4.1.13 Internet Protocol Telephony Service (IPTelS) (L.34.1.4)

Qwest has deployed IP telephony services that satisfy Networx requirements; we deliver Networx IPTelS using this proven network platform.

Qwest's Internet Protocol Telephony Service (IPTelS) provides a network-based telephone service over Qwest Internet Protocol (IP)-based network services, such as Internet Protocol Service (IPS) and Network Based Internet Protocol VPN (NBIP-VPNS), using the Voice over Internet Protocol (VoIP), and providing all of the required features. Fully integrated into the Public Switched Telephone Network (PSTN), Qwest's IPTelS allows Agencies to be reached by direct dialing.

Qwest IPTelS offers a new fully-hosted service that replaces the need for a premises-based phone system and the multiple vendors required to provide popular applications like voice mail and integrated messaging. The features and applications are delivered to an Agency's handset via a single IP network connection. These features can be individually customized by the user through Qwest Control Networx Portal. For the Agency, the solution provides centralized management and control, supporting Moves, Adds, Changes and Deletions (MACDs) from an Internet connection.

Figure 4.1.13-1 provides an easy reference to correlate the narrative requirement to our proposal response.

Figure 4.1.13-1. Table of IPTelS Narrative Requirements

Req_ ID	RFP Section	RFP Requirement	Proposal Response
5239	C.2.7.10.1.3	IPTelS requires a connection to the contractor's IP network.	4.1.13.1.1
5232	C.2.7.10.1.4 (2)(e)	Internet Protocol Telephony Service capabilities are mandatory unless indicated otherwise: 2. The contractor shall provide the following minimum capabilities: e. The contractor's IPTelS shall interoperate with non commercial, Agency specific 700 numbers.	4.1.13.3.1.1
5228	C.2.7.10.1.4 (3)	Internet Protocol Telephony Service capabilities are mandatory unless indicated otherwise: 3. The contractor shall provide	4.1.13.3.1.1

Data contained on this page is subject to the restrictions on the title page of this proposal.

Req_ ID	RFP Section	RFP Requirement	Proposal Response
		gateway's for interoperability with IPTelS and the PSTN, or with Agency UNIs.	
5222	C.2.7.10.1.4 (5)	5. The contractor shall provide a routing prioritization scheme or class of service.	4.1.13.3.1.1
5220	C.2.7.10.1.4 (6)	6. The contractor shall provide the capability to support station mobility.	4.1.13.3.1.1
5217	C.2.7.10.1.4 (8)	8. The contractor shall verify with the Agency that the Agency firewall is compatible with the contractors' service.	4.1.13.3.1.1
5214	C.2.7.10.1.4 (11)	11. The contractor shall ensure security practices and safeguards are provided to minimize susceptibility to security issues and prevent unauthorized access.	4.1.13.3.1.1
5213	C.2.7.10.1.4 (11)	11. The contractor shall ensure security practices and policies are updated and audited regularly.	4.1.13.3.1.1
5211	C.2.7.10.1.4 (11)(a)	11. Internet Protocol Telephony Service capabilities are mandatory unless indicated otherwise: a. Denial of service - The contractor shall provide safeguards to prevent hackers, worms, or viruses from denying legitimate IPTelS users and subscribers from accessing IPTelS.	4.1.13.3.1.1
5210	C.2.7.10.1.4 (11)(b)	11. Internet Protocol Telephony Service capabilities are mandatory unless indicated otherwise: b. Intrusion - The contractor shall provide safeguards to mitigate attempts to illegitimately use IPTelS service.	4.1.13.3.1.1
5209	C.2.7.10.1.4 (11)(c)	11. Internet Protocol Telephony Service capabilities are mandatory unless indicated otherwise: c. Invasion of Privacy - The contractor shall ensure IPTelS is private and that unauthorized third parties cannot eavesdrop or intercept IPTelS communications.	4.1.13.3.1.1
5129	C.2.7.10.3.2 (2)	IP Telephony Service Interfaces UNI Type 1 Interface Type: Router or LAN Ethernet port: RJ-45 (Std: IEEE 802.3), Payload Data Rate or Bandwidth: Up to 100 Mbps, Signaling Type: SIP, H.323, MGCP	4.1.13.3.1.3

4.1.13.1 Qwest's Technical Approach to IPTelS Delivery (L.34.1.4.1)

Qwest's solution for the Networx IPTelS leverages our commercial Hosted VoIP service as described in the following sections.

4.1.13.1.1 Approach to IPTelS Delivery (L.34.1.4.1(a))

Qwest IPTelS is a market leading IP-based application that provides real-time, two-way voice capability over IP. Qwest IPTelS offers a fully-hosted service that replaces the need for a premises-based phone system (e.g. Private Branch Exchange (PBX), KTS), Public Switched Telephone Network (PSTN) infrastructure, and the multiple vendors required to provide popular applications like voice mail and integrated messaging. Features and applications are delivered to a subscriber's handset via a single access facility and can be individually customized through the Qwest Control Networx Portal. Our IPTelS solution is hosted on Qwest's OC-192, IP/ Multi-Protocol

Data contained on this page is subject to the restrictions on the title page of this proposal.

Label Switching (MPLS) backbone network. The low packet loss rate and low jitter of the Qwest IP network supporting the Qwest IPTelS service ensures that Agencies will experience the same voice quality they receive from their existing PBX and the PSTN.

Qwest extends its VoIP backbone expertise in the areas of dedicated Networx pre-sales engineering, network planning, provisioning, and operations to the IPTelS offerings through dedicated teams and resources committed to end-to-end service delivery. Network Operations, Field Engineering, Service Enabling Devices (SED) selection, and Engineering, and Voice Implementation Teams with years of experience in IP Telephony, ensure the highest levels of service availability and quality of service. Likewise, VoIP Engineering works closely with Network Operations, Security, Product, and IT to ensure network performance and technology advances in the underlying architecture. Qwest's experience in deploying toll-quality VoIP switches in the Qwest PSTN is demonstrated by a service that today carries more than 4 billion minutes per month of VoIP traffic.

A representation of a typical implementation of Qwest IPTelS solution is shown in [redacted]

Qwest currently supports VoIP handsets and PC-based clients [redacted] These are generally connected through an Agency workgroup switch. If Agencies require Virtual LAN (VLAN) Quality of Service (QOS) (dual-access output queues and 802.1q) capabilities, Qwest will work with Agencies to determine the optimal configuration and Qwest will coordinate with Agencies to ensure that required Agency firewall configuration standards support the VoIP traffic and signaling. Firewalls must be able to pass all standard VoIP signaling protocols such as Media Gateway Control Protocol (MGCP), Real-Time Transport Protocol/RTP Control Protocol (RTP/RTCP), Network Time

Data contained on this page is subject to the restrictions on the title page of this proposal.

[redacted]

Protocol (NTP), Domain Name Service (DNS), Trivial File Transfer Protocol (TFTP), User Datagram Protocol (UDP), Transmission Control Protocol (TCP), and Session Initiation Protocol (SIP). An IPTelS SED (or compatible Agency Router) is used to connect between the firewall and the Qwest IP-based services (e.g., IPS, NBIP-VPNS).

IPTelS Connectivity to Qwest IP Network (Req_ ID 5239; C.2.7.10.1.3)

An Agency site will connect to the Qwest IP network via the access options available with IPS and NBIPVPN. Once connected to a Qwest IP-based network service, Qwest uses [redacted] feature servers to provide PBX-like functionality and call control. Off-net originating and terminating calls are routed through one of several [redacted] VoIP gateways to connect to the PSTN. The PSTN destination of the traffic, having been determined by the called number, is forwarded by Integrated Services Digital Network (ISDN) Primary Rate Interface (PRI) to the appropriate Local Voice Network, or via a Feature Group D connection to Long [redacted]

Data contained on this page is subject to the restrictions on the title page of this proposal.

[redacted] Call Flow Example – IPTelS On-Net, shows call flow for on-net calling. This call flow applies for on-net IPTelS calls as well as calls to Qwest-provided Converged IP Services (CIPS). Specifically, once the call is determined to be another IPTelS or CIPS customer (by signaling to the [redacted] feature server), the VoIP connection is made between the end equipment VoIP phone sets.

[redacted] Call Flow Example – IPTelS Off-Net, shows the call flow for IPTelS calls that terminate on the PSTN. The Qwest Feature server handles standard NPA/NXX calls as well as special calls, specifically E911 and 411.

Data contained on this page is subject to the restrictions on the title page of this proposal.

[redacted]

The IPTelS solution also provides centralized management and control of the IP telephony service, allowing an Agency IP Telephony Manager (Administrator) to service changes, hunt/pickup group setup, and Class of Service (CoS) administration via the Qwest Control Networx Portal. [redacted]

Qwest's IPTelS will provide a hierarchical Web-based management capability to enable comprehensive administration and management of the service. [redacted]

Data contained on this page is subject to the restrictions on the title page of this proposal.

[redacted]

Data contained on this page is subject to the restrictions on the title page of this proposal.

Data contained on this page is subject to the restrictions on the title page of this proposal.

Data contained on this page is subject to the restrictions on the title page of this proposal.

[redacted]

Data contained on this page is subject to the restrictions on the title page of this proposal.

[redacted]

Data contained on this page is subject to the restrictions on the title page of this proposal.

[redacted]

Data contained on this page is subject to the restrictions on the title page of this proposal.

4.1.13.1.2 Benefits of Qwest's IPTelS Technical Approach (L.34.1.4.1(b))

Qwest IPTelS gives Agencies the same voice quality and capabilities associated with their own PBX. The Qwest IPTelS's management applications, based on our VoIP service applications, were built with a browser-based model in mind, making it easy for the Agency to administer, manage, and update their features (such as speed dial keys, handset templates, and service changes). ***Figure 4.1.13-8*** summarizes the features and benefits of our IPTelS.

Figure 4.1.13-8 Qwest's IPTelS Features and Benefits

Feature	[redacted]	[redacted]
Qwest's IP/MPLS Network was built to support VoIP.	[redacted]	[redacted]
Web-based IPTelS Office Administration capabilities enable centralized management of IPTelS	[redacted]	[redacted]
Extensive dial plan functionality enables a broad set of required and reliable features	[redacted]	[redacted]

The Qwest IPTelS facilitates the Federal Enterprise Architecture objectives in the following ways, as summarized in ***Figure 4.1.13-9.***

Figure 4.1.13-9 Qwest's IPtelS Support to FEA Objectives

FEA Objective	[redacted]
Improve utilization of Government information resources to focus on core Agency mission and service delivery to citizens by using the FEA.	[redacted]
Enhance cost savings and avoidance	[redacted]

Data contained on this page is subject to the restrictions on the title page of this proposal.

FEA Objective	
Increase cross-Agency and inter-Government collaboration.	

4.1.13.1.3 Solutions to IPTelS Problems (L.34.1.4.1(c))

Figure 4.1.13-10 summarizes the problems that could be encountered in meeting IPTelS requirements and our solutions.

Figure 4.1.13-10. Qwest's Approach to Common IPTelS Delivery Challenges

Problem	
IP latency adversely affecting voice quality	
Call oversubscription can result in quality problems	
Security	

4.1.13.1.4 Synchronization Network Architecture (L.34.1.4.1(d))

Time of Day Synchronization (IP Network)

Data contained on this page is subject to the restrictions on the title page of this proposal.

[redacted]

Data contained on this page is subject to the restrictions on the title page of this proposal.

[redacted]

Data contained on this page is subject to the restrictions on the title page of this proposal.

[redacted]

[redacted]		
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[redacted]

Data contained on this page is subject to the restrictions on the title page of this proposal.

[redacted]

4.1.13.2 Satisfaction of IPTelS Performance Requirements (L.34.1.4.2)

The Qwest IPTelS solution meets all Networx performance requirements. Qwest has proven network monitoring and measuring systems, procedures, and evaluation methods in place to ensure compliance.

4.1.13.2.1 IPTelS Quality of Service (L.34.1.4.2 (a))

As shown in ***Figure 4.1.13-13***, Qwest meets the thresholds for all AQLs with its IPTelS solution. Qwest's performance measurement methodology is fully compliant with the Government's requirement. Qwest leverages the robustness of its OC-192 IP network and the redundancy of its Core High-Speed Backbone Pops (TeraPOPs) to provide high availability, high performance service. Each TeraPOP has multiple fiber links interconnecting it to other TeraPOPs, ensuring no single point of failure in the IP network backbone. Full node redundancy and network symmetry allow for element or patch failure, as dynamic routing logic keeps track of the active systems and application routes. The Qwest VoIP network is currently deployed in geographically diverse locations to ensure fault-tolerance and high-availability. Qwest also assumes responsibility for the local loop (POP – SDP) circuit in measuring performance. Note that for requirements with a service level marked "critical," Qwest requires that all access loops be fully redundant and protected in order to meet the performance level.

Data contained on this page is subject to the restrictions on the title page of this proposal.

Figure 4.1.13-13 Qwest Compliance with Government IPTelS Performance Metrics

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	[redacted]
Latency	Routine	200 ms	≤ 200 ms	[redacted]
Grade of Service (Packet Loss)	Routine	0.4%	≤ 0.4%	[redacted]
Availability	Routine	99.6%	≥ 99.6%	[redacted]
	Critical	99.9%	≥ 99.9%	[redacted]
Jitter	Routine	10 ms	≤ 10 ms	[redacted]
Time to Restore	Without Dispatch	4 hours	≤ 4 hours	[redacted]
	With Dispatch	8 hours	≤ 8 hours	[redacted]

Qwest understands latency to be the average round trip time for a packet to travel between source and destination Service Delivery Points (SDPs) (CONUS only). Latency is measured via [redacted] Qwest's industry leading OC-192 IP/MPLS backbone and IP services network ensures [redacted].

Qwest understands Grade of Service (packet loss) to be the percentage of packets sent by the source SDP that never arrive at the destination SDP. Qwest continually measures the packet loss rate on every aspect of our IPTeIS solution [redacted]

Qwest understands availability to be the percentage of the total reporting interval time that the IPTelS is operationally available to an Agency. Qwest's underlying IP/MPLS-based transport [redacted] Network Availability is measured by Network Downtime, which exists when a particular port is unable to transmit or receive data, as recorded in the [redacted] application based, in part, on auto-generated trouble tickets.

Data contained on this page is subject to the restrictions on the title page of this proposal.

Qwest's IPTelS is provided on multiple server and gateway platforms in geographically diverse data centers and Qwest POPs. [redacted]

Qwest understands jitter to be the variation in the delay between received packets of an IP data stream from SDP to SDP (CONUS only). Jitter is typically the result of network overload. [redacted] Jitter is the measurement of inter-packet delay variance, and is measured by generating synthetic UDP traffic.

4.1.13.2.2 Approach for Monitoring and Measuring IPTelS KPIs and AQLs (L.34.1.4.2 (b))

Qwest monitors and measures the KPIs and Acceptable Quality Levels (AQLs) SDP to SDP using automated processes that pull data from the root source, summarize it, and display it using Web tools. These Web tools display actual results and provide 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

Data contained on this page is subject to the restrictions on the title page of this proposal.

performance report generation. The automated reporting process eliminates any question of manipulating the performance data.

Measuring SDP-to-SDP Latency, Packet Loss and Jitter and the Role of SEDs

All of Qwest's IP-based services, which include the eight mandatory services (IPS, NBIP-VPNS, Premises-based IP VPN Services (PBIP-VPNS), Layer 2 Virtual Private Network Service (L2VPNS), CIPS, Content Delivery Network Services (CDNS), Voice Over Internet Protocol Transport Services (VOIPTS), and IPTelS), are provided over the same IP services infrastructure.

Data contained on this page is subject to the restrictions on the title page of this proposal.

[redacted]

Data contained on this page is subject to the restrictions on the title page of this proposal.

[redacted]

[redacted]

Data contained on this page is subject to the restrictions on the title page of this proposal.

[redacted]

If an Agency orders a service in which the technical performance requirements are specified on an SDP-to-SDP basis (including performance requirements specified on an end-to-end and/or Agency premises-to-Agency premises performance requirement basis) and where Qwest requires the use of SEDs to meet the requirements and/or requires access to, or use of, the Agency's customer-premises equipment or software to meet the requirements, Qwest understands that the ordering Agency may (1) elect to not order such SEDs and/or (2) elect to not permit Qwest access to, or any use of, the Agency's customer-premises equipment or software for such purposes.

Qwest further understands that in these situation(s) and unless otherwise agreed to by Qwest and the user Agency, Qwest, when directed by the user Agency or by GSA, will monitor, measure, and report the performance of the service for KPI/AQL and for SLA purposes either (1) on an SDP-to-SDP basis, by defining the SDP for performance metric measurement purposes for affected location(s) as being located at the connecting POP(s) of the location(s), or (2) on a POP-to-POP basis. If directed to use the latter method by the Agency, Qwest will comply with the following:

Data contained on this page is subject to the restrictions on the title page of this proposal.

1. For all IP-based network services, the applicable POP-to-POP performance requirements to be used will be those defined in Section C.2.4.1 (IPS).
2. For all other services, the service-specific SDP-to-SDP performance metrics will be applied on a POP-to-POP basis unless a stipulated POP-to-POP performance metric already applies for the associated service(s).

   In summary, three options are available:

   1. Standard SDP-to-SDP approach
   2. Auxiliary SED for SDP-to-SDP monitoring
   3. POP-to-POP as defined in Amendment 8

Use of Statistical Sampling in lieu of Direct KPI Measurements

[redacted]

The Use of Government Furnished Property

If an Agency orders a Transport/IP/optical service in which they are employing a Generic Framing Procedure (GFP) device, Qwest will provide KPI monitoring and measurement of the delivered service in three ways:

A. Request the Agency provide SNMP capability to the device for the Qwest NOC
B. Request that the Agency buy a monitoring SED from Qwest
C. Coordinate with the Agency per Amendment 8 change for the following:

   Qwest understands that the ordering Agency may (1) elect to not order such SEDs and/or (2) elect to not permit Qwest access to, or any use of, the Agency's customer-premises equipment or software for such purposes.

Data contained on this page is subject to the restrictions on the title page of this proposal.

Qwest further understands that in these situation(s) and unless otherwise agreed to by Qwest and the user Agency, Qwest, when directed by the user Agency or by GSA, will monitor, measure, and report the performance of the service for KPI/AQL and for SLA purposes either (1) on an SDP-to-SDP basis, by defining the SDP for performance metric measurement purposes for affected location(s) as being located at the connecting POP(s) of the location(s), or (2) on a POP-to-POP basis.

[redacted]

For all services that Qwest offers, we use [redacted] a trouble ticketing system that is an industry-leading off-the-shelf commercial application which we have customized to make more effective for our needs. From this system, we collect many useful metrics that we use internally to evaluate and improve our processes including Time to Restore (TTR). The calculation for TTR uses the same business rules, as the Government requires for its services.

IPTelS will rely heavily on the integrity of Qwest's underlying Transport and Data infrastructures. Also, as with VS and TFS, Qwest relies on service layer-specific performance data. For IPTelS, standard IP measurements tools are used to measure the common IP KPIs such as delay, packet loss, and jitter. These parameters are measured using specialized equipment [redacted] where a call path is

Data contained on this page is subject to the restrictions on the title page of this proposal.

monitored from a network availability perspective. Utilizing the [redacted] tools, Qwest provides proactive management alerts to our network management centers to drive prompt problem resolution. Data is analyzed, formatted, and sent to operations, engineering, and planning for pro-active network enhancement and capacity planning. This combined approach enables Qwest to reduce TTR and increase mean time between failures (MTBF) to effectively support our world class network operation.

SDP to SDP performance is determined through active measurement from probes to SED. The probes are installed in each IPTelS-capable POP, and provide PE to SDP measurements. The probes also monitor POP-to-POP performance through active measurements among themselves. These measurements combine to give a full end-to-end performance picture to the NOC and to the Agency.

The Qwest Infrastructure Group monitors IP Network utilization and reports statistics to the Data Network Planning and Design group. This information also is distributed to internal databases and is available to customers through the Qwest Control Networx Portal. This portal provides Agencies with performance statistics to verify that customer-specified AQLs are met. Agencies may also submit a real-time performance query to the Qwest North America IP Network. [redacted]

Qwest's Next Generation VoIP Switch (NGS) has been in existence for the last six years and interconnects with the Time Division Multiplexers (TDM) at each end, providing Long Distance Voice services (PSTN) with VoIP transport in the middle. A separate Qwest VoIP network handles only the Local Voice (PSTN) calling services. [redacted]

Data contained on this page is subject to the restrictions on the title page of this proposal.

Equipment Alarm systems: [redacted] has been designed to monitor all of the Switches for Alarms and SNMP traps. This is a centralized collection for simple monitoring. Our [redacted] are platform specific monitoring systems that utilize of SNMP alarms. [redacted] maintains the monitoring while system logs are kept for any network issues or problems.

Statistics:. Qwest's custom tools monitor the switching environments and provide alerts for proactive intervention, including Switch capacity of [redacted] Our [redacted] tool is used for monitoring the CPU, disk space, and memory on the equipment, and also includes key statistics like Calls per Second. Another Qwest internal tool provides comparisons between logs from all of the network equipment for correlation and analysis for better root cause analysis and to verify how equipment is running at different levels. All of the above statistics gathered provide us with levels of utilization.

QOS systems:

- [redacted]
- [redacted] maintains and tests QOS levels for IP
- [redacted]
- Various diagnostic tools check interaction between TDM, IP, and record system logs.

Surveillance/Support groups: Qwest's surveillance group handles both VoIP and TDM networks.

4.1.13.2.3 IPTelS Performance Improvements (L.34.1.4.2 (c))

Qwest proposes to meet all required KPIs and AQLs for IPTelS. In the event an Agency has a specific business need or application problem, Qwest is willing to discuss service enhancements. Qwest will operate in good faith to engineer an IPTelS solution to serve unique Agency needs. Qwest is able to leverage our vast IPTelS product portfolio which includes a variety of SED

Data contained on this page is subject to the restrictions on the title page of this proposal.

providers and specific IPTelS solutions. Through a special combination of vendor solutions and talented engineering capabilities Qwest will be able to serve an Agency's business needs.

4.1.13.2.4 Additional IPTelS Performance Metrics (L.34.1.4.2 (d))

[redacted]

4.1.13.3 Satisfaction of IPTelS Specifications (L.34.1.4.3)

Qwest is fully compliant to all IPTelS requirements using our commercial, Hosted VoIP service as a base.

4.1.13.3.1 Satisfaction of IPTelS Requirements (L.34.1.4.3 (a))

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

4.1.13.3.1.1 Satisfaction of IPTelS Capability Requirements (L.34.1.4.3(a); C.2.7.10.1.4)

Figure 4.1.13-14 below summarizes Qwest's technical approach to delivering the IPTelS capabilities in RFP C.2.7.10.1.4. Qwest fully complies with all mandatory stipulated and narrative features, capabilities, and interface requirements for IPTelS. Figure 4.1.13-14 is intended to provide the technical description required per L.34.1.4.3(a), and does not limit or caveat Qwest's compliance in any way.

Figure 4.1.13-14. Qwest's Technical Approach to IPTelS Capabilities

ID #	Name of Capability	[redacted]
1	Originate and Terminate on-net and PSTN calls	[redacted]
2	Minimum Capabilities	[redacted]

Data contained on this page is subject to the restrictions on the title page of this proposal.

ID #	Name of Capability	[redacted]
		[redacted]
3	Gateways	[redacted]
4.	Alternate Routing	[redacted]
5	Routing Prioritization	[redacted]
6	Station Mobility	[redacted]
7	911 & E911	[redacted]
8	Traverse Agency Firewalls	[redacted]
9	Minimum Quality Level	[redacted]
10	Local Number Portability	[redacted]
11	Security Practices and Safeguards	[redacted]

Data contained on this page is subject to the restrictions on the title page of this proposal.

ID #	Name of Capability	[redacted]
		[redacted]
12	Call Routing between PSTN and IP	[redacted]
13	Secure Web Site for Subscribers	[redacted]
14	Basic Phone Service Features	[redacted]

Interoperability with Agency-specific 700 numbers (Req_ ID 5232; C.2.7.10.1.4 (2)(e))

The IPTelS dial plan supports routing of Agency specific 700 numbers. The 710 NPA is currently implemented in the Qwest network. Qwest will implement other 7XX NPAs as needed. The [redacted] RMS is a fully functional route management server, which allows us the capability to build and assign flexible dial plans and routing on an Agency basis allowing for necessary customization to support Agency specific 700 numbers.

Interoperability with PSTN and Agency UNIs (Req_ ID 5228; C.2.7.10.1.4 (3))

IPTelS supports interoperability for non-IP telephone devices. Qwest provides non-proprietary telephony station UNIs including (a) analog station and (b) ISDN BRI station (Optional) interfaces via gateway devices. IPTelS will provide transparent access to and interwork with the domestic and non-domestic PSTNs. IPTelS supports interoperability with any 10 digit telephone

Data contained on this page is subject to the restrictions on the title page of this proposal.

number, whether the number is part of the PSTN or part of the VoIP platform. The [redacted] and [redacted] PSTN gateways work in concert to provide seamless interoperability and access to the PSTN network.

Routing Prioritization/Class of Service (Req_ ID 5222; C.2.7.10.1.4(5))

To enable the convergence of customer applications, such as the use of private real-time applications like VoIP and IP-based videoconferencing, or access to Qwest's VoIP and video conferencing services, Qwest provides a [redacted] CoS queue design:

[redacted] Agencies may select any of the queuing implementations on a per-port basis, restricted only by what options are available on the applicable access type for the port.

All queuing methods described are applied at the network egress router port (traffic leaving the Qwest network PE on the access line towards the Agency CE router). Therefore, the queuing prioritizes one or more types of Agency traffic over other types of traffic. Because it is applied at the port

Data contained on this page is subject to the restrictions on the title page of this proposal.

level, these mechanisms are not prioritizing Agency traffic over another customer's traffic and vice versa. All traffic that exceeds the speed of the Agency's port is buffered or discarded at the egress point in the network.

[redacted]

Data contained on this page is subject to the restrictions on the title page of this proposal.

Agencies have the option to apply Unique QOS policies on each port, as follows:

Data contained on this page is subject to the restrictions on the title page of this proposal.

[redacted]

Station Mobility (Req_ ID 5220; C.2.7.10.1.4 (6))

Station mobility and portability is supported via DHCP at the service location. After the local DHCP resource assigns an IP Address the station will re-register with the IPTelS system. Mobility outside of the physical location is supported through the same mechanism. The mobility is provided by the functionality of Qwest's OneFlex portal and can be used at any Internet location. For example, if a phone has been moved to another station location on the network, the portal can be accessed at that location.

A change of physical location requires notification to Qwest so that E.911 databases can be kept current.

Agency Firewall Compatibility (Req_ ID 5217; C.2.7.10.1.4 (8))

Qwest voice implementation will work with the Agency at the time of Agency turn-up to ensure that Agency firewall is configured to interoperate with the Qwest IPTelS. If any issues are detected by the Qwest team, Qwest will work with the Agency to isolate and guide the Agency to the appropriate configuration.

Security Practices and Safeguards (Req_ ID 5214; C.2.7.10.1.4 (11))

IPTelS complies with all industry security best practices and safeguards to minimize susceptibility to security issues and prevent unauthorized access. The network architecture is built around [redacted] The VoIP firewalls [redacted] perform many security functions. One such function is anchoring the media and signaling to protect Agency and network external IP addresses from being exposed. DDOS protection, rogue calls, Call Admission Control, and other mechanisms are

Data contained on this page is subject to the restrictions on the title page of this proposal.

analyzed and enforced as well. A Routing Engine coordinates traffic between the VoIP Firewalls and multiple feature and media servers.

Qwest implements industry standard security to ensure data assurance, integrity, and confidentiality of customer and company information in support of our telecommunications services. These practices include implementing controls specifically in the areas of personnel, systems, and facility security. Qwest has also implemented comprehensive business continuity and disaster recovery measures and controls to ensure the availability of customer and corporate networks.

To ensure the security architecture stays current with best practices, Qwest takes a lead role in developing standards, working with vendors and implementing new, innovative approaches to improve our products, including security services. Qwest maintains relationships with key network equipment vendors to provide a bi-directional dialog on best security practices and new feature development along with our membership and participation in a variety of industry and standards forums including [redacted] Additionally, we provide a dedicated representative at the NCS's National Coordinating Center for Telecommunications.

Qwest will provide safeguards to prevent hackers, worms, or viruses from denying legitimate IPTelS users and subscribers from accessing IPTelS. Qwest also uses a combination of physical security, operational procedures, and logical separation of services to ensure the integrity of IPTelS and prevent hackers, worms, or viruses from penetrating or spreading across network elements and degrading IPTelS.

Data contained on this page is subject to the restrictions on the title page of this proposal.

Specific protections against cyber attacks include:

a) [redacted]

Data contained on this page is subject to the restrictions on the title page of this proposal.

[redacted]

Security Updates and Audit (Req_ ID 5213; C.2.7.10.1.4 (11))

Qwest will ensure security practices and policies are updated and audited regularly. Qwest performs on-going audit scans on production

Data contained on this page is subject to the restrictions on the title page of this proposal.

network elements. We have a mature auditing process that includes [redacted]

Qwest implements industry standard security to ensure data assurance, integrity, and confidentiality of customer and company information in support of our telecommunications services. These practices include implementing controls specifically in the areas of personnel, systems, and facility security. Qwest has also implemented comprehensive business continuity and disaster recovery measures and controls to ensure the availability of customer and corporate networks

Qwest takes a lead role in developing standards to ensure the security architecture stays current with best practices, working with vendors and implementing new, innovative approaches to improve our products, including security services. Qwest maintains relationships with key network equipment vendors to provide a bi-directional dialog on best security practices and new feature development along with our membership and participation in a variety of industry and standards forums including [redacted]

Denial of Service (Req_ ID 5211; C.2.7.10.1.4 (11)(a))

Multiple safeguards are in place to protect the IPTelS network from hackers, worms, and viruses. Primarily, [redacted] screen all traffic into and out of the IPTelS Network. In addition, the following protective measures are used:

Data contained on this page is subject to the restrictions on the title page of this proposal.

[redacted]

Qwest will provide safeguards to prevent hackers, worms, or viruses from denying legitimate IPTelS users and subscribers from accessing IPTelS. Qwest also uses a combination of physical security, operational procedures, and logical separation of services to ensure the integrity of IPTelS and prevent hackers, worms, or viruses from penetrating or spreading across network elements and degrading IPTelS.

Specific protections against cyber attacks include:

[redacted]

Data contained on this page is subject to the restrictions on the title page of this proposal.

[redacted]

Data contained on this page is subject to the restrictions on the title page of this proposal.

[redacted]

Intrusion/Illegitimate Use Of IPTelS (Req_ ID 5210; C.2.7.10.1.4 (11)(b))

Only registered subscribers of the IPTelS or CIPS can access the network. Numerous safeguards, from [redacted] prevent unauthorized users from illegitimately using the system.

Invasion of Privacy (Req_ ID 5209;C.2.7.10.1.4 (11)(c))

The combination of physical security, operational procedures, and logical separation of services ensures the privacy of IPTelS traffic. Qwest ensures the privacy of customer IPTelS traffic through security built into the design of the network and operational procedures that provide ongoing security; the network is physically and logically protected. Qwest facilities ensure physical security with the use of controlled access equipment rooms.

With Qwest on-net service, traffic traverses the Qwest trusted network over a private backbone infrastructure that inherently prevents third party attempts to intercept VOIP and data communications. Qwest analyzes, assesses, designs, and implements security solutions designed to review security and improve security policy and infrastructure. Qwest will ensure the IPTelS can not be intercepted or unauthorized third parties cannot eavesdrop

Data contained on this page is subject to the restrictions on the title page of this proposal.

on the packet payloads through the use of [redacted]

Only registered subscribers of Qwest's IPTelS service can access the network. Numerous safeguards, including [redacted] prevent unauthorized users from illegitimately using the system. [redacted]

Allowing [redacted]

4.1.13.3.1.2 Satisfaction of IPTelS Feature Requirements (L.34.1.4.3(a); C.2.7.10.2)

Figure 4.1.13-15 below summarizes our technical approach to satisfying all IPTelS features required for the Networx program. All of the enumerated features are provided by the [redacted] server. Qwest fully complies with all mandatory stipulated and narrative features, capabilities, and interface requirements for IPTelS. Figure 4.1.13-15 is intended to provide the technical description required per L.34.1.4.3(a), and does not limit or caveat Qwest's compliance in any way.

Figure 4.1.13-15. Summary of Technical Approach to Meeting IPTelS Feature Requirements

ID Number	Name of Feature	[redacted]
1	Find Me Follow Me Routing	[redacted]
2	IP Telephony	[redacted]

Data contained on this page is subject to the restrictions on the title page of this proposal.

ID Number	Name of Feature	[redacted]
	Manager (Subscriber)	[redacted]
3	IP Telephony Manager (Administrator)	[redacted]
4	Voice Mail Box	[redacted]

4.1.13.3.1.3 Satisfaction of IPTelS Interface Requirements (L.34.1.4.3(a); C.2.7.10.3)

Figure 4.1.13-16 summarizes our support of IPTelS interfaces, including the SED that we intend to use to deliver the services. Qwest fully complies with all mandatory stipulated and narrative features, capabilities, and interface requirements for IPTelS. Figure 4.1.13-16 is intended to provide the technical description required per L.34.1.4.3(a), and does not limit or caveat Qwest's compliance in any way.

Data contained on this page is subject to the restrictions on the title page of this proposal.

Figure 4.1.13-16. Qwest's Provided IPTelS Interfaces at the DSP

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Signaling or Protocol	[redacted]
1	Router or LAN Ethernet port: RJ-45 (Std: IEEE 802.3)	Up to 100 Mbps	SIP, H.323, MGCP, or SCCP (Optional)	[redacted]
2	Analog Line: Two-Wire (Std: Telcordia SR TSV-002275)	4 kHz Bandwidth	Line - Loop Signaling	[redacted]
3 Optional	Digital line: ISDN BRI S and T Reference Point (Std: ANSI T1.607 and 610)	Up to 128 Kbps (2x64 kbps)	ITU-TSS Q.931	[redacted]

IP Telephony Interfaces UNI Type 1 (Req_ ID 5129; C.2.7.10.3.1 (1))

Qwest will meet this requirement with a [redacted] with a 10/100 LAN interface at the Agency site.

4.1.13.3.2 Proposed Enhancements for Internet Protocol Telephony Service (L.34.1.4.3(b))

Figure 4.1.13-17 summarizes several proposed capabilities for Qwest IPTelS that exceed Networx requirements.

Figure 4.1.13-17. Qwest IPTelS Enhanced Capabilities

Name of Feature	Description	[redacted]
Microsoft Outlook Integration	IPTelS Dashboard integrated with customer's Outlook Email Client.	[redacted]
Unified Messaging	Integrated email, voice messaging, and electronic faxing.	[redacted]
My Assistant Tool	IPTelS Dashboard tool that enables a user to set-up special call treatments by type of caller and time of day settings.	[redacted]
Auto Attendant	IPTelS Auto Attendant feature automatically answers and routes all incoming calls to the correct destinations in a Government Agency.	[redacted]

Data contained on this page is subject to the restrictions on the title page of this proposal.

4.1.13.3.3 Network Modifications Required for IPTelS Delivery (L.34.1.4.3 (c))

There are no modifications required to the Qwest Hosted VoIP service offering to satisfy Networx IPTelS requirements.

4.1.13.3.4 Experience with IPTelS Delivery (L.34.1.4.3 (d))

Qwest has years of experience in VoIP technology and has performed numerous trials and implementations of commercialized Hosted VoIP services within the manufacturing, legal, retail, and financial services industries. Qwest has been carrying large portions of its classic long distance traffic over IP [redacted] since 2001. This has enabled Qwest to provide more cost effective and reliable long distance service.

Qwest is a proven player in the IP and VoIP market. Qwest seamlessly sends four billion minutes of use per month of VoIP traffic across our IP network.

Qwest has long been a leader in IP network technology. Its robust fiber-based OC-192 network provides IP and MPLS services to a number of Government customers. With its experience, Qwest can offer various solutions to begin the migration of existing TDM equipment utilizing the Qwest IPTelS solution.

Qwest's IP services solutions have supported Federal, commercial, and educational enterprises for more than 20 years, including our past experience as US West. [redacted]

Qwest provides IP transport services on a nationwide and global basis to a majority of the Fortune 500 U.S.-based businesses and continues to

Data contained on this page is subject to the restrictions on the title page of this proposal.

exceed industry performance measurements for service, features, and availability. Qwest presently supports [redacted] dedicated IP access connections originating from Qwest's OC-192 IP/MPLS Network. [redacted]

4.1.13.4 Robust Delivery of IPTelS (L.34.1.4.4)

The following sections describe the Qwest support of Government traffic and the engineering approach to network design by Qwest that will provide a robust delivery of IPTelS.

4.1.13.4.1 Support for Government IPTelS Traffic (L.34.1.4.4 (a))

The Government traffic model requirements are modest in the early years, adding only about 1,000 clients a year through Year 3. In Year 4, the demand begins to increase, culminating in a total of approximately 190,000 subscribers (telephone numbers) by year 10.

The Qwest infrastructure that supports IPTelS is modular, consisting of discrete components to provide the [redacted] Each one of these modules can be expanded or supplemented as required. [redacted] However, we expect that future generations of these components will provide much higher subscriber density per element. The [redacted] As later year requirements increase, Qwest would add network components as required to meet the demand.

Data contained on this page is subject to the restrictions on the title page of this proposal.

4.1.13.4.2 IPTelS Measures and Engineering Practices (L.34.1.4.4 (b))

The speed and size of Agencies' telecommunications systems can grow easily and transparently on the Qwest Network. Qwest has a history of adapting rapidly to meet customer requirements. [redacted] As their traffic requirements grew, Qwest used the practices described here to incrementally transition the customer to an OC-192 wavelength network. IPTelS explicitly requires that network resiliency and growth be addressed both from an IP transport infrastructure standpoint and from the support of voice capabilities. The following paragraphs first address our approach for engineering planning for our core network, then discuss our voice oriented strategy.

Qwest builds its network to provide high availability to our customers. Qwest's performance measures and engineering practices are designed to provide robustness of the access and backbone networks, to ensure resiliency, and to prepare for growth. Our design procedures, network modeling, and circuit route checks provide a high level of customer service.

These practices include application of network design rules, network capacity modeling for failure scenarios, and circuit route check to ensure redundant and diverse routing. In addition, the design of our network unifies technologies under a common service platform where all network elements are designed with resiliency and growth in mind.

A consistent capacity management model is applied by a centralized engineering team for all data services. Qwest establishes design rules for both edge and backbone network elements. Using these rules as a guide, we gather usage statistics to verify network status and take corrective action as necessary. [redacted]

Data contained on this page is subject to the restrictions on the title page of this proposal.

[redacted] Edge aggregation devices are those devices that directly terminate customer circuits. Usage statistics are gathered on every edge aggregation circuit, and reports are generated using these samples for weekly review. [redacted]

[redacted] of the same speed, provisioned over diverse physical facilities provided by the Qwest state-of-the-art nationwide Dense Wavelength Division Multiplexing wavelength network and self-healing SONET backbone. Usage reports are gathered and reviewed for all backbone circuits (defined as those circuits that interconnect core backbone devices) just as they are for the edge aggregation circuits. [redacted]

Data contained on this page is subject to the restrictions on the title page of this proposal.

Qwest engineers continuously model network capacity using current and forecasted traffic to ensure that customer traffic is routed efficiently through the network. This assists with sizing backbone links.

We analyze how the traffic utilization patterns will be affected under abnormal network conditions, then take the appropriate action, such as adding new nodes or links. [redacted] We are able to predict how the failure would affect traffic utilization on the other backbone circuits and identify backbone circuits that need to be upgraded.

When placing an order to have a new backbone link added to the network, the Qwest engineers will circuit-route check the facilities to make sure the new backbone link is distinct from the other backbone links. The new circuit route information will then be entered into the order to be carried out by the Qwest Provisioning team. Qwest engineering audits existing backbone circuits several times a year to make sure that the backbone links are diverse.

In addition, simulations are run to determine the traffic distribution in the event of a failure of any router, link, or fiber path in the network. This takes into consideration the fact that multiple long haul circuits may share a single conduit in some sections of the fiber network. The network is designed to be able to handle the full offered load in the event of any single failure, so the physical routing of the new circuit must follow a path that allows it to meet these requirements. The new circuit route information will then be entered into the order to be carried out by the Qwest provisioning team.

Qwest's network planning and engineering organizations use strict engineering rules to create the highly robust private MPLS core, Public Provider Edge, and border router architectures that comprise the Qwest domestic and Asian IP network. These organizations continually monitor

Data contained on this page is subject to the restrictions on the title page of this proposal.

network performance, and the capacity utilization of core network connections and our peering points, to ensure the highest performance for our customers.

A key element of IPTELS involves the support for voice-based services. Qwest VoIP service will scale to meet future Agency capacity requirements through modular network architecture consisting of discreet components providing [redacted] Each one of these modules can be expanded or supplemented as required.

[redacted]

Qwest has chosen vendor platforms that meet some form of high availability scheme. Depending on the system, there may be a 1+1 or N+1 configuration of hardware to ensure high reliability for voice services. Qwest's goal is to provide its Agencies with a network that meets their requirements.

[redacted] Connectivity to the Agency premise can be done via diverse paths.SS7 Signaling is done via an extremely robust network. [redacted] All of the SS7 systems are fully redundant and geographically redundant as well. Voice traffic and signaling traffic is carried over SONET rings for secured transport.

Data contained on this page is subject to the restrictions on the title page of this proposal.

Qwest's IPTelS network supporting elements [redacted] etc.) are built to support a specific number of subscribers. Subscriber growth and new subscriber additions are constantly monitored to determine targeted growth rates and capacity additions are engineered and implemented far in advance of the estimated dates of exhaustion of current network resources. Qwest ensures that accurate forecasts are evaluated on a regular basis to provide appropriate capacity for the VoIP platform.

4.1.13.5 IPTelS Optimization and Interoperability (L.34.1.4.5)

The following sections detail Qwest's optimization approach, optimization of the network architecture, access optimization, and service internetworking.

4.1.13.5.1 Optimizing the Engineering of IPTelS (L.34.1.4.5(a))

Planning and Engineering of IPTelS services centers around a multi-set design process. Planning produces monthly reports for the IPTelS system that specify current utilization and forecast utilization. [redacted] In addition to monthly reporting, large Agency orders will also trigger this process to ensure that capacity is available.

Once this trigger is met, a number of activities result. First, the planning team builds a proposal for the capacity augmentation. This proposal identifies scenarios for how much new capacity will be built, how much that capacity will cost, and a list of project milestones. The growth proposal is built using existing models and configurations that have been certified for field use by the [redacted] This method ensures that capacity will be available for Qwest customers and that new service will not be delayed. Use of certified models and configurations mitigates risk of

Data contained on this page is subject to the restrictions on the title page of this proposal.

network deployment through standardized deployments and software configurations that are the result of detailed testing.

[redacted]

4.1.13.5.2 Methods Applied to Optimize the Network Architecture (L.34.1.4.5 (b))

We use a variety of methods to optimize our network architecture. The current Qwest network-based MPLS service offering is built on a nationwide OC-192 core IP/MPLS network. The Qwest Internet network consists of a global AS 209 ID with [redacted] major TeraPOPs that are interconnected by 10

Data contained on this page is subject to the restrictions on the title page of this proposal.

Gbps connections. Qwest has [redacted] smaller regional IP POPs connected via SONET connections ranging from OC-3 to OC-48. Most of the network was built within the last five years, including all aspects from the optical layer to the IP network elements. Therefore, Qwest has the advantage of not having to accommodate pockets of legacy equipment in our MPLS network.

Even though we do not have legacy equipment in our network, we are constantly evaluating and optimizing the network architecture, primarily due to the following:

a) Services – what services are riding on the network for our customers
b) Network growth – what is the projected utilization of the network
c) Technology evolution – what new technology is available that will help us deliver better service to our customers

Architecture Optimization for Services

As Qwest is in the business of providing network services, the architecture and behavior of the network is predominantly based on the type of service being provided. Every product is developed and tested against the current architecture before it is launched. If the existing architecture does not support the product, it is modified and optimized. For example, the initial Qwest IPS network was built to [redacted] The network consisted of routers connected via OC-48 links. When we started carrying Inter-Exchange Carrier voice traffic on the IP network, we reviewed the architecture and deployed MPLS on the backbone to improve the performance of the network.

For all voice services, including IPTelS, the Qwest network is migrating to a packet-based backbone, particularly through the use of IP/MPLS infrastructure. The migration to this routed network infrastructure improves Qwest's use of transmission facilities supporting voice services by eliminating

Data contained on this page is subject to the restrictions on the title page of this proposal.

the inefficiencies in maintaining two separate networks (IP data and PSTN) and moving to one IP/MPLS network.

Network High Availability is addressed via redundancy at multiple levels:

[redacted]

Call Admission Control prevents over-utilization of access links. Defense in Depth maximizes protection of service and network elements in several layers:

[redacted]

Architecture Optimization for Network Growth

The IPTelS network has been carrying growing amounts of traffic. As the volume of traffic grows, the network architecture is reviewed to ensure that it is still scalable and that it can be improved to continue to provide excellent service.

Data contained on this page is subject to the restrictions on the title page of this proposal.

As the IPS Network started growing, our OC48 backbone links were no longer sufficient to carry the traffic. With the help of our transport network, we changed the underlying architecture to use wavelength based 10Gbps circuits to connect the core routers. Qwest implemented MPLS Fast Re-route to provide better protection on the network. [redacted]

Architecture Optimization for Technological Advances

Over the years, the IPTelS network has evolved to a strategic network for Qwest and Qwest has always stayed ahead of the technology. As the equipment vendors have provided improved platforms with more features and functionality, Qwest evaluates them against the current architecture. With the help of this evaluation, Qwest can optimize any part of the network and grow with services and customer requirements. [redacted]

4.1.13.5.3 Access Optimization for IPTelS (L.34.1.4.5(c))

Convergence of edge technologies is progressing rapidly as customers strive to handle many applications over a single facility type. Qwest is focused on providing access facilities that meet this need with dedicated and switched technologies. To be effective, a multi-application access facility must meet a number of requirements.

QOS is critical for this environment. Data, voice, email, video, and other applications all have different QOS requirements. QOS measures will ensure that these applications can be used across a common facility effectively. In the case of IPTelS, QOS implemented in the edge routers ensures that VoIP traffic is given priority over other IP traffic. The Qwest network recognizes individual applications within the IP stream and prioritizes based upon CoS markings.

Data contained on this page is subject to the restrictions on the title page of this proposal.

Qwest further provides access to traditional telephony applications through the customer's multi-service connection. Qwest's IPTelS and TDM networks are interconnected through distributed [redacted] gateways across the U.S. IPTelS has access to these gateways and their services through the dedicated Internet access connection.

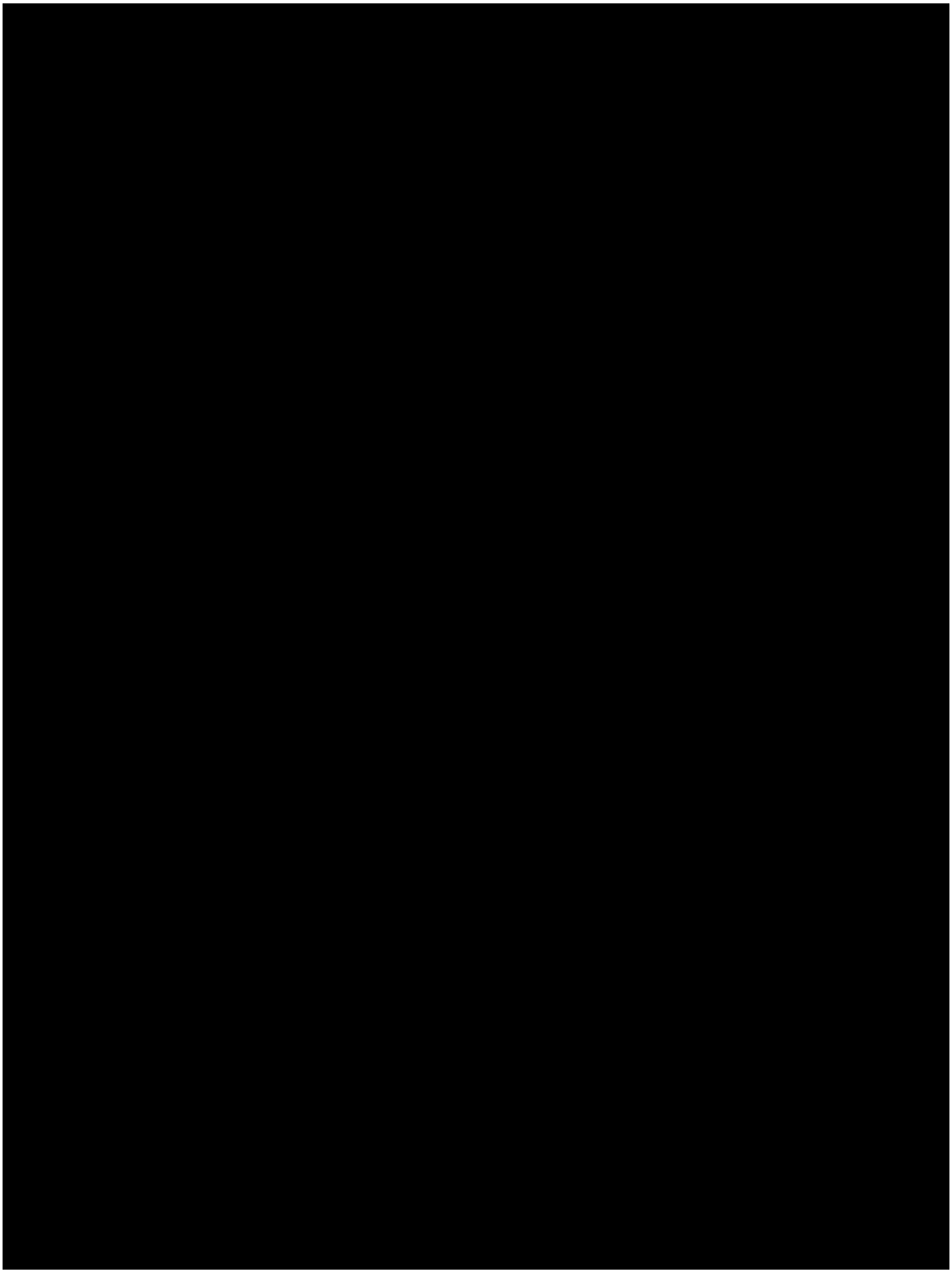
4.1.13.5.4 Vision for IPTelS Internetworking (L.34.1.4.5(d))

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

Qwest's service delivery model supports multiple types of customer requirements. Qwest's approach for network architecture evolution guides our investments and provides the overall direction for our technology evolution and services convergence. Qwest's service delivery model also allows us to assess the interoperability impacts of changes in the technical elements in each network area (e.g., Access, Service Control, Edge, Core, MPLS, and Optical).

[redacted]

Data contained on this page is subject to the restrictions on the title page of this proposal.



Data contained on this page is subject to the restrictions on the title page of this proposal.

[redacted]

Data contained on this page is subject to the restrictions on the title page of this proposal.

[redacted]

Data contained on this page is subject to the restrictions on the title page of this proposal.

[redacted]

In summary, the Qwest backbone has been transformed from primarily serving Internet traffic into a general-purpose packet transport network with TDM-like quality characteristics, capable of serving multiple kinds of application traffic, including Internet, Layer 3 VPNs, Layer 2 VPNs, VoIP, Video over IP, Storage over IP, etc.

Data contained on this page is subject to the restrictions on the title page of this proposal.