-based MPLS contingency solutions to ensure both service continuity and 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

To accommodate TacDoh's redundancy needs Qwest will offer a redundant MPLS port of equal capacity at all domestic and Asian locations. These redundant links will be provisioned with Qwest's diversity options which include:

- Access loop diversity – Second local loop between TacDoh premise and Qwest access POP. Qwest with not guarantee Telco Central Office redundancy with standard loop diversity, as this often requires special construction from the telco to ensure a diverse cable router to a diverse Central Office.
- Router card diversity – Second Port on separate card within the same router
- Router Diversity – Second port on separate router within the same TeraPOP.
- IP POP Diversity –- Second Port on a router in a separate TeraPOP.

Based on TacDoh's business continuance needs Qwest proposes the following diversity options by site type:

Data Center	Access Loop and POP Diversity
Regional Headquarters	Access Loop and Router Diversity
District Hubs	Access Loop and Router Diversity
Territorial Sales offices	Dial back-up for order entry moving to DSL when and where available.

The Primary ports will use a standard flat rate pricing method while the redundant ports will be priced using Qwest's Data Transfer billing method. Data Transfer is a usage sensitive pricing method that bills based on the amount of gigabytes transferred. This is an ideal billing method for back up service. A small minimum monthly fee, listed under Monthly Cost, will be applied to ensure port availability.

For the European locations Qwest will use BT's frame relay service. This is not an MPLS based service, however Qwest can extend our MPLS network to international locations through frame relay with one of our international partners. The backup design has Sterling as the hub and single PVC to Qwest's domestic MPLS along with individual PVCs to London, Glasgow Paris, Berlin, and Madrid, all of these locations have a single port back to Sterling.

Because TacDoh's has an existing Frame network in Europe, it may make sense for TacDoh to continue to use that network for backup and get a single OC3 frame port and PCV to Qwest's domestic MPLS network. However for the purposes of this response Qwest has priced out the recommended infrastructure so TacDoh can understand all costs involved.

Finally, for the sales offices, because the required bandwidth at this time is only 192k, Qwest is proposing using Qwest Remote Access, a dial back up service for secure remote access, utilizing an embedded commercially available client known as ROVA™. Qwest's Remote Access dial service utilizes the public Internet for the transport. The ROVA client supports IPSec encryption for a secure connection back to the host facility. Qwest Remote Access will enable order entry to take place from individual sales offices should the primary network be unavailable. We expect that applications like VoIP would be out of commission, but since most sales staff has an alternative voice service through mobile phone, we believe they will survive short to moderate outages.

Qwest expects to have DSL availability as an access type into our iQ Networking suite of products in six to eight month. Once available Qwest will propose DSL as either primary, depending on reliability and price or as back up where available to continue to right-size the TacDoh network solution purchased from Qwest..

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.*

Qwest iQ Networking supports a standard three Class of Service queue architecture, utilizing DiffServ with High or Strict priority queuing methodology in the network. Qwest will add full support for four Class of Service queues by late 2005.

- *Recommended or restricted applications characteristics for each class.*

Real time, priority data, non-priority data

Qwest currently offers three classes of service with standard traffic allocation templates that include the option of Low-Latency-Queuing (LLQ) queuing or Weighted-Fair-Queuing (WFQ) for traffic in Priority Queue 1 and WFQ for Priority Queues 2 and 3. The LLQ option is recommended for real-time interactive applications such as VoIP, although Qwest does not place any restrictions on the kind of traffic the customer chooses to classify into any of the Queues. Qwest recommends using the LLQ option for jitter/latency sensitive real-time applications in the Priority 1 queue, priority enterprise applications in the Priority 2 queue (e.g. CRM, SCM or ERP applications) and all other application traffic in the Priority 3 queue (e.g. email, file-transfer, other non-real time, non-critical application traffic). In the case where the customer does not have any application traffic requiring the LLQ option on Queue 1, the customer has 3 priority queues using the WFQ scheduling algorithm to service each of the 3 priority queues as per the QoS template chosen. A sample of some templates that are supported currently include (this is not a complete list) –

Template #	Queuing	Priority 1	Priority 2	Priority 3	Comments
1	LLQ (up to port speed(, WFQ, WFQ	80%	10%	10%	Queue 1 (LLQ) can burst up to port speed, likely to starve other queues
2	LLQ(rate limited, WFQ, WFQ)	60%	10%	30%	Queue 1 (LLQ) is rate limited, Queues 2 and 3 (WFQ) will not starve.
3	LLQ(rate limited, WFQ, WFQ)	40%	10%	50%	Queue 1 (LLQ) is rate limited, Queues 2 and 3 (WFQ) will not starve
4	LLQ(rate limited), WFQ, WFQ	30%	20%	50%	Queue 1 (LLQ) is rate limited, Queues 2 and 3 (WFQ) will not starve
5	LLQ(rate limited, WFQ, WFQ)	20%	20%	60%	Queue 1 (LLQ) is rate limited, Queues 2 and

					3 (WFQ) will not starve
6	WFQ, WFQ, WFQ	25%	25%	50%	Queues 1, 2 and 3 allocated minimum bandwidth per template, but can burst up to port speed.
7	WFQ, WFQ, WFQ	60%	10%	30%	Queues 1, 2 and 3 allocated minimum bandwidth per template, but can burst up to port speed.
8	WFQ, WFQ, WFQ	40%	20%	40%	Queues 1, 2 and 3 allocated minimum bandwidth per template, but can burst up to port speed.

Due to the nature of LLQ, it is possible for traffic that is classified into the LLQ to basically starve out the other queues, since the scheduler may be pre-empted to service LLQ traffic only. Template option 1 above does not place restrictions on the Priority 1 queue to burst up to port speed, and this is available for those customers who feel comfortable with their own ability to classify their applications into Priority queue 1, given the understanding that doing so may starve out queues 2 and 3. Typically, customers that do not rate limit LLQ traffic in Queue 1 are those customers who care most about serving Queue 1 traffic, at the expense of the other queues (e.g. a customer using their VPN service exclusively for VoIP traffic, with a small demand for non-VoIP application traffic).

In order to give customers a “safety net” such that Priority 1 Queue does not starve out other queues, templates 2 thru 5 still offer LLQ for the Priority 1 queue, but in these templates, any traffic that exceeds the bandwidth allocation for Priority 1 queue is discarded (unlike Template 1). Priority queues 2 and 3 are serviced using a WFQ scheduling algorithm, and are guaranteed a CDR as per the respective template. Priority 2 and Priority 3 queues are allowed to burst up to port speed if capacity is available, however, Priority 1 queue is rate-limited to the bandwidth allocated to it in that given template.

Templates 6, 7, and 8 are based on using WFQ for all three Priority queues, such that each of these queues is guaranteed their respective bandwidth allocation per the template if there is 100% utilization, but each queue is allowed to burst up to port speed in capacity is available.

Given TacDoh’s traffic requirements, Qwest recommends the use of Template 4, with the following mapping of applications to Queues –

- VoIP to Priority Queue 1 (LLQ, rate limited to 30% of port capacity)
- Video and SAP to Priority Queue 2 (WFQ, can burst up to port speed; guaranteed a minimum of 20% of port capacity)

- Email and other data applications to Priority Queue 3 (WFQ, can burst up to port speed; guaranteed a minimum of 50% of port capacity)

The QoS capabilities that Qwest offers make it possible for TacDoh to evaluate this template and if necessary, make changes to the traffic allocation/queuing method by selecting a different template through the customer self-management portal, Q.Control (see service description at the bottom of this question's response.)

- *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.

The following goals are for Domestic services only.

Class of Service offerings	Delay	Packet Loss	Jitter (or other quality indicators)
Class 1	25mls	.5%	2mls
Class 2	25mls	.5%	2mls
Class 3	25mls	.5%	2mls
Class 4			
Class 5 (if any)			

Qwest SLA goals apply equally to all traffic classes. Qwest currently does not offer a SLA for CE to CE latency. The SLA parameters mentioned above are from PE to PE.

Qwest does offer customers an enhanced version of end to end performance reporting capability using Visual Networks probes that can be deployed at the Customer premises. This capability comes as part of Integrated Management (service description located under response of Questions #2), and complements standard reporting and self-management capabilities that are available with Q.Control (service description at the end of this question).

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

When the access method into a MPLS VPN port is via dedicated access, the CDR will typically match the access loop speed (e.g. customer orders a DS1 loop directly into a DS1 MPLS VPN port, the CDR for that circuit and port is 1.54Mbps).

The CDR "Committed Data Rate" for a Layer 2 access method such as ATM or Frame Relay is set to match the MPLS VPN port speed. For example, customer orders a DS1 MPLS VPN port with ATM/FR access over the Qwest ATM network, the CDR for that loop is set to match port speed, in this case 1.54Mbps.

CDR per class of service (IP QoS) is determined by which traffic allocation template the customer picks. For example, the customer selects a QoS template which allocates 30% of the port capacity to Priority Queue 1, 30% to Priority Queue 2 and 40% to Priority Queue 3. What this means is that each of these queues are guaranteed a CDR of 30%, 30% and 40% respectively even under congestion. However, each queue is allowed to exceed its CDR and "borrow" capacity from other queues if they are not fully utilized. The maximum/minimum CDR percentages per queue range from 10-80% for Priority Queue 1, 10-80% for Priority Queue 2 and 10-80% for Priority 3 queue. There is not a different cost associated with the CDRs per class.

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

As explained previously. This depends on QoS template chosen. In this context, bursting only means the ability of traffic to burst at Layer 3 (IP QoS), not Layer 2 bursting (only applicable with a Layer 2 access method, and tied to port speed).

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

Qwest Control is a self-service, time-saving web portal gives TacDoh online access to all of your Qwest services and Qwest Control is available at *no additional charge***.**
Full network management capabilities are available including:

- View bills,
- Enter and track trouble tickets,
- **View network statistics,**
- Access your network status,
- Link to support for your accounts (under Qwest contacts),
- **Request IP/QoS configuration directly through Qwest Control.**

For end-to-end performance monitoring and reporting capability on a per Class of Service basis, Qwest recommends the deployment of a probe-based reporting capability, using Visual Networks.

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.

Question 6: Traffic Classification

Please provide details of how traffic is categorized and provides preference to TACDOH different service types. 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.)*

Traffic Classification/marking techniques are only limited by the options that the CE router supports. The CE may choose any available classification/marking technique as per customer's discretion. Qwest honors Marking is via IP ToS IPP values.

- *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.*

It is the CE's responsibility to translate between internal CoS marking methods (whether 802.1p or something else) to IPP bits that Qwest uses for classification of traffic into appropriate queues as per the following table –

IPP traffic classification rules
IPP 4/5 = PRIORITY 1
IPP 2/3 = PRIORITY 2
IPP 0/1 = PRIORITY 3
Note: IPP=6/7 is reset to IPP=0

If customer chooses a Qwest managed solution, Qwest will configure the CE router to map between the customer's internal classification/marking scheme and the Qwest IPP classification scheme.

- *Traffic prioritization techniques for different traffic types. For example, real time, non-real time, etc.*

As previously explained.

- *Traffic congestion avoidance techniques for different protocol type (TCP, UDP, SNA, etc.)*

As explained previously, traffic congestion is not likely to occur in the Qwest backbone network, and as such there is no per-hop treatment of different classes of service in the Qwest core network. The CE-PE link is the only place where congestion is likely to occur, and this is where the Qwest QoS capability is most useful. On the upstream between the CE and Qwest PE, it is the CE's responsibility to prioritize, mark and queue traffic before placing it outbound to the Qwest PE. Based on the classification provided at ingress by the CE router, the Qwest PE prioritizes traffic outbound to the customer CE.

As such, we support any CE-based congestion avoidance schemes that are transparent to the carrier network.

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.

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;*
  Qwest offers full meshing through our MPLS solution. Communities of interest and security are maintained through defining closed user groups upon each interface.

- *Technical limitation to create partial clouds (if required) to accommodate TACDOH current and future community of interest;*
  By default any site with connectivity into the solution will have full access to every other site (full mesh). Partial mesh solutions where locations are limited to who they communicate with can be implemented one of two ways. Depending on the security controls in place, the Customer Premise Equipment (CPE) of the restricted site can have either a limited set of static routes entered (to limit reachability) or have ACLs placed on the device itself limiting this access (then keeping a simple default route pointing into the cloud). It is also possible, though not as scalable, to place ACLs on all of the remote sites to prevent access from restricted site. Another option is to use traditional layer-2 PVCs to those sites needing access limited access. There is no additional cost to mix the traditional Layer 2 PVC for this implementation, as long as the Frame or ATM transport for the "restricted site" is purchased from Qwest.

  RFC2547bis BGP/MPLS VPN topologies are configured and enforced in the service provider cloud, specifically by the Provider Edge routers. BGP uses an extended-community attribute, *route-target*, to filter appropriate VPN routes into the correct Virtual Route & Forwarding tables (VRF). The service provider can define the route-target import list and the route-target export list to include only the route-target extended-community values for the VPN(s) that the VRF belongs. To schedule a change, a request is submitted by opening a ticket using the Qwest Web portal service called Q.Control.

- *Intra-connectivity between partial clouds for same provider*
  Each cloud is unique and isolated from others. If a customer wishes to join networks together this would be accomplished using Customer Premises Equipment (CPE) to route between the two connections. The customer would then need to handle routing and IP address overlap issues at the CPE. If a customer has a need for multiple clouds it may be possible to build a single cloud and perform the partial mesh described in the above bullet, this would be the preferred solution.

- *Inter-connectivity between partial clouds between different providers.*
  If another provider has an MPLS cloud, interconnecting it with the Qwest cloud would be done the same way as between two clouds for the same provider (above). Qwest is working on inter-AS MPLS solutions such that a customer could directly their secondary carrier MPLS solution to their Qwest solution, or extend the Qwest MPLS solution elsewhere using a secondary MPLS network.

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.

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

All non-IP protocols must be encapsulated inside IP packets by the CE systems. Qwest can transport any IP-based encapsulation method used in a CE router, including GRE, IPsec and others. Qwest also recommends raising the access line maximum transmission unit (MTU) size above the 1500 byte default when encapsulation protocols are used. The Qwest MPLS VPN network will support larger MTU sizes such that any IP protocol encapsulation scheme can be transported across our network without IP packet fragmentation.

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.)*

Qwest supports IP Multicast through GRE tunnels.

- *IP Voice call processing functionality (Voice over IP Gateway, IP Telephony call processing, on-net and off-net);*

Voice-over-IP

Qwest is uniquely positioned to offer converged data & voice services due to our IP network, long-distance network, and local telephony presence.
Voice-over-IP (VoIP) technology is about much more than converged data and voice transport. Qwest believes the future of VoIP is about providing intelligent services across multiple modes of communications that enable companies to conduct business more effectively.

Voice communication is only one of many communication channels in the enterprise today. Email, voice conferencing and instant messaging are already ubiquitous while new voice applications like push-to-talk are becoming common. Qwest believes that integration of these different channels is an essential feature of tomorrow's communication services.

Qwest now offers **OneFlex Hosted VoIP** a fully hosted solution that does not require an IP PBX on premise, delivering features from the network and supporting multiple IP endpoints and analog phones (with an IAD (Internet Access Device))

- *IP Video bridging functionality (point-to-point and point-to-multi-point);*

Not offered by Qwest at this time.

- *Internet Access Service;*

Internet Port
Qwest's Internet Port, a member of the iQ suite of ports, offers TacDoh a crucial element in creating your virtual enterprise by delivering customized high-speed, reliable, scalable Internet access service.

The service is provided via a Qwest owned and operated, world class networking platform. Qwest network operations centers (NOCs) have full visibility and control of the platform with 24-hour, 7-day per week management. To facilitate access into your network, TacDoh can choose from a variety of port speeds, ranging from 56 Kbps to 2.4 Gbps. The following port types are available in fractional or full speeds:

- DS-1 (1.544 Kbps)
- DS-3 (45 Mbps)
- NxDS-1 (3-12Mbps)
- OC-N (155 Mbps and up)
- Ethernet (10 Mbps)
- Fast Ethernet (100 Mbps)
- Gigabit Ethernet (1,000 Mbps)

Qwest offers TacDoh Internet Access through our global IP network for your locations around the world. TacDoh may obtain IP connectivity from Qwest globally via strategic relationships with network partners like British Telecom and Infonet. Customers may obtain IP connectivity through Qwest points of presence (POPs) in Hong Kong, Tokyo, Singapore and Sydney.

Network technology
Qwest Internet Port provides a complete range of services for various enterprise networking requirements. The Qwest OC-192 Internet protocol (IP) network backbone is engineered for minimal packet loss and network congestion. Multi-protocol label switching (MPLS) fast re-route is used between every core router in the Qwest network ensuring a quicker recovery time over synchronous optical network (SONET). Ports are available from 56 Kbps to 2.4 Gbps.

While the Qwest public and private peering arrangements are extensive (111 Gbps utilizing 99 percent private connections), “cold potato” routing (Qwest transmits customer traffic on the Qwest network for as long as possible) virtually eliminates most of the latency issues faced by other service providers. The Qwest OC-192 IP network, one of the most advanced networks available, offers exceptional service level agreements (SLAs) and some of the highest customer access speeds in the industry today. Qwest is one of the first network service providers (NSP) to offer an off-net latency SLA guaranteeing 95 Ms among the top five networks.

Port options
Security
Protecting your enterprise-wide communications has never been more important. How do you know whether your network is secure when you are unsure of all the ways it might be vulnerable? Qwest has the dedication and expertise to recognize and minimize threats to your security—from hackers attempting to disrupt applications to attacks designed to halt your entire network. Qwest offers a broad array of managed security services, including Managed Firewall Service, which provides a valuable premises-based security measure for your network, particularly when integrated with Internet Port connectivity or dedicated hosting services.

Diversity
Qwest recognizes your need for 100 percent availability of your network to support your mission-critical applications. Qwest Internet Port offers Diversity configurations as an optional service enhancement. At customer's request and where available, Qwest provides secondary network connectivity provisioned and maintained separately from the customer’s primary Qwest Internet Port connection.
The Qwest Internet Port Diversity option provides customers the ability to fortify their disaster recovery and resiliency strategy. Qwest Internet Port Diversity options include local loop diversity, card diversity, router diversity and TeraPOP diversity.

Allowable Protocols

- All IP publicly routable protocols
- Quest Routing Protocols
    - Static (RIP)
    - BGP4

Network Management Services
Qwest Internet Port can be packaged with Qwest Network Management Services (NMS). This provides your organization with a comprehensive service, including an integrated ordering process, invoice and customer care/NOC support. This managed service is just one more way Qwest brings you value. An attractive part of the offer is that the service uses in-band monitoring/management tools that eliminate the need for a separate dedicated circuit.

As most Qwest Internet Port customers will require routers for their external network connection, a robust portfolio of customer premises equipment (CPE) options is also available through Qwest.

NMS is a fully integrated package of products and services that offers comprehensive solutions for managing voice, data and video networks. NMS is backed by a highly trained team of Qwest technicians and experts with proven expertise and experience in network management and maintenance, as well as by a strong group of allies. A Qwest solution eliminates the need to manage the many different pieces of the network puzzle.

Qwest's long track record in network design and integration provides the extensive experience and knowledge necessary to develop methods, procedures and tools to cohesively and comprehensively manage your data network.

- *Broadband Access Service (e.g., connectivity for TACDOH small locations and Corp. Remote Access Users) to customer Network-Based MPLS cloud*

For the purpose of this response Qwest is recommending TacDoh use our cost effective **Frame Partner Access** for the small locations like the Sales Offices. Frame Partner Access is a Local loop connection from the TacDoh sales office to LEC's Frame Relay POP that is interconnected to Qwest's Frame Relay network via a NNI. Once on the Qwest frame network the user can now access Qwest's IP private and or public MPLS based service. In addition to offering frame relay within our 14 state LEC territory, Qwest has established NNIs with Verizon, Bell South and SBC giving Qwest a highly dense nationwide frame relay footprint.

Migration of any offices that currently use Qwest's frame relay network is a simple matter of configuring the existing frame port to connect to Qwest's iQ Networking Private port. No new loop or CPE change is required. For offices with a frame relay provider other than Qwest, the existing CPE may continue to be utilized.

TacDoh will have the ability to order iQ Ports with DSL Access within six to eight months. DSL access will be provided by a 3rd party National Provider as well as Qwest's 14 state LEC DSL services. DSL access to iQ ports enables Qwest to offer TacDoh further cost effective access methods into our MPLS network. It is recommended that TacDoh consider DSL as a replacement in the Sales Offices for the dial backup proposed in this response.

- *Traffic encryption between all or selective TACDOH locations; please outline the technology used.*

Qwest is proposing our Private IP network as the solution for all TacDoh locations. This network is completely private from the routers to the core network. It does not use public access anywhere in the service. With that in mind if TacDoh requires further security through encryption of all data Qwest recommends the use of IPsec offered through our Integrated Management service. A service description is located under Question #2.

- *Provider's future plan to add additional class of service to the current service offering (if any).*

Qwest will be adding a fourth queue by the end of this year.

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.

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*

Qwest supports multicast applications through GRE tunneling. There is no additional charge associated with GRE tunneling.

- *IP Voice routing/processing functionality*

There is no additional cost for an IP Voice application enabled on the to the proposed network. Should TacDoh wish to consider Qwest's OneFlex Hosted VoIP service, detailed information of the domestic locations considering VoIP will be required.

- *IP Video bridging functionality*

Qwest does not off a Video Bridging service at this time.

- *Internet access service*

Qwest is providing a DS3 of Internet access at the three Data Centers pricing is found in the Monthly Cost pages.

- *Broadband access service*

If by Broadband you mean DSL for the Sales Offices, Qwest will be offering DSL as an access type into the Qwest network in sxi to eight months. There will be an access charge associated with DSL as there is for dedicated, frame or ATM access, DSL is expected to be our lowest priced hardwired access type.

- *Adding a new class of service*

No change for changing or adding class of service.

- *Traffic Encryption*

IPSEC is available through Integrated Management. The service description is found in the response to Question #2.
Pricing for Integrated Management is $50/location/month

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

Nothing is being customized for this response. All pricing is within Qwest's standard pricing models.

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).

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:

Qwest recommends that TacDoh use the following steps to coordinate your migration from frame relay to MPLS:

Step 1 Start in the US with the Regional Headquarters that do not have any international locations, i.e. Plano, TX

Step 2 Migrate the sales offices first followed the District Hub, then move to the next hub and sales offices.

Step 3 Once the migration of all District Hubs and associated sales offices is complete, migrate the Regional Headquarters.

Step 4 With the exception of the White Plains Data Center, complete the migration of the North American Regional Headquarters by bringing up all domestic and Canadian locations on the MPLS network.

Step 5 Begin Asia migration following the same pattern as above with the District Hubs migrating first followed by the Regional Headquarters.

Step 6 Once Asia is complete begin the European District Hubs and Regional Headquarters migration.

Step 7 Finally begin the migration of the Data Centers starting with White Plains followed by Bangalore then Sterling.

It is expected this process will take several months to complete, during that time overlap of existing frame network and new MPLS network should be expected.

In all locations equipment in place will be considered for use prior to considering new equipment. If new equipment is required and that equipment is purchased from Qwest, for the domestic locations, Qwest will configure and stage equipment prior to shipment.

- *Change Bandwidth (CDR) associated for specific Class of Service*

Included with Integrated Management

- *Change the status of classes of services (e.g., upgrade from one class to three classes)*

Included with Integrated Management

- *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)*

Included with Integrated Management

- *Change the current status of CE from partial cloud to Any-to-Any connectivity or visa-versa*

RFC2547bis BGP/MPLS VPN topologies are configured and enforced in the service provider cloud, specifically by the Provider Edge routers. BGP uses an extended-community attribute, *route-target*, to filter appropriate VPN routes into the correct Virtual Route & Forwarding tables (VRF). The service provider can define the route-target import list and the

route-target export list to include only the route-target extended-community values for the VPN(s) that the VRF belongs. To schedule a change, a request is submitted by opening a ticket using the Qwest Web portal service called Q.Control.

In the event that the customer prefers to create a VPN topology from the CE, then one would open a change request ticket with the Integrated Management Service (service description in Question #2). Referencing the "Move-Add-Change" list of activities, TacDoh could have Integrated Management engineers configure access control lists and/or modify routing lists on the CE. This service is included with Integrated Management and no down time would occur unless the router were to be recycled.

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.

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.*

In addition to the 11 TeraPOPs deployed with Private Edge MPLS router (PEs) Qwest has PEs deployed in Singapore, Hong Kong and Tokyo. Qwest will be utilizing this deployment as a solution for TacDoh's regional Asian network. Thus TacDoh will be riding the Qwest MPLS network for all North American and Asian locations.

For the European locations Qwest has chosen Infonet as our initial off-net MPLS partner. In order to implement off-net MPLS services, we have developed an "Inter-AS" MPLS gateway between Qwest and Infonet. Basically this involves dedicated Cisco GSR routers on Qwest network, one for Pacific Rim the other for Europe/Middle East and Africa that will act as a private edge routers. Dedicated Cisco devices on the Infonet network will also act as private border routers. This router combination will have an MP-BGP session that will pass all MPLS traffic and routing information between the partner networks.

InfoNet offers MPLS with QoS templates in 23 countries including those immediately required by TacDoh in England, in a manner consistent with Qwest's QoS policy.

With BT's acquisition of InfoNet the natural next step is to develop an MPLS gateway between Qwest and BT.

- *Inter-providers connectivity (e.g., DiffServ Gateway); partial cloud connectivity with class of service mapping.*

The Inter-AS MPLS architecture that Qwest offers through its International partners is fully compatible with the Qwest Class of Service definition. That is, customers will have a consistent QoS policy that is fully aligned with the QoS description already provided in this document. The CE will not be required to have any special configuration whether it connects directly to the Qwest MPLS cloud or the partner's MPLS cloud.

The MPLS PE router on the partner network will be responsible for making the necessary translation between the Qwest QoS policy and that providers QoS policy. The MPLS Gateway routers will also be configured to map between QoS policies that are local to each MPLS network so as to keep such differences transparent to the customer.

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.