

4.2.12 Layer 2 Virtual Private Network Services (L2VPNS) (L.34.1.4.6, M.6, C.2.7.12)

Qwest has a long history of delivering Layer 2 Virtual Private Network services. Our Networkx L2VPNS applies this experience with our converged infrastructure to deliver flexible, high-quality services.

The Qwest Layer 2 Virtual Private Network Service (L2VPNS) provides Virtual Private Local area network Service (VPLS) functionality that allows Government Agencies to connect multiple sites in a single, bridged domain over the Qwest network. We do not intend to offer the optional Virtual Private Wire Services at this time.

Qwest delivers L2VPN VPLS through the Qwest Multi-Protocol Label Switching (MPLS) core network. The Qwest L2VPN Service delivery approach combines diverse user-to-network interfaces, multiple access types, private supplier arrangements, and MPLS-enabled transport services to deliver a flexible and fully functional L2VPN solution to Agencies. Qwest's L2VPN provides four Quality of Service (QoS) categories, based on service priority (e.g., network-critical, time-critical, business-critical, and standard application). [REDACTED]

Qwest L2VPN services, as it relates to the VPLS standard and MPLS, is a recent offering in the telecommunications industry that builds upon the breadth of Qwest experience in legacy L2 services (Asynchronous Transfer Mode (ATM) and Frame Relay (FR)) and our knowledge of L3VPN services (RFC 4364 standard). In developing our L2VPN service offering, we apply [REDACTED] of engineering, management, and operational expertise. Qwest already provides ATM, FR and L3VPN for many Government Agencies, [REDACTED]

[REDACTED]

[REDACTED] Qwest is a leader in delivery of L3VPN services and will continue to deliver comprehensive and flexible solutions to Agencies through L2VPNS.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Figure 4.2.12-1 provides an easy reference to correlate narrative requirements to our proposal response.

Figure 4.2.12-1. Table of L2VPNS Narrative Requirements

Req_ ID	RFP Section	Proposal Response
32457	C.2.7.12.1.4 (8)	4.2.12.3.1

4.2.12.1 Reserved (L34.1.4.6 (a))

4.2.12.2 Reserved (L.34.1.4.6 (b))

4.2.12.3 Satisfaction of L2VPNS Requirements (L.34.1.4.6 (c), C.2.7.12.1-C.2.7.12-3)

This section addresses how Qwest will meet the RFP's L2VPNS features, capabilities, and interface requirements.

Qwest owns and operates a nationwide Layer 2 and 3 MPLS core service infrastructure that satisfies all the mandatory standards, connectivity, capabilities, features, and interfaces required for Networx L2VPNS VPLS. Qwest uses MPLS technology to provide multi-faceted services built on a unified services architecture. We have employed MPLS for many years and

have extensive experience in all aspects of network design, operational support, and service delivery.

Qwest will provide the L2VPNs using vendor implementations that comply with all necessary Internet Engineering Task Force (IETF) and Institute of Electrical and Electronic Engineers (IEEE) standards or draft standards. [REDACTED]

Qwest's ongoing participation in many standards and technology forums, such as the IETF, IEEE Standards Committees and Working Groups, and the Metro Ethernet Forum, ensures our awareness and compliance with evolving industry standards.

The two major encapsulation options used for building VPLS instances are still in draft state in the IETF. The first draft is draft-ietf-ppvnp-vpls-ldp, sometimes referred to as the Lasserre draft. The second draft is draft-ietf-l2vpn-vpls-bgp, also known as the Kompella draft. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] Qwest's ongoing participation in many standards and technology forums, such as the IETF and IEEE standards committees and working groups and the Metro Ethernet Forum, ensures our awareness and compliance with evolving industry standards.

The following three sections describe how Qwest will satisfy the capability, feature, and interface requirements of the RFP.

ID #	Capability	
2	VPWS [Optiona]	
3	Service Interworking	
4	Network Interworking	
5	Routing Control	
6	Scalability	
7	UNIs	

ID #	Capability	
8	Encapsulation Methods	[REDACTED]
9	Traffic Types	[REDACTED]
10	Supported Topologies	[REDACTED]
11	Configuration Not Broadcast or Visible	[REDACTED]
12	Traffic Separation	[REDACTED]
13	QoS	[REDACTED]
14	Management	[REDACTED]

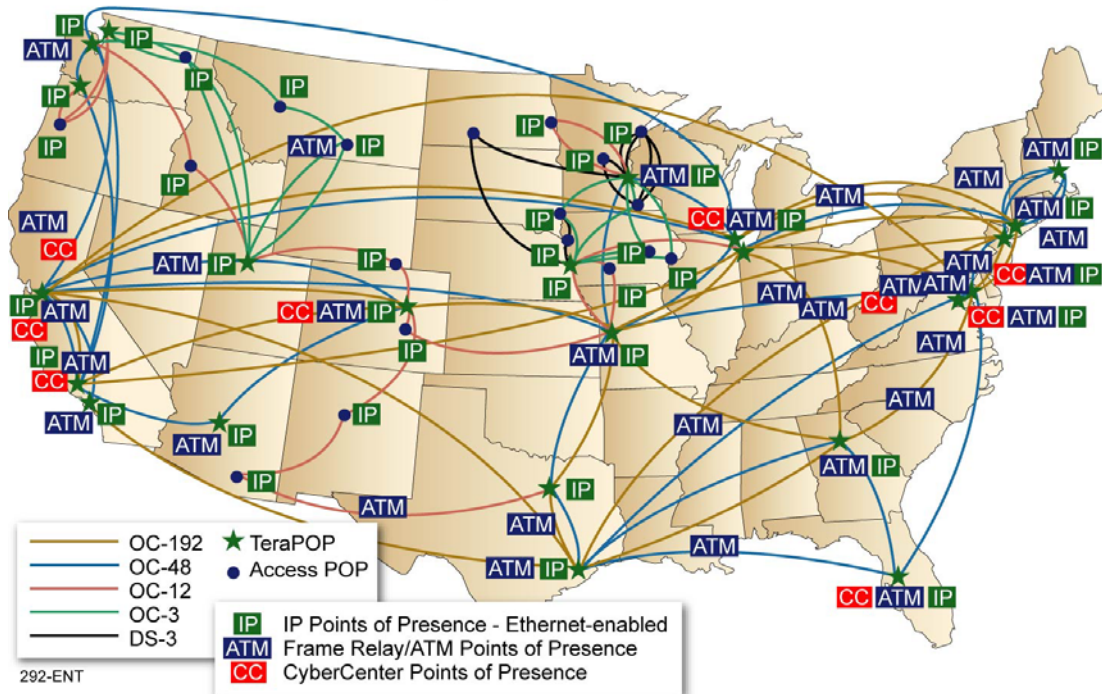
ID #	Capability	
15	Interoperability	
16	Multiple Contractor Networks [Optional]	

The following paragraphs describe the various components of L2VPN service delivery and explain the benefits [REDACTED] with Qwest's approach. The Qwest approach to delivery of L2VPNS builds on Qwest's proven processes and resources—comparable across a range of Qwest service offerings—that work together to provide a robust solution for Agencies. Qwest has the business service expertise, Network Elements (NEs), operational groups, access methods, and supplier arrangements to deliver L2VPNS as specified within the Networx RFP.

Qwest provides L2VPNS VPLS through our high-capacity MPLS core network backbone, shown in **Figure [REDACTED]** L2VPNS combines Ethernet, ATM, FR, and other protocols on a solution platform that can be customized to meet many different customer requirements. As noted above, the Qwest L2VPNS provides VPLS functionality that allows Agencies to connect multiple sites in a single, bridged domain over the Qwest network. VPLS provides Ethernet ports that are set up as part of the same LAN across the WAN.

Figure 4.2.12-3. The Qwest Core MPLS Backbone – Qwest L2VPN.

Qwest L2VPN is available in major cities throughout the country. Qwest L2VPN is built upon high speed OC 192 MPLS core technologies, enabling a robust and scalable networking environment.



Traditionally, LANs are restricted to an office floor or building. However, with VPLS, the LAN is configured across and between buildings, states, and countries. Traditional Ethernet networks connect sites in a single local area. VPLS is an Ethernet bridged/switched network with locations geographically dispersed. Qwest L2VPNS provides connections between Agencies' LANs, providing SDP-to-SDP connectivity across both Metro Area Networks and the WANs.

In VPLS, the attachment circuits usually are exclusively Ethernet.



[REDACTED]

No explicit customer configuration is required to add new locations into the VPLS service. Signaling protocols such as BGP auto-discover new locations based on implicit information that identifies a particular location as belonging to a particular VPLS instance. Since VPLS is a Layer 2 service, it runs completely transparently to the higher-layer protocols. As a result, the customer can carry any protocol over VPLS that standard Ethernet supports.

Qwest's L2VPNS customers benefit from end-to-end support provided by Qwest's engineering, operation, and business groups. Qwest's Government sales and pre-sales engineering groups work directly with Agencies to understand their requirements and provide matching service solutions. [REDACTED]

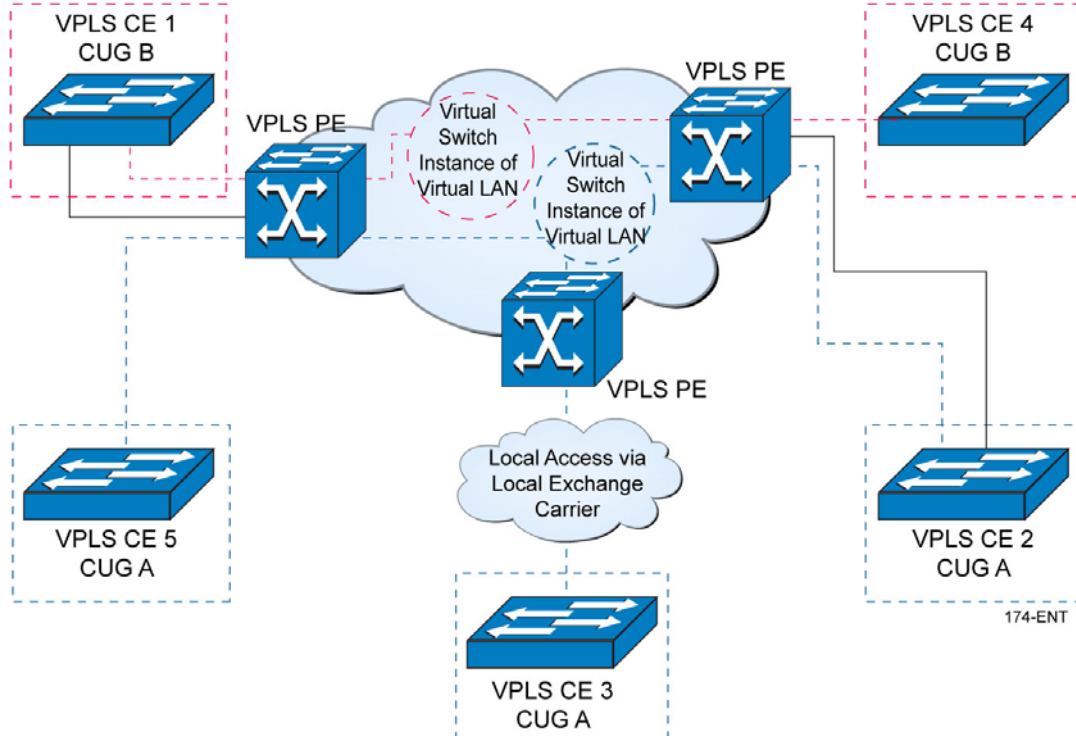
[REDACTED]

[REDACTED] The NOCs maintain and monitor all NEs on the Qwest data networks, including customer access and network backbone circuits. They provide 24x7x365 service and proactively identify, isolate, and resolve network issues and fault conditions. To provide

emergency continuity of operations, the NOCs are redundant and staffed with cross-functional technical resources.

[REDACTED]

Figure 4.2.12-4. Qwest L2VPN SDP to Qwest Edge Connectivity. Qwest L2 VPLS provides emulated VLAN environments for multiple communities.



[Redacted content]

[REDACTED]

Supported Encapsulation Schemes [Req_ID 32457; C.2.7.12.1.4 (8)]

The two major encapsulation options used for building VPLS instances are still in draft state in the IETF. The first draft is draft-ietf-ppvnp-vpls-ldp, sometimes referred to as the Lasserre draft. The second draft is draft-ietf-l2vpn-vpls-bgp, also known as the Kompella draft. [REDACTED]

[REDACTED]

4.2.12.3.2 Satisfaction of L2VPNS Feature Requirements (L.34.1.4.6(c), C.2.7.12.2)

Qwest L2VPNS satisfies all the mandatory feature requirements as listed in the Networx RFP. Through the flexibility of our core MPLS backbone, combined with the experience and knowledge of the Qwest Program Management and Operation support teams, Qwest is able to offer a wide array of L2VPN service features. Our MPLS backbone network enables the support of Class of Service (CoS) through the implementation of separate traffic classes. The MPLS backbone also provides a high degree of service availability and the inherent security associated with a non-peered private network.

Figure 4.2.12-5 summarizes Qwest's technical approach to satisfying the feature requirements of L2VPNS. Qwest fully complies with all mandatory

stipulated and narrative feature requirements for L2VPNS. The text in Figure 4.2.12-5 provides the technical description required per L.34.1.4.6(c) and does not limit or caveat Qwest's compliance in any way.

Figure 4.2.12-5. Qwest's Technical Approach to L2VPNS Features

ID #	Feature	
1	Class of Service	<div>[REDACTED]</div>

ID #	Feature	
2 [Optional]	Non Peered Private IP Network [Optional]	
3	High Availability Options	

4.2.12.3.3 Satisfaction of L2VPNS Interface Requirements (L.34.1.4.6 (c), C.2.7.12.3, C.2.7.12.3.1)

Qwest L2VPNS satisfies all mandatory and several optional interface requirements as defined in the Networkx RFP. Using the native capabilities on the Qwest local broadband infrastructure, combined with ILEC and CLEC carrier relationships, Qwest is able to offer a variety of Ethernet access options for L2VPN VPLS, [REDACTED] Qwest L2VPN VPLS UNIs and SEDs are provided, as specified in the Networkx RFP, at speeds ranging from 10Mbps up to 10Gbps in both copper and fiber media types. L2VPN service SEDs are customized depending on access method or selected feature (for example, the L2VPN high-availability feature). Qwest may substitute other SEDs of equivalent functionality and performance over the course of the Networkx program. Qwest fully complies with all mandatory stipulated and narrative interfaces requirements for L2VPNS. The text in

Figure 4.2.12-6 provides the technical description required per L.34.1.4.6(c) and does not limit or caveat Qwest's compliance in any way.

Figure 4.2.12-6. Qwest-provided L2VPNS Interfaces at the SDP

UNI Type	Media Type	IEEE Standard	Max Speed Supported	Bandwidth Profiles Supported	
1 [Optiona]	Optical (same as 14)	802.3z	1000Mbps	100Mbps to 1000Mbps	
2 [Optiona]	Optical (same as 15)	802.3z	1000Mbps	100Mbps to 1000Mbps	
3	Optical (Single Mode)	802.3u	100Mbps	10Mbps to 100Mbps	
4 [Optiona]	Optical	IEEE 802.3ae	1310 nm	10Gbps	
5 [Optiona]	Optical	IEEE 802.3ae	850 nm	10Gbps	
6 [Optiona]	Optical	IEEE 802.3ae	1550 nm	10Gbps	
7 [Optiona]	Optical	IEEE 802.3ae	1310 nm	10Gbps	
8 [Optiona]	Optical	IEEE 802.3ae	1550 nm	10Gbps	
9 [Optional]	Optical	IEEE 802.3ae	1310 nm single mode	10Gbps	
10 [Optiona]	Optical	IEEE 802.3ae	1550 nm single mode	10Gbps	
11	Electrical	802.3	10Mbps	10Mbps	
12	Electrical	802.3u	100Mbps	10Mbps to 100Mbps	
13	Optical	802.3z	1000Mbps	100Mbps to 1000Mbps	
14	Optical (Multi-mode)	802.3z	1000Mbps	100Mbps to 1000Mbps	
15	Optical (Single Mode)	802.3z	1000Mbps	100Mbps to 1000Mbps	
16 [Optiona]	Electrical 1000BASE-CX (Copper)	802.3z	1000Mbps	100Mbps to 1000Mbps	
17 [Optiona]	Electrical 1000BASE-T (Twisted Pair)	802.3ab	1000Mbps	100Mbps to 1000Mbps	
18 [Optiona]	Optical	GR-253, ITU-T G.707	1310 NM	10Gbps	

Information about the access arrangements available between these SEDs and L2VPNS is included below in Section 4.2.12.7, *Characteristics and Performance of Access Arrangements*.

4.2.12.4 L2VPNS Quality of Service (L.34.1.4.6 (d), C.2.7.12.4, C.2.7.12.4.1)

Qwest understands and fully complies with Networkx L2VPNS performance requirements. **Figure 4.2.12-7** compares the Networkx L2VPNS performance standards to the Qwest-proposed L2VPN QoS for Networkx.

Figure 4.2.12-7. Qwest Compliance with Government L2VPNS Performance Metrics

Key Performance Indicator	Service Level	Performance Standard Level	Acceptable Quality Level	
Availability	Routine	99.8%	> 99.8%	
	Critical [Optiona]	99.999%	> 99.999%	
Latency (CONUS)	Routine	100ms	< 100ms	
Latency (OCONUS)	Routine	400ms	< 400ms	
Time to Restore	Without Dispatch	4 hours	< 4 hours	
	With Dispatch	8 hours	< 8 hours	
Jitter (Packet)	Routine	10ms	< 10ms	
Grade of Service (Data Delivery)	Routine	99.9%	> 99.9%	
	Critical [Optiona]	99.95%	> 99.95%	

The Qwest L2VPN network is designed as part of a geographically distributed and redundant topology. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

4.2.12.5 Qwest's L2VPNS Exceeds Service Requirements (L.34.1.4.6 (e))

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

4.2.12.6 Experience with L2VPNS Delivery (L.34.1.4.6 (f))

Qwest has several years of experience delivering similar services, (e.g., network-based IP VPN via MPLS RFC 4364 standard, and legacy L2VPN services (ATM and FR)). L2VPNS employs relatively new technology and standards, with approximately two years of general commercial and Government use.

Qwest has successfully offered ATM service nationwide since [REDACTED]. Qwest was an early adopter of MPLS technology to provide high-quality L3VPNs with the same security profile as traditional Layer 2 methods such as ATM and FR. [REDACTED]

[REDACTED]

4.2.12.7 Characteristics and Performance of Access Arrangements (L.34.1.4.6 (g))

Qwest provides the access arrangements for L2VPNS needed to satisfy the diverse requirements of Agencies. SEDs connect to several types

[illegible]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

4.2.12.8 Approach for Monitoring and Measuring L2VPNS KPIs and AQLs (L.34.1.4.6 (h))

Qwest monitors and measures the Key Performance Indicators (KPIs) and Acceptable Quality Levels AQLs using automated processes that pull data from the network elements, summarize it, and create a Web-based display of the information. This display presents actual results, and provides a color-coded visual indicating whether performance goals have been achieved. Our approach is to completely automate the Web display of results from data collection. This ensures that the focus is on responding to performance issues, rather than on performance report generation. The automated reporting process eliminates any question of manipulating the performance data.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[illegible][illegible][illegible]

[illegible]

[illegible]

[illegible]

4.2.12.9 L2VPNS Support of Time-Sensitive Traffic (L.34.1.4.6 (i))

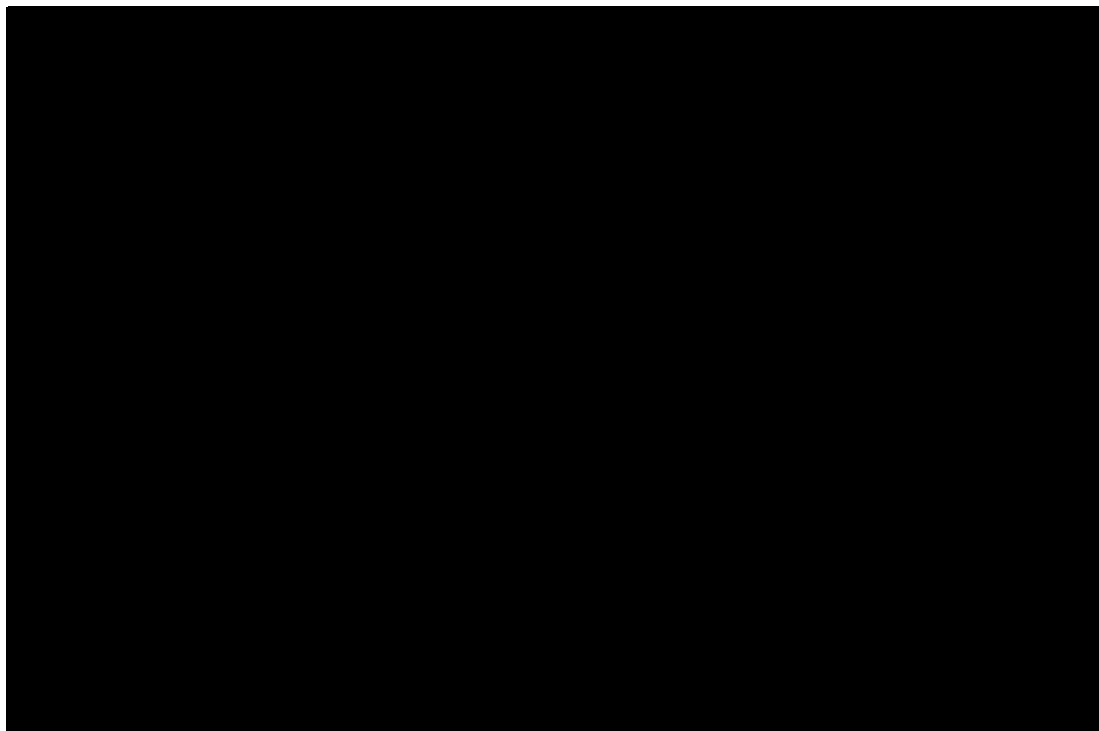
All of Qwest's data networking solutions provide proven, industry-standard methods to ensure the quality of time-sensitive traffic. Qwest has best-in-class technical solutions and implementations of QoS mechanisms for our MPLS network, which supports our L2VPNS offering. Our network engineering and capacity planning ensure our ability to meet the challenge of transporting time-sensitive traffic. [REDACTED]

[REDACTED]

Traditional IP networks have evolved around "best effort" service and typically have not provided guarantees for key performance criteria. The need to support real-time services on IP networks has driven the development of IP prioritization and queuing mechanisms as well as MPLS technology. The Qwest network is engineered to enable QoS to prioritize certain types of traffic over other types of traffic if there is congestion in the network.

Qwest's MPLS network supports the ability to prioritize LSPs. This means that the IP network supporting our VoIP network has a higher priority than our VPN network and that the IP network supporting our VoIP network has a higher priority than the network that provides Internet services. Because of our ability to manage and prioritize traffic, impacts from different traffic loads can be handled immediately to ensure no impact to the bandwidth required to support all of our customer's VPN and VoIP traffic requirements. [REDACTED]

[REDACTED]



Qwest's MPLS network employs standards-based MPLS and QoS mechanisms to enable high quality voice, video, and data transmission. The process of applying QoS in a network consists of multiple actions, defined as follows:

- **Classification:** Classifies applications based on their relative network performance needs. For example, is the point-of-service application more or less sensitive to latency, jitter, and loss than the VoIP application?
- **Marking:** Marks and classifies packets belonging to the applications so they may be recognized. For example, setting the IP precedence or DiffServ Code Point (DSCP) bits.
- **Policing:** Packets determined to be out of profile (that is, not conforming to the QoS policy) are either dropped or re-marked into lower priority packets (for example, rate-limiting).

- **Shaping:** Out-of-profile packets may also be buffered and shaped to conform to the configured QoS policy.
- **Queuing:** Scheduler resources are allocated to different classes (or queues) so traffic may be serviced (for example, last-in, first-out; first-in, first-out; weighted fair queuing; and low latency queuing).

[REDACTED]

[illegible]

[REDACTED]

These QoS actions ensure that low-latency, real-time applications such as Voice and video can share network resources with non-real-time data applications. Our convergence approach means that Qwest data services will migrate to a common MPLS network, so we can easily plan and identify any quality of service issues. Qwest's network planning methodology ensures that there is sufficient bandwidth to meet our customer's full port-limited capability, even in the event of core router failure or an access router or backbone trunk failure.

4.2.12.10 L2VPNS Support for Integrated Access (L.34.1.4.6 (j))

Qwest's network architecture and data services approach directly enables a complete menu of Integrated Access options to virtually all of Qwest's services. Section 3.3.1 provides additional information regarding our integrated access approach. As depicted [REDACTED], Qwest's network architecture and services already integrate several access methods, including:

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

**4.2.12.11 Infrastructure Enhancements and Emerging Services
(L.34.1.4.6 (k))**

Qwest has mature processes that enable us to envision, research, evaluate, engineer, deploy, and operate new or emerging services. Driven initially by the Chief Technology Office, Qwest evaluates new products and technologies for incorporation into the Qwest network, in partnership with Qwest Product Management.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

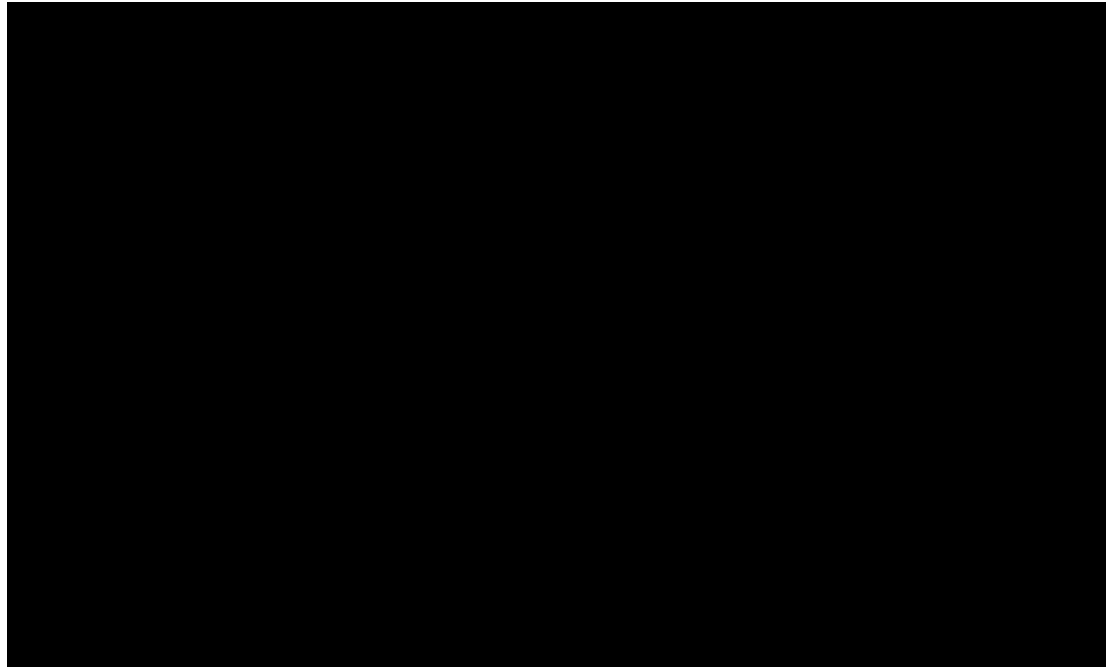
[REDACTED]

[illegible]

[REDACTED]

4.2.12.12 Approach for Network Convergence (L.34.1.4.6 (I))


As described in Section 3.3, Qwest already has a clear approach and has made significant progress in deploying a network that not only enables convergence from the customer's perspective, but is also a highly converged platform. Qwest is moving toward a packet-based architecture to enable network evolution and convergence. Using our private MPLS-based core, Qwest has already converged our IP-based services (private port MPLS VPNs, public port Internet services, and our VoIP transport for PSTN traffic) over this network. Qwest is committed to the elimination of stovepiped networks that create planning, operations, and interoperability issues for our customers. [REDACTED] shows Qwest's approach to support service quality by having a uniform view of network and support infrastructure.

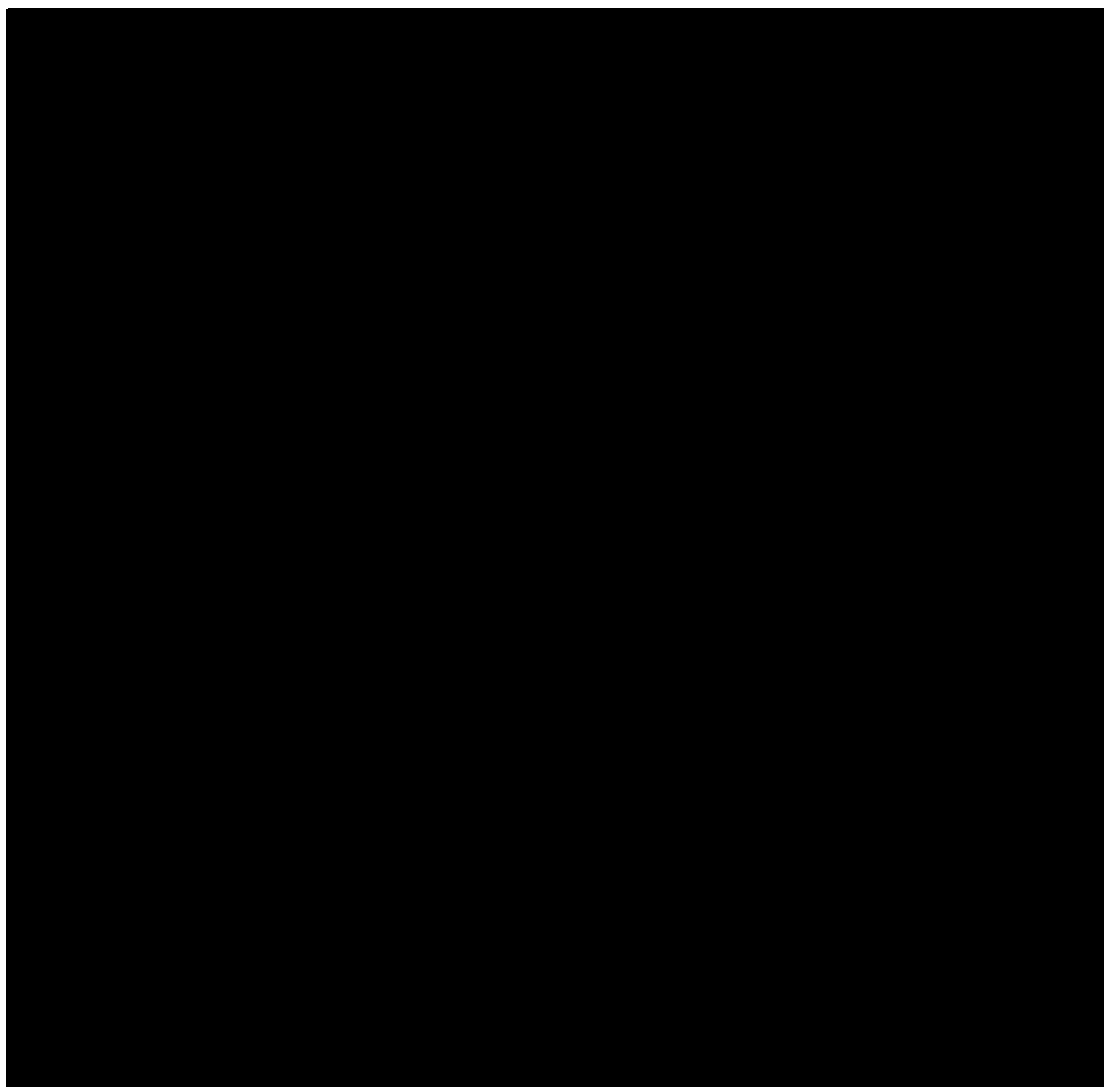


Multiple overlay networks are no longer established to deliver new services. Value is shifted to network-based services, where Qwest becomes a solutions provider. Applications-based services are delivered independent of the network infrastructure. Excellent service quality is maintained during network convergence through the following practices:

- Consistent and rigorous technology management methodology that includes evaluation, selection, and certification of NEs
- Accommodation of legacy services as the network evolves
- Network simplification through de-layering and introduction of multi-service access devices
- Coincident convergence of back-office systems, including introduction of a next-generation Network Management Layer (NML) packet Operational Support Systems (OSS).

Qwest Backbone Convergence:

As shown in , the use of a converged MPLS core significantly eases the problems normally associated with backbone traffic engineering. Without a converged backbone, each services network (for example, one for Internet, one for private IP services, and one for Voice) needs to be traffic engineered independently. The normal state of affairs is that one network has too much capacity and another has performance limitations that require a backbone or router upgrade. For example, the



[illegible][illegible]

[REDACTED]

[REDACTED]

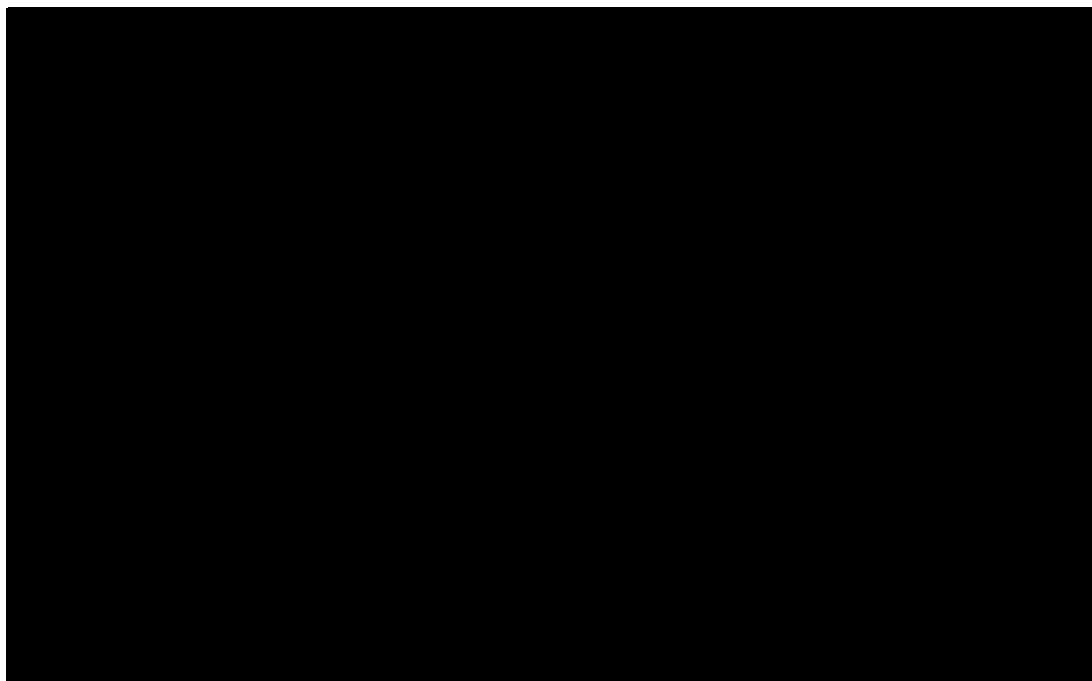
4.2.12.13 IP-PSTN Interoperability (L.34.1.4.6 (m))

The interoperability between our IP-based networks and the PSTN is addressed in Section 3.3.5, though not repeated here, as it does not apply to the L2VPNS requirements.

4.2.12.14 Approach for IPv4 to IPv6 Migration (L.34.1.4.6 (n))

[REDACTED]





4.2.12.15 Satisfaction of NS/EP Requirements (L.34.1.4.6 (o))

Qwest uses a structured multi-layered approach to support National Security and Emergency Preparedness (NS/EP) that is designed to address each required function. Qwest has organizationally and strategically integrated risk management and security to encompass information technology and physical security. Our priorities are to protect our customers from the physical layer up through the entire OSI stack, including all facets of cyber security.

Our approach ensures that Qwest complies with and provides priority for the Government's telecommunications requirements for NS/EP survivability, interoperability, and operational effectiveness during an emergency threat, whether caused by natural hazards, man-made disasters, infrastructure failures, or cyber events. Our approach consists of multiple levels of NS/EP support, including the assignment of a full-time dedicated

liaison, established Telecommunications Service Priority (TSP) policies and procedures, implementation of the 14 basic NS/EP telecommunications functional requirements, and our robust redundant network architecture in the National Capital Region (NCR).

Specifically, in accordance with RFP Section C.5.2.2.1, *NS/EP Basic Functional Requirements Matrix for Networx Services*, Qwest supports the following basic functional requirements for L2VPNS:

- **Enhanced Priority Treatment** (C.5.2.1 (1)) – L2VPNS supporting NS/EP missions are provided preferential treatment over all other traffic.
- **Secure Networks** (C.5.2.1 (2)) – L2VPNS supporting NS/EP missions have protection against corruption of, or unauthorized access to, traffic and control, including expanded encryption techniques and user authentication, as appropriate.
- **Non-Traceability** (C.5.2.1 (3)) – L2VPNS users are able to use NS/EP services without risk of usage being traced (that is, without risk of user or location being identified).
- **Restorability** (C.5.2.1 (4)) – Should a service disruption occur, L2VPNS supporting NS/EP missions are capable of being re-provisioned, repaired, or restored to required service levels on a priority basis.
- **International Connectivity** (C.5.2.1(5)) – According to RFP section C.5.2.2.1, this requirement is not applicable to L2VPNS.
- **Interoperability** (C.5.2.1 (6)) – L2VPNS will interconnect and interoperate with other Government or private facilities, systems, and networks, which will be identified after contract award.
- **Mobility** (C.5.2.1 (7)) – The L2VPNS infrastructure supports transportable, re-deployable, or fully mobile Voice and data

communications (i.e., Personal Communications Service, cellular, satellite, high frequency radio.

- **Nationwide Coverage** (C.5.2.1 (8)) – L2VPNS is readily available to support the National Security leadership and inter- and intra-Agency emergency operations, wherever they are located.
- **Survivability/Endurability** (C.5.2.1 (9)) – L2VPNS is robust to support surviving users under a broad range of circumstances, from the widespread damage of a natural or man-made disaster up to and including nuclear war.
- **Voice Band Service** (C.5.2.1(10)) – According to RFP Section C.5.2.2.1, this requirement is not applicable to L2VPNS.
- **Broadband Service** (C.5.2.1 (11)) – L2VPNS will provide broadband service in support of NS/EP missions (e.g., video, imaging, Web access, multi-media).
- **Scaleable Bandwidth** (C.5.2.1 (12)) – NS/EP users will be able to manage the capacity of L2VPNS to support variable bandwidth requirements.
- **Affordability** (C.5.2.1 (13)) – L2VPNS leverages network capabilities to minimize cost (for example, use of existing infrastructure, commercial-off-the-shelf technologies, and services).
- **Reliability/Availability** (C.5.2.1 (14)) – L2VPN services perform consistently and precisely according to their design requirements and specifications and are usable with high confidence.

Details of how Qwest supports all 14 basic functional requirements listed in RFP Section C.5.2.2.1 are provided in Section 3.5.1, *Approach to Satisfy NS/EP Functional Requirements*, in this Technical Volume.

4.2.12.16 Support for Signaling and Command Links (L.34.1.4.6 (p))

Per Section C.2.16.2, SatAA is not a valid access arrangement for L2VPNS.

4.2.12.17 Service Assurance in the National Capital Region (L.34.1.4.6 (q))

As discussed in Section 3.2, *Approach to Ensure Service Quality and Reliability*, Qwest provides network services in the NCR with a robust network architecture designed and engineered to ensure service continuity in the event of significant facility failures or catastrophic impact. Qwest will continue to engineer critical services to meet each Agency's requirements to eliminate potential single points of failure or overload conditions that may impact their network service performance.

Qwest has an active, compliant NS/EP plan. Qwest has been providing Telecommunications Service Priority (TSP) services locally for decades and nationally for more than [REDACTED] years with an excellent track record of meeting critical emergency requirements. Qwest also provides functionality that enables Government Emergency Telecommunications Service priority calling mechanisms.

Qwest will provide full NS/EP Functional Requirements Implementation Plan (FRIP) documentation upon contract award when requested to proceed with plan delivery. Qwest will update plans, including Part B, addressing our strategy for supporting Agency NCR requirements in accordance with RFP Section C.7.16.

Qwest understands the Government's requirement to assure performance of network services in and around the NCR. [REDACTED]

[REDACTED]

Qwest has recently acquired OnFiber, a metro SONET and Ethernet provider with yet another diverse network in the NCR. This gives Qwest at least [REDACTED] fiber optic networks to use to ensure redundancy and survivability in the greater Washington D.C. area.

[REDACTED] shows the logical configuration of the major transport facilities as well as the services provided at each POP.

[REDACTED]

[REDACTED]

[REDACTED] This

configuration enables these [REDACTED] locations to participate in the routing of access and backbone traffic, providing significant load balancing and reconfiguration options in the event of a switch, router, or even a complete POP failure. In effect, this means that Qwest can completely avoid Washington, D.C. to continue to provide services in an emergency.

The route-diverse SONET backbone, access networks, redundant Ethernet, ATM, and FR switches enable the transport of services to any Qwest POP nationwide. [REDACTED]

[REDACTED]

[REDACTED]. As with Voice services, critical Qwest customers can be dual-homed to ensure extremely high availability of their data services—again protected from any single point of failure in the NCR.

[REDACTED]

Qwest will address the strategy, technical systems, and administration, management, and operation requirements for the NCR in part B of our NS/EP FRIP (a draft appears as Appendix 2 in the Technical Volume).

4.2.12.18 Approach to Satisfying Section 508 Requirements (L.34.1.4.6 (r))

According to RFP Section C.6.4, *Section 508 Provisions Applicable to Technical Requirements*, Section 508 provisions are not applicable to L2VPNS. Qwest has fully described our approach to satisfying Section 508 requirements for applicable, offered services in Section 3.5.4, *Approach for Meeting Section 508 Provisions*, of this Technical Volume.

4.2.12.19 L2VPNS Impact on Network Architecture (L.34.1.4.6 (s))

Qwest will make the following changes to already deployed equipment in our network to support VPLS capabilities for L2VPNs that use 10/100/1000Mbps Ethernet access:

- Software configuration changes to support L2VPNS capabilities on the PE routers. Note that MPLS and Layer 3 MPLS services have been deployed and operational in the Qwest network since 1999. Software and configuration changes to support L2VPNs will be incremental and minimal.
- Qwest already has operational systems and processes in place to support L3VPNs. These systems and processes will be modified incrementally to support L2VPNs.

The risk of carrying out the necessary software/configuration services to support L2VPNS is minimal due to the maturity of MPLS and Layer 3 MPLS VPNS in the Qwest network. Qwest follows a stringent process of

quality control with multiple iterations of laboratory testing of software features and configurations before deploying them in the network. This disciplined approach to network modification mitigates much of the associated risk. Prior to deployment of any new capabilities in the network, Qwest procedures always include a risk mitigation back-out plan for restoring the network to its prior stable state.

4.2.12.20 Optimizing the Engineering of L2VPNS (L.34.1.4.6 (t))

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

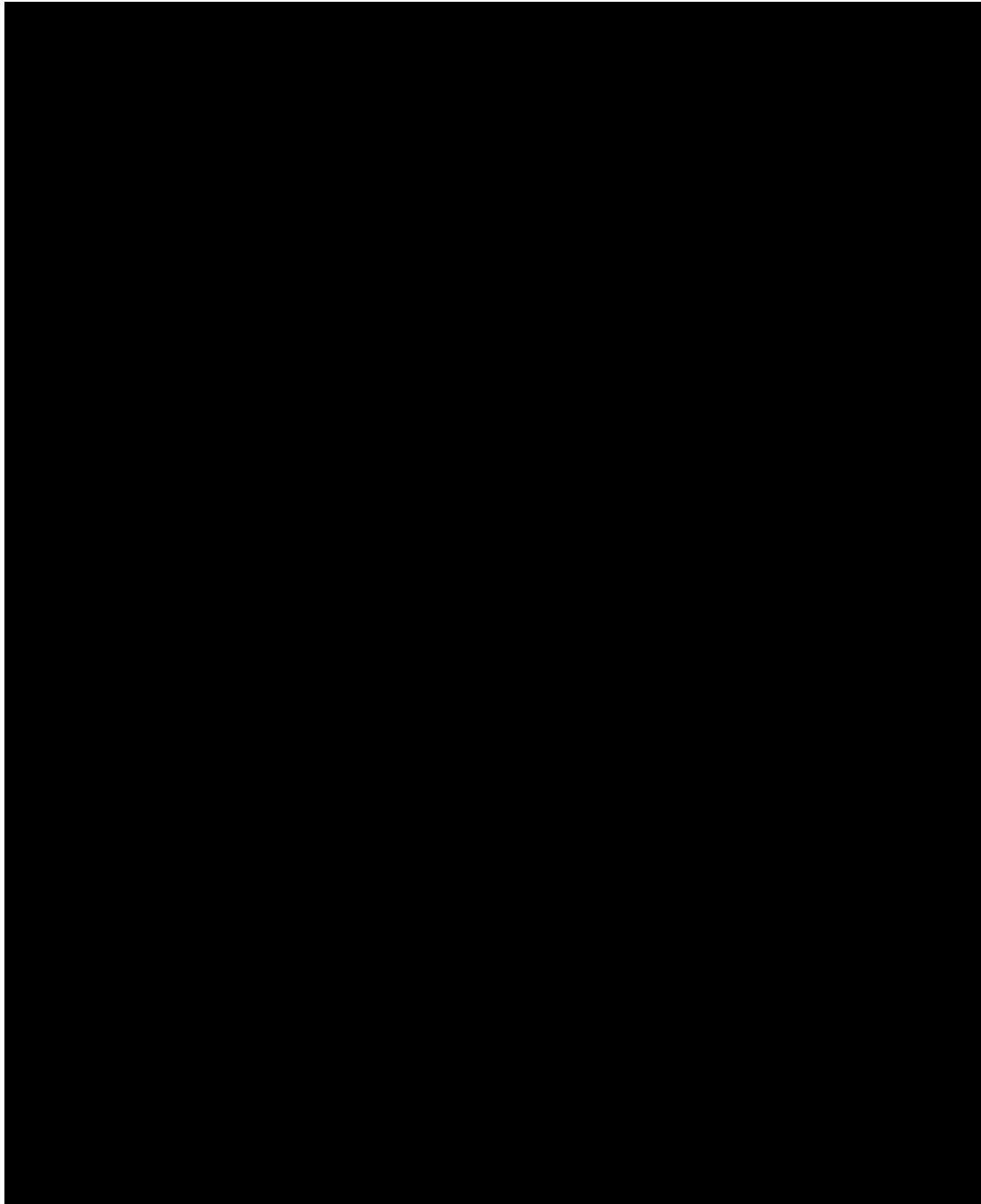
[REDACTED]

4.2.12.21 Vision for Service Internetworking (L.34.1.4.6 (u))

Qwest is committed to the elimination of single-purpose, stovepipe networks that create planning, operations, and interoperability issues for our customers.

[REDACTED]

[illegible]



[illegible]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

4.2.12.22 Support for Government Traffic (L.34.1.4.6 (v))

Qwest has reviewed the Government's traffic model for L2VPN service and does not anticipate any significant impact on currently deployed capacity or the necessity for any specific infrastructure build-out. Qwest L2VPNS is delivered through the Qwest unified service architecture, which consists of an OC-192 MPLS-based infrastructure, engineered for minimal packet loss and network congestion. Qwest closely and continuously monitors its backbone network links and has an aggressive upgrade policy to minimize any effects of congestion on all customer traffic flows.