4.1.3 VOICE OVER INTERNET PROTOCOL TRANSPORT SERVICES (VOIPTS) (L.34.1.4)

Qwest currently carries more than four billion minutes of voice traffic per month over our VoIP infrastructure. We will employ this proven service to deliver VOIPTS to Agencies.

Qwest is well positioned to offer Voice Over Internet Protocol Transport Services (VOIPTS) to Federal Agencies using Qwest's commercial OneFlex Voice Termination solution. Qwest's VOIPTS is an Internet Protocol (IP)-based solution that rides on Qwest's National Network System (NNS) and leverages Qwest's worldwide Long Distance (LD) network. The service uses Voice over IP (VoIP) technology but also permits traditional Time Division Multiplexing (TDM) interface through a common gateway architecture.

The VoIP capability of Qwest's VOIPTS provides termination of voice calls over compliant voice telephony solutions via Public Switched Telephone Network (PSTN) connectivity. Qwest's VOIPTS supports PSTN termination to all domestic LATAs [redacted] including both fixed and mobile termination. The system supports on-net terminations that can be to either VoIP-enabled locations or TDM dedicated terminations. This includes combinations of VoIP on-net to on-net and VoIP on-net to off-net.

Qwest has used IP and the Qwest core Multi-Protocol Label Switching (MPLS) network to carry LD voice traffic since 2001. The Qwest network currently carries [redacted] of IP-based voice traffic.

Figure 4.1.3-1 lists the mandatory narrative requirements that are included within Section 4.1.3, *Voice over Internet Protocol Services*.

Figure 4.1.3-1. Table of VOIPTS Narrative Requirements

Req_ ID	RFP Section	Proposal Response
32084	C.2.7.8.1.4 (2)	4.1.3.3.1.1
32089	C.2.7.8.1.4 (3)(d)	4.1.3.3.1.1
32090	C.2.7.8.1.4 (4)(b)	4.1.3.3.1.1
32091	C.2.7.8.1.4 (4)(c)	4.1.3.3.1.1
32092	C.2.7.8.1.4 (4)(d)	4.1.3.3.1.1
32095	C.2.7.8.1.4 (6)	4.1.3.3.1.1
32097	C.2.7.8.1.4 (8)	4.1.3.3.1.1
32100	C.2.7.8.1.4 (11)	4.1.3.3.1.1
32101	C.2.7.8.1.4 (11)	4.1.3.3.1.1
32102	C.2.7.8.1.4 (11)(a)	4.1.3.3.1.1
32103	C.2.7.8.1.4 (11)(b)	4.1.3.3.1.1
32104	C.2.7.8.1.4 (11)(c)	4.1.3.3.1.1

4.1.3.1 Qwest's Technical Approach to VOIPTS Delivery (L.34.1.4.1)

Qwest's VOIPTS approach is based on our well-established, highly reliable and secure fiber optic infrastructure and our adherence to proven engineering practices. Qwest has fine-tuned processes to research, evaluate, engineer, deploy, and operate new VOIPTS features and functionality.

The sections that follow describe our approach to service delivery and how our approach benefits the Government. We will also describe how Qwest VOIPTS will facilitate the Federal Enterprise Architecture (FEA) objectives, how Qwest proposes to address problems that may be encountered in providing VOIPTS, and how our synchronization network architecture supports VOIPTS.

4.1.3.1.1 Approach VOIPTS Delivery (L.34.1.4.1 (a))

The Qwest technical approach to providing a fully compliant VOIPTS is based on Qwest's commercial OneFlex Voice Termination service, an IP-based solution that terminates IP voice traffic to PSTN end users. [redacted] Qwest's VOIPTS can deliver IP call traffic over the Qwest IP/MPLS network to any domestic or non-domestic location via IP or PSTN interconnections. The service supports calls to fixed and mobile PSTN interconnections as well as 8XX (outbound) calls to the PSTN. [redacted]

[redacted]

[redacted]

For VOIPTS, the Agency will connect to the Qwest IP/MPLS network Via Internet Protocol Service (IPS) or Network Based Internet Protocol VPN (NBIP-VPNS). Qwest supports both trunking and access gateways. If the

[redacted]

Agency connects into the Qwest network using various traditional TDM methods including Integrated Serviced Digital Network (ISDN) Primary Rate Interface (PRI), in-band signaling trunk groups, or SS7 trunk groups, then a Service Enabling Devices (SED) will be required to interface to Qwest IP/MPLS network. Qwest can identify Agency/customer groups based on the trunk group of the originating Agency, or in the case of an IP-based service, Qwest utilizes the source IP address to identify the originating Agency. Qwest VNS switched customers are identified using their Automatic Number Identification (ANI). The switched customer accesses the Qwest NNS through a PIC'd call.

Agencies may utilize the private dial plan features provided to our traditional circuit switched customers. These customer locations will have access to Qwest's SCPs for service logic use in the same fashion as the circuit switched customer locations. Agencies may use a private dial plan that the Qwest SCP will translate to either a circuit switched or a VoIP destination. The destinations may be on-net in the form of a dedicated trunk group or a private dial plan that allows numbers to be translated to domestic and non-domestic switched locations. Agencies will have the same flexible control of dial plans for VoIP locations as for circuit switched locations.

Qwest's VNS services allow Agencies to dial off-net locations. The Qwest SCP supports range privileges that provide Agency control of terminations. Agencies may restrict users dialing patterns from dedicated locations by using the dedicated access location or by requiring an authorization code.

Assume that an on-net Agency group is defined by Agency locations 1, 3, and 4 in Figure 4.1.3-4. Locations 1, 2, and 3 will each have unique sets of IP addresses. [redacted] This association is what allows the Qwest SSPs and SCPs to translate dial plans for the specific Agency group. At the time of a call, the SSP will have a trigger based on the Agency's originating location information (typically a trunk group ID). The call attributes will trip the trigger, resulting in a query to the SCP. The

SCP will translate the dialed number according to the Agency group information and return routing information to the SSP. The SSP then routes the call to the appropriate destination regardless of the connectivity type to the terminating point.

Qwest understands the need to support fully qualified domain names as an access identifier and has incorporated this concept as part of Qwest's strategic network plan.

The Qwest VoIP architecture employs the [redacted] Qwest refers to the [redacted] and associated network components as the Next Generation Switch (NGS) network. Qwest utilizes the [redacted] NGS network for VoIP service access as well as TDM gateway functionality. The Qwest NGS provides the connectivity between the Agency VoIP gateway and the PSTN. Qwest's VOIPTS architecture utilizes any of the [redacted] deployed NGS LD switches to terminate the call. The [redacted] redirect functionality is used to route the call to the appropriate terminating gateway. The [redacted] platform uses the Session Initiation Protocol (SIP) source IP address to uniquely define each source of VoIP traffic. To properly bill the Agency, a unique IP address and SIP trunk group per origination is used. Local Number Portability (LNP) will be enabled on the SIP trunk groups to support LNP lookup of national numbers at the point of origination into the Qwest network. Preprocessing and digit manipulation may be required to ensure that both the called and calling numbers are of the proper format.

NGS [redacted] Components

The following deployed NGS components will be utilized:

- [redacted]
- [redacted]

[redacted]

The Agency's VoIP network connects to the Qwest IP/MPLS backbone using IPS and NBIP-VPNS. Qwest's VOIPTS achieves comparable voice quality to the PSTN by using Quality of Service (QoS) techniques to ensure very low VoIP packet loss and industry-standard Coder-Decoders (CODECs). Diffserv, along with packet marking, are used to prioritize VoIP traffic over other data traffic. The IPS and NBIP-VPNS QoS scheme is implemented in the Agency router. The router must have similar functionality enabled for the QoS mechanism to work. The [redacted] gateway and [redacted] router will be used to mark the VoIP packets appropriately. Real-Time Transport Protocol (RTP) packets will be given highest priority followed by signaling.

The VoIP traffic is secured by the use of a SBC that provides firewall functionality between the IPS or NBIP-VPNS edge router and the [redacted] NGS network. The SBC for Qwest VoIP service is the [redacted] Director. The Session Director (SD) is a small form-factor, DC-powered, rack-mountable unit. The SD supports [redacted] multimode fiber gigabit Ethernet interfaces; one for Agency-facing public traffic and one for NGS-facing private traffic. Additional serial and fast Ethernet interfaces are supported for platform management traffic.

The SBC is deployed in redundant pairs in an active-standby configuration. The platform supports automated failover while maintaining stable calls. The platform uses a virtual IP address mechanism. The IP addresses are transferred to the standby platform in the event of a failover. ***Figure 4.1.3-5*** shows the SBC configuration.

[redacted]

The primary configuration activity on the platform is the mapping of VoIP traffic from public-side IP addresses to private-side addresses. [redacted]

[redacted] For Qwest's VOIPTS, each Agency requires its own public-side and private-side address. The private-side address is used to provision the SIP trunk group in the NGS. [redacted] This can be used to limit the number of calls from that customer based on the size of the port used by the Agency. For example, a DS-3 supports approximately 400 G.711 calls. [redacted] If the Agency wants only a percentage of the link to be used for VoIP, the SBC can be set to limit the number of calls to a number smaller [redacted] The CAC value is configured as part of the Agency [redacted] setup.

[redacted]

[redacted] A typical call flow for SIP-based traffic in the VOIPTS network is shown in [redacted]

Qwest supports G.711 (a-law and µ-law) and G.729a and G.729ab CODECs. For Agencies sending a mix of compressed and uncompressed calls, the SBC can use this realm concept to identify calls requesting

[redacted]

compression support. The NGS will identify this realm/address as requiring compression-based routing and route the call to the gateway compression card resource. Qwest has deployed compression resources as all NGS gateways.

Qwest's VOIPTS access gateway offers a communications service supporting VoIP traffic exchange with Agency sites providing their own VoIP infrastructure. Qwest engineering will work with the Agency to provide this custom configuration service.

The NNS supports a selection of gateway devices that can be used to terminate as:

Access Gateway – provides 10/100 BaseT Ethernet interface to an Agency's network.

Trunking Gateway – provides the required analog and digital terminations. Qwest can recommend and/or provide SED devices to permit Agency analog hardware to interface in IP with Qwest's VOIPTS.

PSTN Gateway – the LD-to-VoIP gateways that connect to Qwest's LD network to enable outbound calling.

Qwest extends our VoIP expertise in the areas of dedicated pre-sales engineering, network planning, provisioning, and operations to the VOIPTS offerings through dedicated teams and resources committed to end-to-end service delivery. Network Operations, Field Engineering, 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 Information Technology (IT) to ensure network performance and technology advances in the underlying architecture. Additionally, the Networx Contractor Program Office is the Agency's single point of contact for post-implementation support.

Qwest's sales engineering and network security experts will work with the appropriate Agency staff to create solutions that work within the Agency's security framework. For example, our sales engineering team will work with each Agency to ensure compatibility issues are addressed based on their specific Private Branch Exchange (PBX) or Key System selection. Qwest supports utilizing the Agency Service Delivery Point (SDP) interfaces as the initial baseline specifications for PBX and Key System compatibility.

4.1.3.1.2 Benefits of Qwest's VOIPTS Technical Approach (L.34.1.4.1 (b))

Qwest's VOIPTS is a natural extension of our experience and is fully integrated into Qwest's capabilities of all data transport products. Agencies are not limited just to voice services on their IP network port. The same IPS and NBIP-VPNS port can be used for data traffic in addition to the voice services. For example, an Agency that creates a nationwide private data network based on a NBIP-VPNS can provide VOIPTS over the same access connection—whether it is a dedicated connection or a Layer 2 connection such as ATMS or FRS.

Figure 4.1.3-8 gives a summary of the VOIPTS features and benefits.

Figure 4.1.3-8 Qwest's VOIPTS Features and Benefits

Feature	Benefit	Substantiation
VNS Plan	[redacted]	[redacted]
VOIPTS Protocol and CODEC	[redacted]	[redacted]

Feature	Benefit	Substantiation
Qwest VOIPTS interoperates with a variety of Agency interfaces	[redacted]	[redacted]

In addition to the benefits of the service, Qwest's VOIPTS will also support the Federal Enterprise Architecture and its key objectives, as shown in ***Figure 4.1.3-9***.

Figure 4.1.3-9 Qwest's VOIPTS Support to FEA Objectives

FEA Objectives	Qwest VOIPTS Solutions
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]
Increase cross-Agency and inter-Government collaboration.	[redacted]

4.1.3.1.3 Solutions to VOIPTS Problems (L.34.1.4.1 9 (c))

Qwest has extensive experience in the delivery of VOIPTS services. We apply this experience to ensure the delivery of high-quality VOIPTS to Agencies. Extensive pre-deployment laboratory system and integration testing identifies the majority of problems, and Qwest's proactive network and configuration management/fault management systems and methods are leveraged to quickly resolve unforeseeable operational issues. ***Figure***

4.1.3-10 summarizes some of the key problems we have encountered and the solutions we apply to resolve issues.

Figure 4.1.3-10. Qwest's Approach to Common VOIPTS Delivery Challenges

Problem	[redacted]
Voice quality may be adversely affected by data traffic packets.	[redacted]
Call oversubscription can result in quality problems.	[redacted]
Failure of NGS gateway or SBC causing a major network outage.	[redacted]

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

Time of Day Synchronization (IP Network)

[redacted]

Transport Network Synchronization

[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]

4.1.3.2 Satisfaction of VOIPTS Performance Requirements (L.34.1.4.2)

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

4.1.3.2.1 VOIPTS Quality of Service (L.34.1.4.2 (a))

Qwest's VOIPTS solution will meet Networx performance requirements as defined in RFP Section C.2.7.8.4.1, summarized in ***Figure 4.1.3-13***.

Figure 4.1.3-13 Qwest Compliance with Government VOIPTS 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 [Optional]	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]

Monitoring systems continuously and methodically watch and record the traffic to assist in troubleshooting. QoS test platforms reside in the network and perform proactive tests to validate the network QoS level health. Qwest also supports solutions to test QoS to the Agency location. 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 VOIPTS network is currently deployed in geographically diverse locations to ensure fault tolerance and high availability.

4.1.3.2.2 Approach for Monitoring and Measuring **VOIPTS** *KPIs and AQLs (L.34.1.4.2 (b))*

Qwest monitors and measures the KPIs and AQLs via an automated process that pulls data from the root source, summarizes it, and displays it via Web tools. These Web tools display actual results and indicate via red/green colorizing whether or not goals are met. Our approach is to completely automate displaying results from data collection to Web display so that the focus is on results rather than "report generation." Further, our automated process ensures that business rules are established and there is no chance of manipulating the data.

For Network KPIs, we use [redacted] to display the Network Reliability Scorecard with the KPIs, the objectives, and an indication of whether the objectives are met or missed for each reporting period. The scorecard is our tool to show both upper management and network management the current health of the network. The scorecard is reviewed daily, both at the executive level to ensure the proper attention and focus, and by our network management teams to ensure AQL levels are consistently met.

For all Networx services we use the [redacted] trouble ticketing system. [redacted] is an industry-leading commercial -off-the-shelf trouble management application that 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.

For VOIPTS, all of the AQL/KPI metrics listed in Figure 4.1.3-13 are assessed on an individual site or site-pair basis where applicable. This data is used to ensure that all Agency data network AQLs are systematically being supported by the network. [redacted]

Qwest will ensure the services delivered to Agencies follow a stringent reporting, management, and network capacity strategy to verify that all AQLs are delivered at a consistent acceptable level. Qwest Network Operations Center (NOC) network management systems collect performance data directly from the VOIPTS routers via Simple Network Management Protocol (SNMP). Performance data is collected from the network and SEDs at industry standard [redacted] intervals. The VOIPTS performance data information is distributed to Qwest's NOC, which continuously monitors the performance of the Qwest OC-192 IP MPLS network. VOIPTS utilization is monitored by the Qwest NOC, which is responsible for reporting statistics to [redacted] This information is distributed to internal databases where it will be posted to the Qwest Control Networx Portal. This Portal provides Agencies with performance statistics to verify customer specified AQLs are met.

Based on our past performance on similar programs, we expect actual network performance for VOIPTS [redacted] set for Networx. Our network is designed to minimize the latency between Agency SDP locations. Our current POP density and SDP-to-POP homing design is engineered to achieve under [redacted] of delay between an SDP and its serving POP. In addition, it is our normal network planning process to introduce new access and core POPs as needed to ensure Qwest meets or exceeds the CONUS latency requirements.

[redacted]

Measuring SDP-to-SDP Latency, and the Role of SEDs

All of Qwest's IP-based services - [redacted]

[redacted]

Following standard convention, the SDP is the [redacted] router, as depicted in [redacted] *Qwest SDP-to-SDP Testing Methodology*.

[redacted]

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 General Services Administration (GSA), will monitor, measure, and report the performance of the service for KPI/AQL and for Service Level Agreement (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:

[redacted]

[redacted]

[redacted]

The Use of Government Furnished Property

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

1. Request that the Agency provide SNMP capability to the device for the Qwest NOC
2. Request that the Agency buy a monitoring SED from Qwest
3. Coordinate with the Agency 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 SED 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.

Qwest's solution was originally designed for our commercial offering to be SED-vendor agnostic. Qwest's performance management (PM) architecture is standards-based, scalable, flexible, and network centric, imposing the minimal requirements or load at the SDP level to achieve a rich set of PM metrics. The only major requirement is that the SDP allows ICMP polls from designated Qwest probes. This is nothing more than an Access Control List configuration on the SDP device.

As indicated above, if the device cannot or the Agency does not want to provide responses to ICMP ECHO messages, then an additional SED can be placed at the Agency location to enable the necessary data measurements to generate the required KPI and AQL information.

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, then 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 builds our tools to be able to drill down to our individual services and show detailed metrics. Within our scorecards, we show dozens of metrics with results over several years for each service to give a complete picture of performance over time. The metrics incorporate Agency-facing results including provisioning intervals and percent commitments met, average speed of answer and call volumes, trouble ticket mean time to resolve and percent commitments met, and Agency transaction survey results. On the network side, we track metrics such as network availability, network reliability, and defects per million (for switched networks).

[redacted] is an example of a service metrics scorecard displaying a few key metrics and results. With this scorecard, Qwest is able to see on a daily basis whether results are within objective. Our scorecards are reviewed daily at the executive level to ensure the proper attention and focus. Qwest scorecards are also viewed by all levels of management so that first level supervisors as well as upper level management are viewing the same results and responding on the same issues.

[redacted]

Additionally, we produce fully automated online trend and Pareto Charts on the scorecard metrics to enable prompt identification of trends. We review these trends and ensure potential performance issues have been investigated and resolved.

4.1.3.2.3 VOIPTS Performance Improvements (L.34.1.4.2 (c))

[redacted] Qwest will meet all required KPIs and AQLs for VOIPTS. In the event that 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 a VOIPTS solution to serve unique Agency needs. Qwest is able to leverage our vast VOIPTS product portfolio, which includes a variety of SED providers and specific VOIPTS solutions. Through a special combination of vendor solutions and talented engineering capabilities, Qwest will be able to serve an Agency's business needs.

4.1.3.2.4 Additional VOIPTS Performance Metrics (L.34.1.4.2 (d))

[redacted]

4.1.3.3 Satisfaction of VOIPTS Specifications (L.34.1.4.3)

Based on our existing Qwest OneFlex Integrated Access VoIP service, the Qwest VOIPTS meets all Networx specifications.

4.1.3.3.1 Satisfaction of VOIPTS Requirements (L.34.1.4.3 (a))

The following three sections describe how Qwest will satisfy the capabilities, features, and interfaces requirements of the RFP.

4.1.3.3.1.1 Satisfaction of VOIPTS Capabilities Requirements (L.34.1.4.3(a), C.2.7.8.1.1.4)

Figure 4.1.3-17 summarizes Qwest's technical approach to delivering the VOIPTS capabilities in RFP Section C.2.7.8.1.4. Qwest fully complies with all mandatory stipulated and narrative capabilities requirements for VOIPTS. The text in Figure 4.1.3-17 provides the technical description required per L.34.1.4.3(a) and does not limit or caveat Qwest's compliance in any way.

Figure 4.1.3-17. Qwest's Technical Approach to VOIPTS Capabilities

ID #	Capability	[redacted]
1	Establish & Receive Calls On-Net; Originate Calls to Off-Net	[redacted]
2	Routing Prioritization or Class of Service (CoS)	[redacted]
3	Minimum VOIPTS Capabilities	[redacted]

ID #	Capability	[redacted]
4	VOIPTS Gateway	[redacted]
5	Alternate Routing to PSTN	[redacted]
6	Traverse and Interoperate with Agency Firewalls	[redacted]
7	Provide Secure Website for Performance and Reports	[redacted]
8	Minimum & Optimal for Agency Equipment	[redacted]
9	Minimum Quality Level	[redacted]
10	Call Routing Between PSTN and IP	[redacted]
11	Security Practices and Safeguards	[redacted]

Class of Service Support (Req_ID 32084; C.2.7.8.1.4(2))

Qwest distinguishes between real-time VoIP packets and non-real time services using ToS settings in the IP packet header. As the data is transmitted through the Qwest backbone, this ToS setting is mapped into an MPLS QoS marking to maintain priority. Qwest assigns VoIP traffic a premium flag and maps this ToS indicator into the appropriate MPLS queue setting for transport, based upon Agency requirements.

For MPLS transport, [redacted] based on Differentiated Services Code Points and IP Precedence bits. Qwest also employs Class-Based Weighted Fair Queuing techniques. Qwest CoS levels will support the Government's CoS naming function as defined by:

[redacted]

Support of Agency Dial Plans (Req_ID 32089; C.2.7.8.1.4(3)(d))

Qwest will interface with the Agency to ensure interoperability with dial plans. Qwest will provide a Private Dial Plan (PDP) for Agency's on-net calling. Qwest utilizes our Virtual Network Service logic as part of our AIN-based services to translate and appropriately route on-net dialing plans. The on-net customers are assured a closed user group dialing plan that prevents other Qwest customers from utilizing the Agency's PDP. The Agency PDP is enabled by the number-to-address translations performed in the [redacted] (combined policy server and gateway).

Support of Access Gateways (Req_ID 32090; C.2.7.8.1.4(4)(b))

Qwest provides access gateways using the Qwest IPS and NBIP-VPNS. This platform will interface with the Agency's Local WAN connection. The IP/MPLS platform will support Ethernet UNI ports to connect with the Agency equipment. These gateways employ standard VoIP signaling and RTP to provide access to and from Agency resources. Qwest provides access through the use of an SBC that acts as a trunking interface to the Agency. The SBC facilitates a secure traffic handoff between the Agency network and Qwest. PSTN gateways are provided via Qwest NGS infrastructure for access to the PSTN.

Support of Trunking Gateways (Req_ID 32091; C.2.7.8.1.4(4)(c))

For VOIPTS, the Agency will connect to the Qwest IP/MPLS network via IPS or NBIP-VPNS. Qwest supports trunking gateways and can identify Agency/customer groups based on the trunk group of the originating Agency, or in the case of an IP based service, Qwest utilizes the source IP address to identify the originating Agency. Qwest VNS switched customers are identified using their ANI. The switched customer accesses the Qwest NNS through a PIC'd call.

The NNS supports a selection of gateway devices that can be used to terminate as trunking gateways that provide the required analog and digital terminations. Qwest can recommend and/or provide SED devices to permit Agency analog hardware to interface in IP with Qwest's VOIPTS.

Support of PSTN Gateways (Req_ID 32092; C.2.7.8.1.4(4)(d))

For VOIPTS, the Agency will connect to the Qwest IP/MPLS network Via IPS or NBIP-VPNS. Qwest supports PSTN gateways, LD to VoIP gateways that connect Agency VoIP traffic to Qwest's LD network. If the Agency connects to the Qwest network using various traditional TDM methods including ISDN PRI, in-band signaling trunk groups, or SS7 trunk groups, then a SED will be required to interface to the Qwest IP/MPLS network. Qwest can identify Agency/customer groups based on the trunk group of the originating Agency, or in the case of an IP based service, Qwest utilizes the source IP address to identify the originating Agency. Qwest VNS switched customers are identified using their ANI. The switched customer accesses the Qwest NNS through a PIC'd call.

Agency Firewall Compatibility (Req_ID 32095; C.2.7.8.1.4(6))

Qwest will verify that Agency firewall resources are compatible as part of the engineering requirements analysis and solution design process. Interoperability testing will be run to ensure compatibility with the Agency equipment.

Agency Equipment Compatibility (Req_ID 32097; C.2.7.8.1.4(8))

Qwest will provide guidance on Agency-owned voice equipment to meet the necessary minimal and optimal equipment requirements for compatibility and interoperability. Testing will be done to ensure interoperability with the Agency equipment. Signaling type requirements to interoperate with the Qwest VOIPTS platform are shown in ***Figure 4.1.3-18****.*

Figure 4.1.3-18. Qwest's Minimum and Optimal VOIPTS Equipment Requirements

Requirement	Description
VoIP signaling	[redacted]
SIP Signaling	[redacted]
[redacted]	[redacted]
Other Signaling Requirements	[redacted]

Requirement	Description
VoIP Audio Encoding	[redacted]

Security Practices- Implementation (Req_ID 32100; C.2.7.8.1.4(11)

Qwest will enforce current best security practices within our network as well as provide guidance to Agencies as necessary. Qwest's VOIPTS complies with all industry best practices for security and safeguards to minimize susceptibility to security issues and prevent unauthorized access.

[redacted]

[redacted]

Security Practices – Updates (Req_ID 32101; C.2.7.8.1.4(11))

Qwest will ensure regular updates and periodic audits, per our current risk management and security practice, to ensure that all necessary safeguards are met. Qwest is constantly evaluating new network threats, and we work in conjunction with our equipment vendors and IT organization to implement patches and software upgrades to ensure that the VOIPTS network has the latest security measure in place. [redacted]

Security Practices – Denial of Service (Req_ID 32102; C.2.7.8.1.4(11)(a))

Qwest's Denial of Service (DoS) detection is provided via several levels of security initiatives. Our customer/peer notification based DDoS detection system, [redacted] monitors and detects DoS/DDoS-type anomalies and traffic routing instabilities. We also mitigate the potential for DoS using scrubbing mechanisms including destination/source [redacted] and extended ACLs that selectively block protocols and IP addresses. Qwest has defined policies and procedures for prevention and uses IP spoofing prevention techniques [redacted]

Security Practices – Intrusion (Req_ID 32103; C.2.7.8.1.4(11)(b))

Qwest's approach is that the security of both control and data planes is critical. Qwest provides safeguards from VOIPTS intrusion by utilizing both network layer access controls as well as end-user activation to ensure only valid, subscribed VoIP endpoints can access the VOIPTS service. [redacted] Traffic between NGS sites is allowed, but no external source is allowed to send traffic directly to an NGS. Any external traffic destined for the NGS network must traverse an SBC.

Security Practices – Invasion of Privacy (Req_ID 32104; C.2.7.8.1.4(11)(c))

The combination of physical security, operational procedures, and logical separation of services ensures the privacy of VOIPTS traffic. Qwest ensures the privacy of customer VOIPTS 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 that the VOIPTS can not be intercepted or that unauthorized third parties cannot eavesdrop on the packet payloads through the use of encryption and message authentication.

Only registered subscribers of Qwest's VOIPTS service can access the network. Numerous safeguards, including gateway router access control, prevent unauthorized users from illegitimately using the system. The Qwest VOIPTS SBCs provide firewall and NAT functions to ensure that Qwest VoIP calls are totally secure and private and that eavesdropping interceptions are minimized.

Allowing direct IP access from external, non-Qwest managed sources to the NGS platforms creates a number of security, QoS, and fraud risks. The

[redacted]

SBC provides the interface to these external traffic sources and mitigates the security, QoS, and fraud risks. [redacted] The SBC becomes a trusted traffic source. [redacted] shows the NGS security concept.

4.1.3.3.1.2 Satisfaction of VOIPTS Feature Requirements (L.34.1.4.2(a); C.2.7.8.2)

Pursuant to RFP Section C.2.7.8.2, there are no VOIPTS feature requirements.

4.1.3.3.1.3 Satisfaction of VOIPTS Interface Requirements (L.34.1.4.2(a); C.2.7.8.3)

Figure 4.1.3-20 summarizes the interfaces supported by Qwest's VOIPTS. Qwest's NNS interfaces to existing Agency analog equipment using

TDM-based interfaces. Qwest has proposed SED equipment to interface to non-IP based Agency equipment in order to meet VOIPTS interface specifications. Qwest may substitute compliant tested and certified alternative SEDs with similar functional and performance capabilities over the course of the program. Qwest fully complies with all mandatory stipulated and narrative capabilities requirements for VOIPTS. The text in Figure 4.1.3-20 provides the technical description required per L.34.1.4.2(a) and does not limit or caveat Qwest's compliance in any way.

Figure 4.1.3-20. Qwest-Provided VOIPTS Interfaces at the SDP

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Signaling or Protocol	[redacted]
1	Ethernet port: RJ-45 (Std: IEEE 802.3)	Up to 100Mbps	SIP and H.323 are supported today. Media Gateway Control Protocol (MGCP) will be added when commercially available.	[redacted]
2	Analog Trunk: Two-Wire (Std: Telcordia SR-TSV-002275)	4kHz Bandwidth	Loop Signaling (loop start and ground start)	[redacted]
3	Analog Trunk: Four-Wire (Std: Telcordia SR-TSV-002275)	4kHz Bandwidth	E&M Wink Start Signaling	[redacted]
4	Digital Trunk: T1 TSV-002275 and ANSI T1.102/1 07/403)	Std: Telcordia SR Signaling Up to 1.536Mbps	T1 Robbed-Bit	[redacted]
5	Digital Trunk: ISDN PRI T Reference Point (Std: ANSI T1.607 and 610)	Up to 1.536Mbps	ITU-TSS Q.931	[redacted]
6. OCONUS/ non-domestic [Optiona]	Digital Trunk: E1 Channelized (Std: ITU-TSS G.702)	Up to 1.92Mbps	SS7, E1 Signaling	[redacted]

4.1.3.3.2 Proposed Enhancements to VOIPTS (L.34.1.4.3 (b))

4.1.3.3.2.1 Voice over IP Telephony Service _Session Initiation Protocol service (VOIPTS_SIP)

CenturyLink's Voice over IP Telephony Service_Sesson Initiation Protocol service (VOIPTS_SIP) provides IP transport and voice services [redacted] The voice service will be delivered with SIP functionality [redacted] In addition, VoIPTS_SIP includes the origination and termination of local voice, dedicated long-distance, domestic and international toll-free service and Enhanced V911 traffic. VoIPTS_SIP Trunk also offers inbound Remote DID capability for customers wishing to offer local numbers for their customers to call in remote rate centers, the calling traffic can be aggregated in SIP format back to those customers. (Remote DID numbers are for inbound use only.)

[redacted]

VoIPTS_SIP Features

- Unlimited local service
- Usage based Long distance
- Emergency 911 dialing
- Domestic and International Inbound Toll Free service
- Switch diversity
- Self service portal
- Local Number Portability

- Caller ID
- Remote DID
- SIP REFER
- Dedicated VoIP Interconnect

4.1.3.3.2.2 CenturyLink Technical Approach

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

4.1.3.3.2.3 CenturyLink VoIPTS SIP Service

CenturyLink's VoIPTS SIP_will comprise of the following service elements listed in Table 4.1.3.3.2.3-1, with add on features listed in Table 4.1.3.3.4-1

4.1.3.3.2.3.1 Flat Local Session CLIN 232120:

[redacted]

Table 4.1.3.3.2.3-1 CenturyLink VoIPTS SIP Service

NRC CLIN	MRC CLIN	Usage	Description	Charging Unit
N/A	232120	N/A	Flat Local Session	PER CALL

4.1.3.3.2.4. VoIPTS SIP Features

4.1.3.3.2.4.1 VoIP SIP Installation CLIN 232121

A service instance is a trunk group location. [redacted]

4.1.3.3.2.4.2 Telephone Number (TN) Fee MRC CLIN 232122 and NRC CLIN 232123

VoIPTS Telephone Number Setup (NRC) and Telephone Number MRC

4.1.3.3.2.4.3 Telephone Number (TN) Porting CLIN 232124

4.1.3.3.2.4.4 Remote Direct Inward Dial (RDID) Telephone Number (TN) MRC CLIN 232125 and NRC CLIN 232126

[redacted]

[redacted]

[redacted]

4.1.3.3.2.4.5 Remote Direct Inward Dial (RDID) Porting CLIN 232127

4.1.3.3.2.4.6 Business Blue Page Listing CLIN 232128

[redacted]

[redacted]

4.1.3.3.2.4.7 IP Diversity Set-Up CLIN 232129

[redacted]

4.1.3.3.2.4.8 8XX Service CLIN 232130

[redacted]

4.1.3.3.2.4.9 Dedicated VoIP Interconnect MRC CLIN 232131 and NRC CLIN 232132

[redacted]

4.1.3.3.2.4.10 SIP REFER MRC CLIN 232133 and NRC CLIN 232134

[redacted]

4.1.3.3.2.4.11 VoIP Switch Diversity MRC CLIN 232135 and NRC CLIN 232136:

[redacted]

4.1.3.3.2.4.12 Remote Direct Inward Dial (RDID) CLIN 232137

[redacted]

[redacted]

Table 4.1.3.3.4-1 CenturyLink VoIPTS SIP Features

NRC CLIN	MRC CLIN	Usage	Description	Charging Unit

NRC CLIN	MRC CLIN	Usage	Description	Charging Unit
232121	N/A	N/A	VoIP_SIP Installation	PER LOCATION
N/A	232122	N/A	TN Fee	PER NUMBER
232123	N/A	N/A	TN Fee	PER NUMBER
232124	N/A	N/A	TN Porting	PER NUMBER
N/A	232125	N/A	Remote Direct Inward Dial TN	PER NUMBER
232126	N/A	N/A	Remote Direct Inward Dial TN	PER NUMBER
232127	N/A	N/A	RDID Porting	PER NUMBER
N/A	232128	N/A	Business Blue Page Listing	SUBSCRIPTION
232129	N/A	N/A	IP Diversity Set Up	PER INSTANCE
232130	N/A	N/A	8XX Service	PER INSTANCE
N/A	232131	N/A	Dedicated VoIP Interconnect	PER SOLUTION
232132	N/A	N/A	Dedicated VoIP Interconnect	PER SOLUTION
N/A	232133	N/A	SIP REFER	PER INSTANCE
232134	N/A	N/A	SIP REFER	PER LOCATION
N/A	232135	N/A	VoIP Switch Diversity	PER INSTANCE
232136	N/A	N/A	VoIP Switch Diversity	PER INSTANCE
N/A	N/A	232137	Remote Direct Inward Dial (RDID)	PER MINUTE

4.1.3.3.3 Network Modifications Required for VOIPTS Delivery (L.34.1.4.3 (c))

Qwest’s VOIPTS offering is based on our fully mature, commercially available OneFlex VoIP Termination product. Qwest does not foresee making any changes to our existing architecture.

4.1.3.3.4 Experience with VOIPTS Delivery (L.34.1.4.3 (d))

Qwest has more than five years of VoIP technology and converged voice environment experience. Qwest has been carrying large portions of our LD traffic over IP (via [redacted] gateways) since 2001. This has enabled Qwest to provide a more reliable LD service to Agencies. Qwest's proven leadership in voice and emerging voice solutions such as VoIP is demonstrated by the following:

- Experience with VoIP since 2001 and currently running more than four billion minutes per month on our VoIP platform
- Deployment and comprehensive management of nationwide IP/PSTN gateways
- Proven provider for LD service
- Deployment of the OneFlex Voice Termination service commercially in July of 2004. The service currently [redacted] carries traffic in excess of [redacted] minutes of use per day.
- [redacted]

4.1.3.4 Robust Delivery of VOIPTS (L.34.1.4.4)

The following sections discuss Qwest's approach to support Government VOIPTS traffic and Qwest's approach to engineering network design for VOIPTS.

4.1.3.4.1 Support for Government VOIPTS Traffic (L.34.1.4.4 (a))

Qwest has analyzed the voice traffic requirement of the Government's traffic model and has determined that it represents an [redacted] incremental increase to the Qwest voice network. Capacity planning for Qwest's VOIPTS solution is based on a threshold [redacted] utilization rate. Qwest does not currently forecast any build-out based on the traffic model. Ongoing traffic analysis and capacity planning will be conducted to ensure that the network is expanded as needed to support Networx traffic growth.

4.1.3.4.2 VOIPTS Congestion and Flow Control Strategies (L.34.1.4.4 (b))

Qwest has tremendous backbone bandwidth based on our implementation of Dense Wavelength Division Multiplexing (DWDM) and aggressive capacity planning to ensure no congestion in our data and voice services networks. Qwest data networks have significant POP redundancy, including multiple redundant core MPLS routers, access routers, route diverse wavelength, and SONET access to multiple other POPs. Our Next Generation Switch (our VoIP platform) has redundant control servers and VoIP-to-PSTN gateways. Our network planning engineers examine all failure modes and design network capacity and switch or router redundancy to ensure performance during failures. While Qwest engineers our network to handle congestion, our primary approach to maintaining service quality is to plan, engineer, and operate the network to avoid congestion and single points of failure.

Network resiliency is also built into our data network services. For example, even though our flagship network uses 10 Gbps unprotected wavelength links to connect our private MPLS core routers, our engineering and use of technology ensures no single-point-of-failure or service degradation in the event of failures. For example, Qwest's MPLS fast-forwarding core design uses MPLS fast re-route, which provides pre-provisioned multi-path healing for all Qwest IP services to ensure 50 to 100 ms range service restoration even in the event of catastrophic backbone circuit or router failure.

The Qwest IP backbone is already MPLS-enabled and runs resource reservation protocol. This provides a solid foundation upon which to build end-to-end bandwidth management. This approach to traffic engineering allows sets of bandwidth-guaranteed label-switched paths to carry different classes of traffic—meaning our core will ensure that our VoIP and MPLS VPN traffic is prioritized over Internet-type service—further ensuring the ability to handle both predicted traffic loads as well as increased loads due to unexpected events such as trunk or router failures.

To ensure high availability of our VOIPTS, Qwest employs redundant port cards, line cards, control processors, SBCs, and switching fabrics in our carrier class equipment. This redundant and reliable equipment is then replicated either locally or in a geographically diverse location. In the event of a loss of a single router, SBC, or switch (combined with our rigorous capacity planning methodology), an Agency will not only see continued service, but also will experience no degradation of service.

Qwest VoIP networks are built with significant extra capacity to allow for bursting and to absorb changes in traffic patterns when failure conditions exist. Qwest also adopts a stringent capacity-planning methodology to ensure there is enough room in the backbone network to accommodate traffic surges in the event of micro bursts, DoS attacks, or link failures. By rigorously following such capacity-planning rules, we ensure that the Qwest backbone network will maintain service quality for Agencies.

4.1.3.4.3 VOIPTS Measures and Engineering Practices (L.34.1.4.4 (c))

Qwest's VOIPTS approach to the architecture is designed such that scaling can occur in a seamless manner and not impact existing systems. Capacity planning is ongoing to ensure growth is addressed to meet Agency demand.

The Qwest approach is modular, consisting of discreet components to provide the Feature Server, SBC, and Gateway services. Each one of these modules can be expanded or supplemented based on growth demands.

Qwest utilizes key trending and utilization thresholds to determine load and scaling of the Feature Servers. Qwest will proactively monitor the subscriber load and will add additional servers once the threshold [redacted] is reached. The same logic applies to the SBCs and the Gateways.

Access capacity is defined as the available capacity between our edge aggregation devices and the core backbone devices. Edge aggregation devices are those devices that directly terminate customer circuits. Core backbone devices are those devices that provide the backbone (long-haul) connectivity between Core High-Speed Backbone POPs (TeraPOPs). To ensure redundancy, [redacted] Usage statistics are gathered on every edge aggregation circuit, and reports are generated using these samples for review on a weekly basis. Any edge aggregation circuit with usage [redacted] is flagged for possible upgrade. KPIs are measured based upon 100 percent of usage data. [redacted] Capacity upgrades are typically completed within 30 days of action being initiated. [redacted] This ensures that edge aggregation device access is redundant and access is not impacted in the event of a failure on one of the uplinks.

Backbone capacity is defined as the available capacity from the core backbone devices between TeraPOPs. Every TeraPOP is connected via multiple backbone circuits (mostly OC-192s and OC-48s) to a minimum of three other TeraPOPs over diverse physical facilities provided by the Qwest state-of-the-art nationwide DWDM wavelength network and self-healing SONET backbone. Usage reports are gathered for all backbone circuits (defined as those circuits that interconnect core backbone devices) just as they are for the edge aggregation circuits. [redacted] Such modeling helps predict traffic utilization patterns due to abnormal network conditions. For example, we use the model to predict how failures, such as a failed backbone circuit, affect traffic utilization on the backbone circuits now burdened with the traffic from the failed circuit. [redacted]

Network growth drivers are typically categorized into the following types: customer driven, trended growth, cost savings, and network preservation.

Qwest capacity planning and network teams are dedicated to growing and improving efficiency of the overall Qwest networks to achieve customer driven demands. The Qwest capacity planning and network teams work closely with our sales teams and customers to recommend new builds that meet customer-specific needs. In addition, Qwest's centralized engineering team applies a consistent capacity management model to all data services.

Qwest proactively monitors overall network utilization statistics to develop trended growth patterns. This trend data acts as one of the key factors to trigger new deployments.

Qwest planning and operations teams look at existing configurations and perform studies on how to gain cost savings and network preservation. Examples of this are building to a new end office to reduce dependence upon long local access circuits, which can mean additional cost burdens, or replacing existing equipment with newer technology to increase network bandwidth utilization and resiliency.

Qwest has evolved our network to support a host of traditional and emerging voice services including Toll Free Services, VoIP, and IP telephony services. Over the history of the Qwest network, we have developed tracking mechanisms for monitoring and tracking network performance. The data from the monitoring systems are used to feed planning and engineering organizations with essential data for traffic modeling and network planning.

To ensure reliability, Qwest has chosen vendor platforms that meet high availability schemes. 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 our customers with a network that has a general [redacted] percent reliability. Furthermore, the interior of the Qwest network contains comprehensively meshed backbone circuits between TeraPOPs to ensure that calls will always have a minimum of two paths by which to pass from an originating SSP to a terminating SSP. Connectivity to the Agency premise can be done via diverse paths in some cases, where facilities are available and the customer has specific requirements and agreements.

SS7 signaling is done via a robust network. All links are engineered [redacted] to ensure safe failover to the fully redundant link mate. All of the SS7 systems are fully redundant in addition to being geographically redundant. Voice traffic and signaling traffic is carried over SONET rings for secured transport.

Qwest continuously investigates possible measures and engineering practices to enhance the robustness, resiliency, and growth potential of our network. This is especially true for emerging services such as VOIPTS. [redacted]

4.1.3.5 VOIPTS 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.

4.1.3.5.1 Optimizing the Engineering of VOIPTS (L.34.1.4.5 (a))

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

[redacted]

[redacted]

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

Best-in-class vendors, extensive interoperability testing, and strategic innovative design form the basis of the optimization of the Qwest VOIPTS network. Qwest's Technology Management Group is responsible for the overall network design. This team is constantly evaluating new hardware and software to improve the overall efficiency and capacity of the Qwest network. Some implementation specifics are addressed below. High availability is addressed via redundancy at multiple levels:

[redacted]

4.1.3.5.3 Access Optimization for VOIPTS (L.34.1.4.5 (c))

Convergence of edge technologies is progressing rapidly as customers strive to support applications over a single facility type. Qwest is focused on providing access facilities that meet this need through IPS and NBIP-VPNS.

[redacted]

[redacted]

In addition to QoS, the network must recognize individual applications within the IP stream. [redacted] SBCs are used to provide this application level control.

Qwest further provides access to traditional telephony applications through the Agency's multi-service connection. Qwest's VoIP and TDM networks are interconnected through distributed [redacted] gateways across the United States. Qwest's VOIPTS has access to these gateways and their services through the dedicated Internet access connection.

4.1.3.5.4 Vision for Service Internetworking (L.34.1.4.5 (d))

Qwest makes it possible for Agencies to 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. [redacted] Qwest will continue to leverage our approach of an extremely high-availability and high-capacity core MPLS network.

[redacted]

Qwest's commitment to VoIP and our interoperability with the PSTN is solid. On the voice services side, Qwest is a leader with our deployment of VoIP services. The Qwest voice infrastructure supports traditional voice services over a PSTN Inter-exchange Carrier network, toll-free service, VoIP, and IP telephony services.

In addition to Qwest's established IP/MPLS architecture, Qwest's network vision continues to evolve. Qwest is actively working in the Alliance for Telecommunications Industry Solutions (ATIS) standards forums on next-generation converging platforms for Fixed-Mobile Convergence and the IP Multi-Media System (IMS) architecture. Qwest holds the Technology and Operations chair position in ATIS, an ANSI accredited standards organization. Furthermore, Qwest is actively working with best-in-class vendors, both nationally and internationally, to provide the best-performing, lowest-cost solutions to support a seamless wireline to wireless converged service architecture, as well as optimal bridge solutions between legacy and next generation services.

Qwest is an active participant in the standards forums to define key interoperability control points. Qwest is actively putting in place legacy network interfaces to fully enable the next generation IMS architecture. This transition network solution will enable a seamless wireline-to-wireless convergence across the multiple access infrastructure elements utilizing a common control plane. It bridges existing services with next generation Internet-enabled Web-centric services in a seamless fashion.