4.1.10 VOICE OVER INTERNET PROTOCOL SERVICES (L.34.1.4)

Qwest currently carries over 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 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 Local Access and Transport Areas and [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 long distance voice traffic since 2001. The Qwest network currently carries more than 4 billion minutes a month of IP-based voice traffic.

Figure 4.1.10-1 lists the mandatory narrative requirements that are included within section 4.1.10, Voice over Internet Protocol Services.

Figure 4.1.10-1. Table of VOIPTS Narrative Requirements

REQ _ ID	RFP Section	RFP Requirement	Proposal Response
5492	C.2.7.8.1 .4 (2)	The following Voice over Internet Protocol Transport Service capabilities are mandatory: 2. The contractor shall enable a routing prioritization scheme or class of service to distinguish between IP services.	4.1.10.3.1.1
5486	C.2.7.8.1 .4 (3)(d)	The following Voice over Internet Protocol Transport Service capabilities are mandatory: 3. The contractor shall provide the following minimum capabilities: d. The contractor's VOIPTS shall interoperate with private Agency network dial plans.	4.1.10.3.1.1
5485	C.2.7.8.1 .4 (4)(a)	The following Voice over Internet Protocol Transport Service capabilities are mandatory: 4. The contractor shall provide gateways for interoperability with the contractors VOIPTS and the PSTN, or Agency User-to-Network Interfaces (UNIs).	4.1.10.3.1.1
5479	C.2.7.8.1 .4 (6)	The following Voice over Internet Protocol Transport Service capabilities are mandatory: 6. The contractor shall verify with the Agency that the Agency firewall is compat ble with this service.	4.1.10.3.1.1
5477	C.2.7.8.1 .4 (8)	The following Voice over Internet Protocol Transport Service capabilities are mandatory: 8. The contractor shall state the minimum and optimal requirements for Agency owned voice equipment (such as PBX's or other voice systems) to be compat ble and interoperate with the contractor's VOIPTS.	4.1.10.3.1.1
5474	C.2.7.8.1 .4 (11)	The following Voice over Internet Protocol Transport Service capabilities are mandatory: 11. The contractor shall ensure security practices and safeguards are provided to minimize suscept bility to security issues and prevent unauthorized access.	4.1.10.3.1.1
5473	C.2.7.8.1 .4 (11)	The following Voice over Internet Protocol Transport Service capabilities are mandatory: 11. The contractor shall ensure security practices and policies are updated and audited regularly.	4.1.10.3.1.1
5472	C.2.7.8.1 .4 (11)(a)	The following Voice over Internet Protocol Transport Service capabilities are mandatory: a. Denial of service - The contractor shall provide safeguards to prevent hackers, worms, or viruses from denying legitimate VOIPTS users and subscribers from accessing VOIPTS.	4.1.10.3.1.1
5471	C.2.7.8.1 .4 (11)(b)	The following Voice over Internet Protocol Transport Service capabilities are mandatory: b. Intrusion - The contractor shall provide safeguards to mitigate attempts to illegitimately use VOIPTS service.	4.1.10.3.1.1
5470	C.2.7.8.1 .4 (11)(c)	The following Voice over Internet Protocol Transport Service capabilities are mandatory: c. Invasion of Privacy - The contractor shall ensure VOIPTS is private and that unauthorized third parties cannot eavesdrop or intercept VOIPTS communications.	4.1.10.3.1.1
7794	C.2.7.8.3 .2 (1)	Voice Over Internet Protocol Transport Service Interfaces: The UNIs at the SDP as defined in Section C.2.7.8.3.2 are mandatory unless indicated otherwise. UNI Type 1; Interface Type: Ethernet port: RJ-45 (Std: IEEE 802.3); Payload Data Rate or Bandwidth: Up to 100 Mbps; Signaling Type: Session Initiation Protocol (SIP), H.323, Media Gateway Control Protocol (MGCP)	4.1.10.3.1.3 Figure 4.1.10-10

4.1.10.1 Qwest's Technical Approach to VOIPTS (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.

4.1.10.1.1 Approach to 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, an IP-based solution that terminates IP voice traffic to the 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]

[redacted]

For VOIPTS, the Agency will connect to the Qwest IP/MPLS network Via Internet Protocol Service (IPS) or Network Based Internet Protocol VPN Service (NBIP-VPNS). Qwest supports both trunking and access gateways. If the Agency connects into the Qwest network using various traditional TDM methods including ISDN Primary Rate Interface (PRI), in-band signaling trunk groups, or SS7 trunk groups, then a Service Enabling Device (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. In the case of an IP-based service, Qwest utilizes the source IP address to identify the originating Agency. Qwest Virtual Network Services (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 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 [redacted] Locations 1, 2, and 3 will each have unique sets

of IP addresses. [redacted] 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's 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

[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 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 the highest priority followed by signaling.

The VoIP traffic is secured by the use of a Session Border Controller (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]. The Session Director (SD) is a small form factor, DC powered, rack mountable unit. The SD supports two 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. [redacted] shows the SBC configuration.

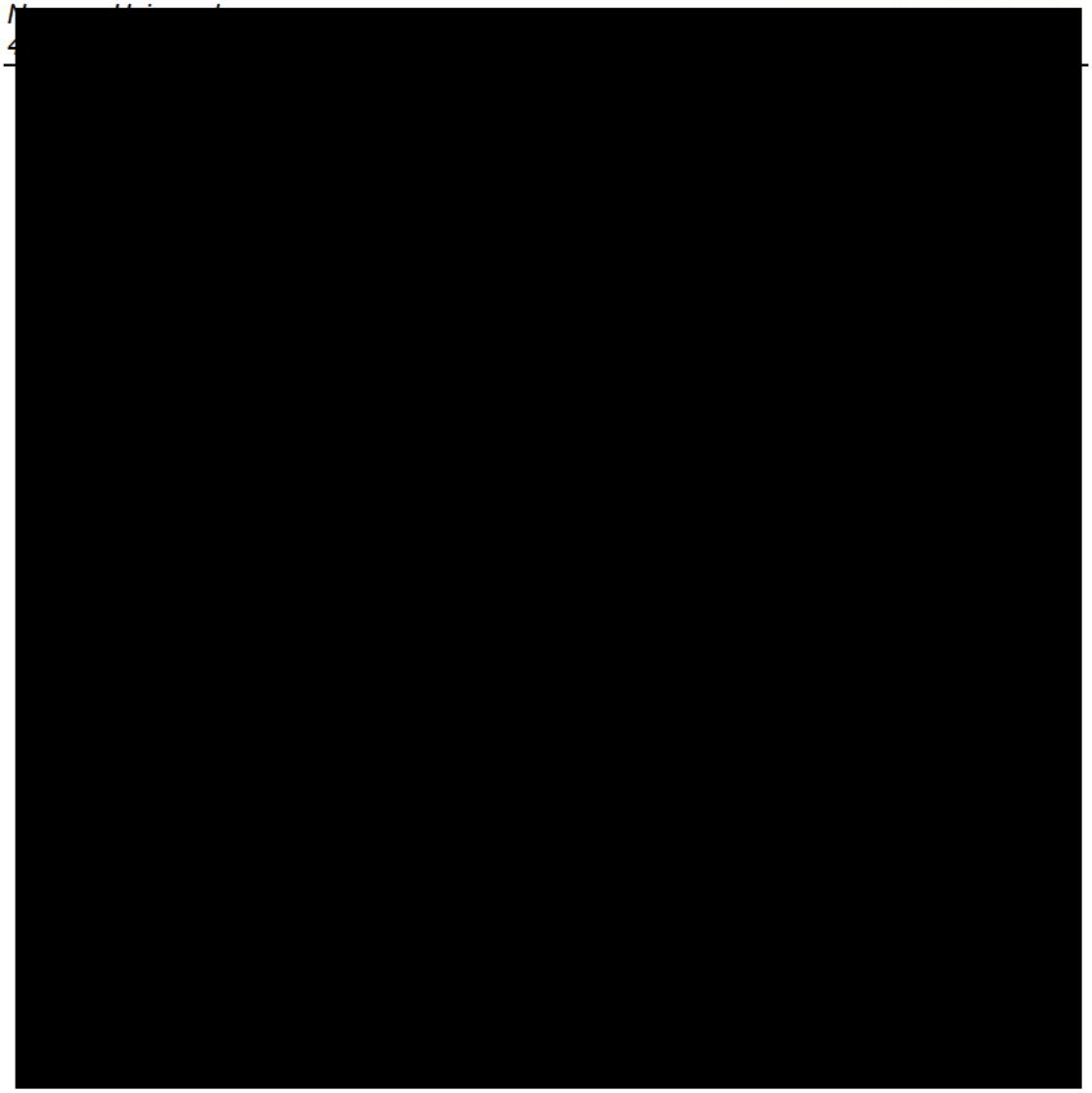
The primary configuration activity on the platform is the mapping of VoIP traffic from public side IP addresses to private side addresses. [redacted] For Qwest's VOIPTS, each Agency requires its own public

[redacted]

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 than [redacted] The CAC value is configured as part of the Agency [redacted] setup.

Qwest's VOIPTS is configured to support both SIP and H.323 protocol. The SBC's H.323-to-SIP interworking function will be used to support an H.323 signaling interface for VOIPTS. A typical call flow for SIP based traffic in the VOIPTS network is shown in [redacted]

[redacted]



Qwest supports G.711 (a-law and μ-law), 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 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 BT Ethernet interface to an Agency's network (shown in Figure 4.1.10-4 in a typical configuration with an Agency firewall and router)

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 that enable outbound calling

Qwest extends its 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 IT to ensure network performance and technology advances in the underlying architecture. Additionally, the Qwest Networx Contractor Program Office is the Government Agency's single point of contact for post-implementation support.

Qwest sales engineering and our 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.

4.1.10.1.2 Benefits of VOIPTS Technical Approach (L.34.1.4.1(b))

Qwest's VOIPTS is a natural extension of our capabilities and experience and is fully integrated into the capabilities of all Qwest's 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 Asynchronous Transfer Mode (ATM) or Frame Relay Service.

Figure 4.1.10-8 gives a summary of the VOIPTS features and benefits.

Figure 4.1.10-8 Qwest's VOIPTS Features and Benefits

Feature	Benefit	Substantiation
VNS Plan	Qwest plan supports a range of privileges that provide customer control of end users including dialing restrictions and security password access	This feature is commercially available today in Qwest's NNS, enabling customers to utilize on-net capabilities.
VOIPTS Protocol and CODEC	Qwest supports both SIP and H.323 as well as G.711 and G.729 CODECs. The VOIPTS service will support traffic steams of mixed CODECs.	This feature is tested, proven and commercially available today in Qwest's VOIPTS network, providing more than the minimum required functionality for Networx.
Qwest VOIPTS interoperates with variety of Agency interfaces	Qwest VOIPTS will interoperate with Ethernet, Analog Trunk (2/4 wire), Digital Trunk (T1, ISDN and E1), IP PBX	All of these interfaces will interoperate with the VOIPTS service [redacted]. Qwest has already deployed this hardware for its commercial VoIP service. [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 4.1.10-9***.

Figure 4.1.10-9 Qwest's VOIPTS Support to FEA Objectives

FEA Objectives	Qwest VOIPTS Solutions
Improve utilization of government information	• The Qwest VOIPTS solution enables multiple Agency clients to interface across a common network. A common set of

FEA Objectives	Qwest VOIPTS Solutions
resources to focus on core Agency mission and service delivery to citizens by using the FEA.	interfaces and VoIP protocols enables a common interface and infrastructure between Agencies. This facilitates a common VoIP solution for each Agency, eliminating the need for a custom one-off solution for each Agency.
Enhance cost savings and avoidance	• Fully integrated VoIP product suite for on-net calling between Agencies using VOIPTS. • Reduced MAC Costs through a common Qwest Control Networx portal for administrative activities • Leverage existing Key and PBX infrastructure
Increase cross-Agency and inter-government collaboration.	• The VOIPTS Solution provides a common communications platform between Agencies, allowing for cross-Agency and inter-government standardization of VoIP communication

4.1.10.1.3 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 4.1.10-10*** summarizes some of the key problems we have encountered and the solutions we apply to resolve issues.

Figure 4.1.10-10. Qwest's Approach to Common VOIPTS Delivery Challenges

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

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

Time of Day Synchronization (IP Network)

[redacted]

[redacted]

SONET Timing and Synchronization Architecture		

4.1.10.2 Satisfaction of VOIPTS Performance Requirements (L.34.1.4.2)

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

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

Qwest's VOIPTS solution will meet Networx performance requirements defined in RFP Section C.2.7.8.4.1 as summarized in ***Figure 4.1.10-13***.

Figure 4.1.10-13 Qwest Compliance with Government VOIPTS Performance Metrics

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

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 path 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.

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

Qwest monitors and measures the Key Performance Indicators (KPIs) and Acceptable Quality Levels (AQLs) via automated processes that pull data from the root source, summarize it, and display it via Web tools. These Web

tools display actual results and indicate red/green colorizing to track performance against targeted goals. Our approach is to completely automate displaying results from data collection to Web display so that the focus is on acting on the results rather than report generation. Further, with the process automated, we ensure that business rules are established and there is no chance of manipulating the data.

VoIP and IP telephony services will rely heavily on the integrity of Qwest's underlying transport and data infrastructures and on service layer specific performance data. For VoIP, standard IP measurements tools are used to measure the common IP KPIs such as delay, packet loss, and jitter. In addition, VoIP introduces new KPIs to be monitored such as Mean Opinion Score. These incremental parameters are measured using specialized equipment [redacted] where a call path is monitored from a network availability perspective. Utilizing the [redacted], Qwest is able to provide proactive management alerts to our network management centers when problems are identified and provide passive management techniques to quickly identify issue isolation to support prompt resolution. Data is analyzed, formatted, and sent to operations, engineering, and planning for proactive network enhancement and capacity planning. This combined approach enables Qwest to reduce mean time to repair and increase mean time between failures to effectively support our world class network operation.

Qwest's VOIPTS performance parameters are collected via Simple Network Management Protocol (SNMP) management information for passive monitoring. Active tests are in a proprietary schema accessible via Open Database Connectivity/JDBC to internally developed analysis systems. The NGS platform utilizes the [redacted] and [redacted] for monitoring the

NGS platform. The [redacted] supports an SNMP V.2 interface for generating alarms on the platform.

Qwest's VOIPTS data is collected in real-time and is archived in a relational database [redacted] for future reference and analysis, if required. Additionally, 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

[redacted]

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.

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.

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, Layer 2 Virtual Private Network Service, Converged IP Service (CIPS), Content Delivery Network Services (CDNS), VOIPTS, and Internet Protocol Telephony Service), are provided over the same IP services infrastructure. [redacted]

[redacted]

[redacted]

[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 the General Services Administration, 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 Points of Presence (POPs) 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:

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 Government Furnished Property device, Qwest will provide KPI monitoring and measurement of the delivered service in three ways:

A. Request that the Agency provide SNMP capability to the device for the Qwest Network Operations Center

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.

- 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 the General Services Administration, 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.

For all services that Qwest offers, we use the [redacted] trouble ticketing system. [redacted] is a trouble ticketing system that is an industry-leading off-the-shelf commercial 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 that the Government requires for its services.

Qwest's VOIPTS KPI information is reported to Qwest's Network Operations teams [redacted]. The data is assigned a minor/major/critical severity level and is acted upon with processes assigned to each of those severity levels for the specific situation. KPI and AQL data collected is distilled at the Agency level for reporting.

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

[redacted] Qwest will meet all required KPIs and AQLs for VOIPTS. In the event 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 should be able to serve an Agency's business needs.

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

[redacted]

4.1.10.3 Satisfaction of VOIPTS Specifications (L.34.1.4.3)

Based on our existing commercial Qwest OneFlex Voice Termination service, Qwest VOIPTS meets all Networx specifications.

4.1.10.3.1 Satisfaction of VOIPTS 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.

4.1.10.3.1.1 Satisfaction of VOIPTS Capabilities Requirements (L.34.1.4.3(a); C.2.7.8.1.4)

Figure 4.1.10-15 below summarizes Qwest's technical approach to delivering the VOIPTS capabilities. Qwest fully complies with all mandatory stipulated and narrative capabilities requirements for VOIPTS. Figure 4.1.10-15 summarizes Qwest's response to the VOIPTS capabilities listed in RFP C.2.7.8.1.4. This figure and subsections are intended to provide the technical description required per L.34.1.4.3(a), and do not limit or caveat Qwest's compliance in any way.

Figure 4.1.10-15. Qwest's Technical Approach to VOIPTS Capabilities

ID #	Capability	Qwest's Approach
1	Establish & Receive Calls On-Net; Originate Calls to Off-Net	[redacted]

ID #	Capability	Qwest's Approach
2	Routing Prioritization or Class of Service (CoS)	[redacted]
3	Minimum VOIPTS Capabilities	
4	VOIPTS Gateway	
5	Alternate Routing to PSTN	
6	Traverse and Interoperate with Agency Firewalls	
7	Provide Secure Website for Performance and Reports	
8	Minimum & Optimal for Agency Equipment	
9	Minimum Quality Level	
10	Call Routing Between PSTN and IP	
11	Security Practices and Safeguards	

Class of Service Support (Req_ID 5492; C.2.7.8.1.4(2))

Qwest distinguishes between real-time (VoIP) and non-real time services using ToS settings. Qwest can assign 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]

[redacted] Priority QoS classifications, 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]
- [redacted]
- [redacted]

Support of Agency Dial Plans (Req_ID 5486; C.2.7.8.1.4(3)(d))

Qwest will interface with the Agency to ensure interoperability with their dial plans. Qwest will provide a Private Dial Plan (PDP) for Agency's on-net calling. Qwest utilizes its 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] Softswitch (combined policy server and gateway).

Support of Access Gateways (Req_ID 5485; C.2.7.8.1.4(4)(a))

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.

Agency Firewall Compatibility (Req_ID 5479; 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 5477; 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 VOPITS platform are shown in ***Figure 4.1.10-16***.

Figure 4.1.10-16. Qwest's Minimum and Optimal VOIPTS Equipment Requirements

Requirement	Description
VoIP signaling	Agency traffic must utilize SIP or H.323 for VoIP signaling and satisfy the specifications set forth in each of the following Internet Engineering Task Force Requests for Comments (RFCs) or Standards: • Internet Protocol (IP) – RFC 791 • User Datagram Protocol (UDP) - RFC 768 • Transmission Control Protocol (TCP) - RFC 793 • Real-Time Transport Protocol (RTP) and • Real-Time Transport Control Protocol (RTCP) – RFC 1889
SIP Signaling	SIP, RFC 3261 with Session Description Protocol, RFC2327 • UDP transport only • T.38 Fax support (with G.729 only) • Agency must send its telephony tone to Qwest in one, and only one, of the following methods: ○ In-band signaling ○ Out-of-band signaling using RFC2833 ○ Out-of-band signaling using SIP INFO
H.323 Signaling	H.323v4 shall be used. TCP transport only: • Must utilize one, and one only, of the following methods: ○ Direct signaling from Agency gateway to Qwest gateway ○ Gatekeeper-routed model where all signaling is sent from the Agency gatekeeper, but the media is sent from a gateway with a separate address ○ Location request (LRQ) model where Agency gatekeeper sends an LRQ to initiate call followed by call setup from Agency gatekeeper ○ H.323 Faststart only ○ H.245 tunneling is preferred ○ Allows for in-band signaling ○ Out-of-band signaling via H.225 facility messages

Requirement	Description

Other Signaling Requirements	• Each address must be an IP address and not a fully qualified domain name (FQDN). Agencies must provide Qwest with all of their initial IP addresses during the order process.
	• Agency signaling must also comply with the signaling rate (calls per seconds) specified below (see section 4.0).
	• The dialed number in the signaling must meet one of the following:
	  • U.S. domestic destinations using 10 digit (E.164) numbers
	  • LNP queries for U.S. domestic destinations
	  • International phone numbers (E.164) using a leading 011 or +011 string
	  • U.S. Domestic Toll-free using 10 digit (E.164) numbers

VoIP Audio Encoding	VoIP audio must be delivered to Qwest using RTP/RTCP, UDP over IP protocol. For H.323, Qwest allows for audio (RTP streams) to originate from a given circuit implementation or location implementation. SIP does not have the same limitation. Each address must be an IP address and not an FQDN. Agencies must provide all of their initial IP addresses to Qwest during the ordering process. Qwest IP Voice Termination product supports the following voice CODECs: • G.711 µ-law • G.711 a-law • G.729A (no silence suppression)* • G.729AB (silence suppression)*• * SDP for G.729 must comply with RFC3555. The supported payload samples sizes are 10, 20, and 30 ms. Qwest recommends that Agencies use 20 ms. For GFE, Agencies must support G.711 / G.729 CODEC auto-negotiation and fallback for FAX.

Security Practices–Implementation (Req_ID 5474; C.2.7.8.1.4(11)

Qwest will enforce current best security practices within its own network as well as provide guidance to the Agency as necessary. Qwest's VOIPTS complies with all industry best practice security practices and safeguards to minimize susceptibility to security issues and prevent unauthorized access.

[redacted]

[redacted]

Security Practices–Updates (Req_ID 5473; C.2.7.8.1.4(11))

Qwest will ensure regular updates and periodic audits, per its current risk management and security practice, to ensure that all necessary safeguards are met. Qwest is constantly evaluating new network threats and works in conjunction with its 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 5472; C.2.7.8.1.4(11)(a))

Qwest's Denial of Service detection is provided via several levels of security initiatives. Our customer/peer notification-based DDoS detection system, [redacted], monitors and detects Denial of Service (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 of IP spoofing prevention techniques such as unicast Reverse Path Forwarding and logon filtering.

Security Practices–Intrusion (Req_ID 5471; 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. The NGS security approach uses filtering and ACL techniques to allow use of public IP addressing for NGS traffic. Qwest uses NAT to hide the internal address space from external sources. 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 5470; 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 cannot be intercepted or 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 traversal functions to ensure that Qwest VoIP calls are totally secure and private and that eavesdropping or interception is prevented.

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

[redacted]

4.1.10.3.1.2 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.

4.1.10.3.1.3 Satisfaction of VOIPTS Interface Requirements (L.34.1.3.2(a); C.2.7.8.3)

Qwest fully complies with all mandatory stipulated and narrative interface requirements for VOIPTS. ***Figure 4.1.10-18*** summarizes Qwest's response to the VOIPTS interfaces listed in RFP C.2.7.8.3.1. This figure and subsections are intended to provide the technical description required per L.34.1.4.3(a), and do not limit or caveat Qwest's compliance in any way.

Qwest's NNS interfaces to an Agency's existing analog equipment using TDM-based interfaces. Qwest has proposed SED equipment to interface to non-IP based Agency equipment in order to meet Qwest's VOIPTS interface specifications. Qwest may substitute tested and certified alternative SEDs with similar functional and performance capabilities over the course of the program.

Figure 4.1.10-18. Qwest-Provided VOIPTS Interfaces at the SDP

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Signaling or Protocol	SED Make and Model (or equivalent)
1	Ethernet port: RJ-45 (Std: IEEE 802.3)	Up to 100 Mbps	SIP and H.323 are supported today. MGCP will be added when commercially available.	[redacted]
2	Analog Trunk: Two-Wire (Std: Telcordia SR-TSV-002275)	4 kHz Bandwidth	Loop Signaling (loop start and ground start)	[redacted]
3	Analog Trunk: Four-Wire (Std: Telcordia SR-TSV-002275)	4 kHz 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 1.536 Mbps	T1 Robbed-Bit	[redacted]

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Signaling or Protocol	SED Make and Model (or equivalent)
5	Digital Trunk: ISDN PRI T Référence Point (Std: ANSI T1.607 and 610)	Up to 1.536 Mbps	ITU-TSS Q.931	[redacted]
6 OCONUS/ non-domestic (optional)	Digital Trunk: E1 Channelized (Std: ITU-TSS G.702)	Up to 1.92 Mbps	SS7, E1 Signaling	[redacted]

VOIPTS Interfaces (Req_ID 7794; C.2.7.8.3.2(1))

Qwest will support all the mentioned interfaces and payload/signaling types as shown in Figure 4.1.10-18. [redacted] Qwest supports the interface requirement for RJ-45 delivery through use of the [redacted] router. This device has been lab tested to support VoIP delivery over a Fast Ethernet interface. The [redacted] is used in production today to support this interface for VoIP traffic on Qwest's IPS and NBIP-VPNS transport networks.

4.1.10.3.2 Proposed Enhancements for VOIPTS (L.34.1.4.3(b))

[redacted]

4.1.10.3.3 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.

4.1.10.3.3.1 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]

[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

4.1.10.3.3.2 CenturyLink Technical Approach

[redacted]

[redacted]

[redacted]

4.1.10.3.3.3 CenturyLink VoIPTS SIP Service

CenturyLink's VoIPTS SIP_will comprise of the following service elements listed in Table 4.1.10.3.3.3-1 with add on features listed in Table 4.1.10.3.3.4-1

4.1.10.3.3.3.1 Flat Local Session CLIN 232120:

[redacted]

Table 4.1.10.3.3.3-1 CenturyLink VoIPTS SIP Service

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

4.1.10.3.3.4. VoIPTS SIP Features

4.1.10.3.3.4.1 VoIP SIP Installation CLIN 232121

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

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

VoIPTS Telephone Number Setup (NRC) and Telephone Number MRC

4.1.10.3.3.4.3 Telephone Number (TN) Porting CLIN 232124

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

[redacted]

4.1.10.3.3.4.5 Remote Direct Inward Dial (RDID) Porting CLIN 232127

4.1.10.3.3.4.6 Business Blue Page Listing CLIN 232128

[redacted]

4.1.10.3.3.4.7 IP Diversity Set-Up CLIN 232129

[redacted]

[redacted]

4.1.10.3.3.4.8 8XX Service CLIN 232130

[redacted]

4.1.10.3.3.4.9 Dedicated VoIP Interconnect MRC CLIN 232131 and NRC CLIN 232132

[redacted]

4.1.10.3.3.4.10 SIP REFER MRC CLIN 232133 and NRC CLIN 232134

[redacted]

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

[redacted]

[redacted]

4.1.10.3.3.4.12 Remote Direct Inward Dial (RDID) CLIN 232137

[redacted]

[redacted]

Table 4.1.10.3.3.4-1 CenturyLink VoIPTS SIP Features

NRC CLIN	MRC CLIN	Usage	Description	Charging Unit
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

NRC CLIN	MRC CLIN	Usage	Description	Charging Unit
[redacted]				

4.1.10.3.4 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 its long distance traffic over IP (via [redacted] gateways) since 2001. This has enabled Qwest to provide a more reliable long distance 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 long distance service
- [redacted]
- Deployment of the OneFlex Voice Termination service commercially in July of 2004. The service currently [redacted] carries traffic in excess of more than four billion minutes per month.

4.1.10.4 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.

4.1.10.4.1 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] Qwest does not currently forecast any needed 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.

4.1.10.4.2 VOIPTS Measures and Engineering Practices (L.34.1.4.4(b))

Qwest's VOIPTS approach to the architecture is designed such that scaling can occur in a seamless manner and not affect existing systems. Capacity planning is ongoing to ensure that 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 of [redacted] is reached. The same logic will apply to the SBCs and 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 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] Such capacity upgrades are typically completed within 30 days of action being initiated. [redacted]. This ensures edge aggregation device access is redundant and access is not impacted in the event there is 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 Dense Wavelength Division Multiplexing 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 its 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 its customers with a network that has a general [redacted]. Furthermore, the interior of the Qwest network contains comprehensively meshed backbone circuits between TeraPOPs to ensure that any call will always have a minimum of two paths by which to pass from an originating SSP to a terminating SSP. Connectivity to the customer 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 at [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 are 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]

4.1.10.5 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.

4.1.10.5.1 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.

A number of activities result once this trigger is met. [redacted]

[redacted]

4.1.10.5.2 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 [redacted] 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]

4.1.10.5.3 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]

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.

4.1.10.5.4 Vision for VOIPTS 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]

[redacted]

Qwest's commitment to VoIP and its interoperability with the PSTN is solid. On the Voice Services side, Qwest is a leader with its deployment of VoIP services. [redacted]

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.