

4.1.11 Content Delivery Network Services (L.34.1.4)

Qwest's Networx Content Delivery Network Services combines our converged Internet Protocol-based network and our team member Akamai's content delivery platform to enable fast and reliable delivery of Web-based content globally.

Qwest's Content Delivery Network Services (CDNS) provides a suite of capabilities that off-loads origin servers and delivers content on their behalf. Our CDNS combines the unparalleled Qwest Internet Protocol (IP) network capability with Akamai's industry-leading content delivery network. Qwest's CDNS extends world-wide through Qwest's international Internet presence and Akamai's extensive global infrastructure. Qwest and Akamai have a proven record of working together to provide CDNS for Government and commercial clients, including award-winning service for the Internal Revenue Service (IRS).

4.1.11.1 Qwest's Technical Approach to CDNS Delivery (L.34.1.4.1)

The Qwest technical approach to providing a fully compliant CDNS has been developed and refined using our well established, highly reliable, and secure fiber optic infrastructure and global distribution of content servers, our commitment to our customers by our Operations and Engineering personnel, and our adherence to proven engineering practices. We recognize the importance of investing in research and development, are affiliated with key technology standards groups, and are represented on key Government advisory organizations, such as the National Security Telecommunications Advisory Council. Qwest has fine-tuned processes to research, evaluate, engineer, deploy, and operate new CDNS features and functionality.

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

4.1.11.1.1 Approach to CDNS Delivery (L.34.1.4.1(a))

Qwest's approach to effective CDNS delivery combines Qwest's proven global IP core network, Akamai's distributed CDNS, our proven deployment methodology, and the combined and dedicated Government service staffs at Akamai and Qwest. The combination of a proven delivery platform and refined processes ensures Agencies of customized, effective solution deployment.

CDNS consists of a collection of surrogate servers that offload work from origin servers by delivering content on their behalf. Our approach to CDNS leverages the Akamai content delivery infrastructure, thereby supporting world-wide distribution of content to meet Networx requirements. Our CDNS addresses four key technical/operational issues:

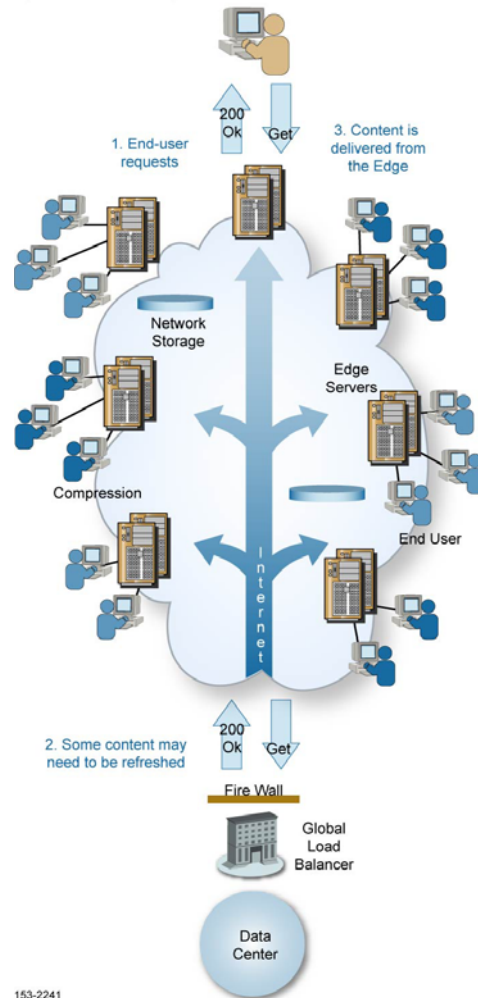
- 1. Latency:** Akamai's extensive distribution of content servers ensures the least possible delay in delivering content to Networx subscribers.
- 2. Scalability:** The high capacity of the CDNS infrastructure meets the requirements of Agencies. Our successful support of the high-capacity IRS website demonstrates the depth of Qwest's capability.
- 3. Reliability:** Our network monitoring and content distribution algorithms ensure 100 percent content availability for connected users. Our security management capabilities ensure content integrity.
- 4. Flash Crowd Control:** The capacity of the CDNS solution ensures our ability to meet unexpected high usage.

Qwest’s proven CDNS approach offers Agencies access unparalleled CDNS capability. Qwest owns and operates the world’s distributed content delivery platform, consisting of 20,000 in 1,100 Internet Service Provider (ISP) networks in 80 countries—a true, granular platform. No other CDNS provider can provide Akamai’s reach and resulting performance, scalability, and availability (see 4.1.11-1).

The Qwest Control Network Portal will enable Agencies to configure their capability. The Qwest Control Network portal will link to Akamai’s EdgeControl

Management Center (ECMC). ECMC delivers a wide range of operational and reporting services. The ECMC places control of the CDNS platform in the hands of Agencies to perform a wide range of services. A 24x7x365 Help Desk provides experienced support using proprietary network tools.

Figure 4.1.11-1. Akamai Content Delivery.
 Qwest/Akamai Network, 15,000 Servers,
 1,100 Networks, 68 Countries.



to an Akamai largest servers global global **Figure** CDNS

4.1.11.1.2 Benefits of Qwest’s Approach to CDNS (L.34.1.4.1(b))

Figure 4.1.11-2 summarizes Qwest’s CDNS customer benefits.

Figure 4.1.11-2 Benefits of Qwest’s Approach to CDNS

Feature	Benefit	Substantiation
Optimal Edge Server Identification	Optimal performance levels and content accessibility.	[Redacted]
Redundant and Resilient Network	Qwest’s solution provides 100% availability and high scalability, ensuring consistent performance and reliability regardless of load.	[Redacted]
Infrastructure Reduction/Optimization	By moving substantial content from the origin site to our network, Qwest dramatically reduces the need for distribution infrastructure. Customer Web and application servers, bandwidth, and software and hardware maintenance typically are reduced significantly.	[Redacted]

CDNS also supports the FEA objectives. *Figure 4.1.11-3* summarizes how our CDNS features support FEA objectives.

Figure 4.1.11-3. Qwest’s CDNS supports FEA objectives

FEA Objective	Qwest’s CDNS Support to FEA Objective
Improving utilization of Government information resources to focus on core Agency mission and service delivery to citizens by using the FEA	CDNS reduces the resources necessary to manage Agency content by providing a flexible service that addresses the spikes typical of Web-based information dissemination. With CDNS services, Agencies can configure origin websites to meet steady-state demand and satisfy high traffic load periods through CDNS. CDNS reduces the resources necessary to manage the origin site—and the hardware, software, and bandwidth necessary at the origin data center—allowing Government information resources to focus on core Agency missions.
Enhances cost savings and avoidance	CDNS allows Agencies to move content off origin infrastructures and significantly reduce the costs of provisioning origin data centers. [Redacted]

FEA Objective	Qwest's CDNS Support to FEA Objective
Increased cross-Agency and inter-Government collaboration	CDNS provides an open platform for both horizontal and vertical service delivery. The ability of CDNS to increase performance, improve scalability, and ensure availability of information among federal, state, and local Agencies can dramatically enhance effective collaboration.

4.1.11.1.3 Solutions to CDNS Problems (L.34.1.4.1(c))

Qwest has extensive experience in delivering CDNS services. We apply this experience to ensure the delivery of high-quality CDNS 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 4.1.11-4** summarizes some of the key problems we have encountered and the solutions we apply to resolve issues.

Figure 4.1.11-4. Qwest's Approach to Common CDNS Delivery Challenges

Problem	Solution
[Redacted]	[Redacted]
[Redacted]	[Redacted]
[Redacted]	[Redacted]

Problem	Solution
[Redacted]	[Redacted]

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

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted content]



Figure 4.1.11-6. Qwest’s Timing and Synchronization Architecture Provides Multiple Levels of Redundancy



Qwest monitors 24x7x365 all synchronization facilities and equipment with a Network Node Manager at the Network Control Facility. The Network Node Manager coordinates the sectionalization, removal from service, and return to service of the defective synchronization equipment in accordance with normal trouble clearance procedures. Integrity of the synchronization network is maintained by Qwest’s stringent surveillance of all facilities. Synchronization management includes the real time monitoring of BITS clock alarms, events, and maintenance activities.

Qwest’s timing and synchronization architecture is compliant with all applicable standards, including:

- Telcordia GR-253, SONET Transport Systems, Common Generic
- Telcordia GR-436, Digital Network Synchronization Plan

4.1.11.2 Satisfaction of CDNS Performance Requirements (L.34.1.4.2)

Qwest meets the performance requirements for CDNS.

4.1.11.2.1 CDNS Quality of Service (L.34.1.4.2(a))

Qwest will meet all Quality of Service requirements for Networx CDNS.

Figure 4.1.11-7 provides Qwest’s Acceptable Quality Levels (AQLs).

Figure 4.1.11-7 Qwest’s CDNS Meets All Networx AQLs

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	
Availability (CDNS network)	Routine	100%	100%	
Latency (static content download)	Routine	Mean = 1.5 sec	Mean < 1.5 sec	
Grade of Service (Time to refresh content)	Routine	5 minutes	≤ 5 minutes	
New Time to Restore (TTR)	Without Dispatch	4 hours	≤ 4 hours	
	With Dispatch	8 hours	≤ 8 hours	

Qwest understands each of the KPIs and meets the requirements for Availability, Latency, Grade of Service (time to refresh content), and new TTR.

Availability: Qwest’s CDNS leverages Akamai’s massive CDNS platform of 20,000 servers, 1,100 networks, and 2,500 physical locations. Akamai applies measures, such as load balancing and mapping software, at multiple levels. At the server level, Akamai provides server redundancy throughout its infrastructure. At an enterprise level, Akamai’s proprietary mapping algorithms continually monitor Internet status to determine the fastest, most reliable routing paths.

Latency for Static Content Download: The combination of Qwest's dedicated IP connectivity and Akamai's high performance platform—with route optimization, flexible caching, and delivery from the optimal edge server—ensures that we will meet the Networx latency performance requirements.

Grade of Service (GoS) (Time to Refresh): Qwest's CDNS meets the requirement. While we can establish time to refresh content in five minutes or less, our CDNS provides much greater and flexible refresh levels, as described in Section 4.1.11.3.2.

Time to Restore: Our CDNS has been designed from the ground up to require minimal human intervention. It is a self-healing, autonomous network that facilitates our support of restoration requirements.

4.1.11.2.2 Approach to Monitoring and Measuring CDNS KPIs and AQLs (L.34.1.4.2(b))

The Qwest Control Networx Portal will provide Agencies with easy-to-use monitoring and measurement tools to support management, operations, and billing of CDNS, including performance data. Through our portal, Agencies can view their traffic, content, applications, and users. Because our platform is open, Agencies can integrate the activation, management, and monitoring of services, content, and applications.

Qwest uses the following approach to measurement of CDNS Availability. This approach will also measure performance enhancement relative to the existing origin site, including Time to Refresh (GoS) and Time to Restore:

- From at least six geographically and network-diverse locations in major metropolitan areas, we will simultaneously poll a test file residing on the Agency's production servers and on Akamai's network.
- The polling mechanism performs two simultaneous http GET operations:

- a. A test file is placed on the customer's origin server (i.e., origin.customer.com)
 - b. One GET operation is performed to retrieve the file directly from the origin server (i.e., "http://origin.customer.com/testobject")
 - c. The other GET operation is performed to retrieve the file through the service by requesting the object from the appropriate Agency hostname CNAMEd to Akamai (i.e., "http://www.customer.com/testobject", where "www.customer.com" is CNAMEd to Akamai and configured to pull content from "origin.customer.com")
- The test content must use a Time To Live (TTL) of two hours or greater.
 - The test content will be a file of approximately 10 Kbps in size.
 - Polling will occur at approximately 12-minute intervals.
 - Akamai may also leverage third-party performance measurement providers such as Keynote Systems and Gomez Networks. These providers have performance measuring agents (i.e., servers that simulate end-user activity) throughout the world. An example of a measurement may consist of downloading a test object directly from the origin site and the same object from Akamai. Download times are recorded and presented.
 - Based on the http GET operations, the response times received from the two sources—1. the Customer server directly; and 2. the Akamai network—will be compared to measure performance metrics (latency, time to refresh), outages, and time to restore.

Each performance metric is based on a daily average of performance for the service, hits, and the Agency's production Web server—measured directly and computed from data captured across all regions. An outage is defined as a period of at least two consecutive failed attempts, six minutes

apart, by a single agent to GET the Agency's test file from the service, while succeeding to GET the test file from the Agency origin server directly. In order to activate the conformance to the AQL, the Agency must enter and indicate the location of two valid test files for the same object into the portal exposed Service Level Agreement (SLA) Activation Tool. Detailed instructions are provided with the SLA Activation Tool. In addition, assistance is available from the Qwest Account Manager. The AQL will go into effect within five business days after the customer enters valid test files into the SLA Activation Tool.

Qwest's CDNS will establish a configuration file for each website or application. Within the GoS (Time to Refresh) configuration file, refresh rates or caching times may be defined down to very granular levels (i.e., every object on every page.) Once the content refreshing rules are established, the content may be updated continually by the content manager. Agencies may view the configuration file and monitor performance using the Qwest Control Networx Portal.

For all services that Qwest offers, we use the Remedy[®] trouble ticketing system. Remedy 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 TTR. The calculation for TTR uses the same business rules as the Government requires for its services.

Measuring SDP-to-SDP Latency, and the Role of Service Enabling Devices

All of Qwest's IP-based services, which include the eight mandatory services (Internet Protocol Service (IPS), Network Based Internet Protocol Virtual Private Network Service (NBIP-VPNS), Premises-based IP VPNS

(PBIP-VPNS), Layer 2 Virtual Private Network Service (L2VPNS), Converged IP Services, CDNS, Voice Over Internet Protocol Transport Services, and Internet Protocol Telephony Services) are provided over the same IP services infrastructure. As a point of reference, Qwest has structured its network into a set of Provider routers that form the core of our network and a set of Provider Edge (PE) routers that provide access to network services.

The Provider routers are private, in that they do not participate in routing to public Internet addresses. Their function is to provide bandwidth between the several sets of PE routers via sets of full-mesh Label Switch Paths.

Following standard convention, the Service Delivery Point (SDP) is the Customer Edge (CE) router, as depicted in [REDACTED]

Monitoring for SLA reporting operates as follows:

[REDACTED]

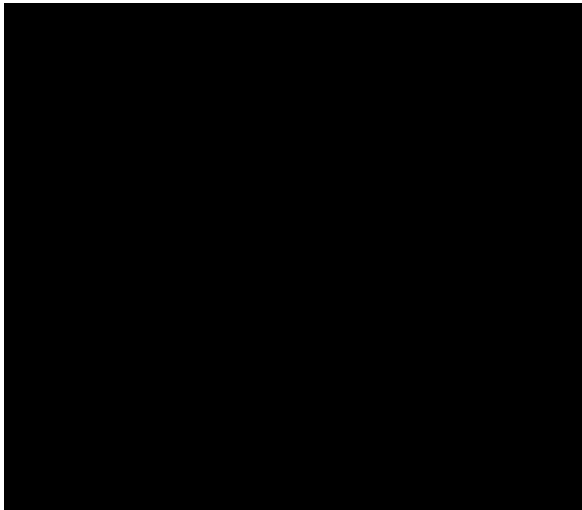
[REDACTED]

[REDACTED]

Qwest's approach consumes few resources at the SDP (generally the CE router) as probes are sent from the Qwest network. This methodology does require that the customer respond to ICMP ECHO (a.k.a. ping) messages.

[REDACTED]

Qwest's solution was designed from the beginning for its commercial offering to be SED-vendor agnostic. Qwest's performance management (PM)



architecture is standards-based, scalable and flexible, as well as 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.



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 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 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 Point(s) of Presence (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:

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:

1. Request that the Agency provide Simple Network Management Protocol capability to the device for the Qwest Network Operations Center (NOC)
2. Request that the Agency buy a monitoring SED from Qwest

3. 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 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.

4.1.11.2.3 CDNS Performance Improvements (L.34.1.4.2(c))

[REDACTED]

[REDACTED] In the event an Agency has a specific business need or application problem, Qwest will to discuss service enhancements. Qwest will operate in good faith to engineer a CDNS solution to serve unique Agency needs. Qwest is able to leverage our vast CDNS product portfolio, which includes a variety of SED providers and specific CDNS solutions. Through a special combination of vendor solutions and talented engineering capabilities, Qwest will serve an Agency's business needs.

4.1.11.2.4 Additional CDNS Performance Metrics (L.34.1.4.2(d))

Qwest is not proposing additional performance metrics for CDNS.

4.1.11.3 Satisfaction of CDNS Specifications (L.34.1.4.3)

Qwest understands and complies with the designated standards, connectivity requirements, and technical capabilities for CDNS. Both team members actively participate in a number of standards-related organizations and have played an active role in bringing new standards to the market. For example, Akamai, together with IBM and Oracle, developed Edge Side Includes standards, which have been widely recognized and adopted by vendors to provide dynamic edge-based content delivery and processing.

4.1.11.3.1 Satisfaction of CDNS Requirements (L.34.1.4.3(a))

The following three sections describe how Qwest satisfies all of the capabilities, features, and interfaces for CDNS.

4.1.11.3.1.1 Satisfaction of CDNS Capabilities Requirements (L.34.1.4.3(a); C.2.4.6.1.4)

Qwest fully complies with all mandatory stipulated and narrative features, capabilities, and interface requirements for CDNS. The text is intended to provide the technical description required per L.34.1.4.3(a) and does not limit or caveat Qwest's compliance in any way. Qwest fully supports the CDNS capabilities for Networx. The requirements are organized into content distribution and site monitoring/server performance measurements.

Content Distribution

Our specific service offerings include static content download service, real-time streaming, and on-demand streaming. The approach to each is briefly described in the following paragraphs.

Static Content Download Service: For delivery of static site content, each end-user request is directed to an edge server via intelligent Domain Name Server (DNS). Upon receiving a request for content, an edge server retrieves the appropriate content (HyperText Markup Language page, image, document download, Secure Sockets Layer (SSL) object, and Video on

Demand file) from a local cache and delivers the resulting content to the requesting user. If requested content is not in cache at the edge, it is retrieved from within the network or the origin site.

Real Time Streaming: For live streaming, depending on the format of the encoded media, encoders push the content—or the Entrypoint pulls the encoded stream—into the CDNS service. If the media being provided to Qwest is in a raw (un-encoded) state, the stream will need to be encoded in at least one of a variety of formats including, but not limited to, RealNetworks Real Media, Microsoft Windows Media, and Apple Quicktime. The format(s) chosen depends on the requirements of the Agency. Encoding requirements (codec, stream rate, and acquisition method) may vary greatly from event to event. After the encoded stream is acquired, the reflectors on the CDNS network then route the stream from the entry point to the edge servers, while maintaining reliability and quality. Routing via the network uses sophisticated packet recovery techniques, including re-transmit and multiple path transmission, to guarantee the highest quality stream delivery to edge regions. The edge regions then distribute the streams to end-users. Pre-bursting, another performance advantage, significantly reduces the time necessary to buffer and start the stream.

On-Demand Streaming: For on-demand streaming, when a user clicks on a stream, they are routed to the optimal server. Encoding for On-Demand Streaming is handled in the same way as Real Time Streaming except that the content is stored on CDNS resident storage and typically not acquired “live.” Our CDNS employs a pull architecture: content is replicated in streaming server caches in response to user requests, as follows:

- The streaming servers cache only the content that the users view, not the entire file.

- The platform load balances among our streaming servers to ensure that no single machine is responsible for the delivery of all content.
- The HyperText Transfer Protocol (HTTP) is employed to deliver on-demand streams to edge streaming servers.



Site Monitoring/Server Performance Measurements

Available through the Qwest Control Networx Portal, the ECMC is a dashboard that provides a comprehensive collection of network management tools. This provides Agencies with instant visibility into their traffic, content, applications, and users on the Internet enterprise management systems, including HP OpenView and IBM Tivoli NetView. Agencies can integrate real-time monitoring and alerts information directly with their existing third-party tools. As a result, they receive the benefits of integrated management, while reducing the costs associated with deploying multiple management platforms. Akamai collects data to support management, operations, and billing of our platform, including data for all the performance metrics of this Request for Proposal, including availability, latency, File Transfer Protocol (FTP) load, Central Processing Unit load, memory usage, SSL service load, HTTP port service load, and HTTP connections queue statistics.

4.1.11.3.1.2 Satisfaction of CDNS Feature Requirements (L.34.1.4.3(a); C.2.4.6.2)

Qwest fully complies with all mandatory stipulated and narrative features, capabilities, and interface requirements for CDNS. The text in **Figure 4.1.11-8** is intended to provide the technical description required per L.34.1.4.3(a) and does not limit or caveat Qwest's compliance in any way. Qwest supports the mandatory and optional CDNS features as summarized in **Figure 4.1.11-8**.

Figure 4.1.11-8 Technical Approach to CDNS Features

ID Number	Name of Feature	Qwest's Technical Approach
1	Failover Service	<p>Qwest meets this requirement and offers several additional features of failover service described in Section 4.1.11.3.2.</p> 
2 (Optional)	Redirection and Distribution Service (Global Load Balancing)	<p>Qwest meets this requirement.</p> 

Qwest's CDNS provides a flexible failover service that ensures multiple options for Agencies. Websites that rely on centralized infrastructure often find that ensuring uptime is a continuous challenge. A typical solution involves mirroring a website at an alternate location; however, this approach creates additional capital and management costs. EdgeSuite Site failover frees Agencies from the unnecessary capital and management costs associated with creating a failover solution, offered as a managed service.

4.1.11.3.1.3 Satisfaction of CDNS Interface Requirements (L.34.1.4.3(a); C.2.4.6.3)

CDNS is an application layer service supported by the connectionless data services available with the IP suite of protocols via the User-to-Network

Interfaces discussed in Section 4.1.14.3.1.3. The CDNS provides data transfer from an origin server to the CDNS servers via IP. The service is available to all Agency servers reachable by IP.

4.1.11.3.2 Proposed Enhancements to CDNS (L.34.1.4.3(b))

Qwest's CDNS exceeds both the Failover Service and Redirection and Distribution Service requirements and offers several additional capabilities to Agencies.


Failover Service: As described in the previous section, Qwest exceeds this requirement through our ability to provide failover as a completely automated managed service, with no hardware or software requirements, and to provide three failover options, based on the needs of the client. Failover options are detailed below.

Failover Option 1—Failover to Qwest's Net Storage: If an Agency wants to ensure that a complete origin site will be available to end users regardless of the health of the origin site and/or Internet connectivity, Qwest can establish a back-up site on [REDACTED]. [REDACTED]

[REDACTED] By running the back-up site on [REDACTED], Qwest is able to ensure a much higher degree of reliability, security, and performance, in addition to offloading the need for additional infrastructure. The Agency can store a default page [REDACTED]

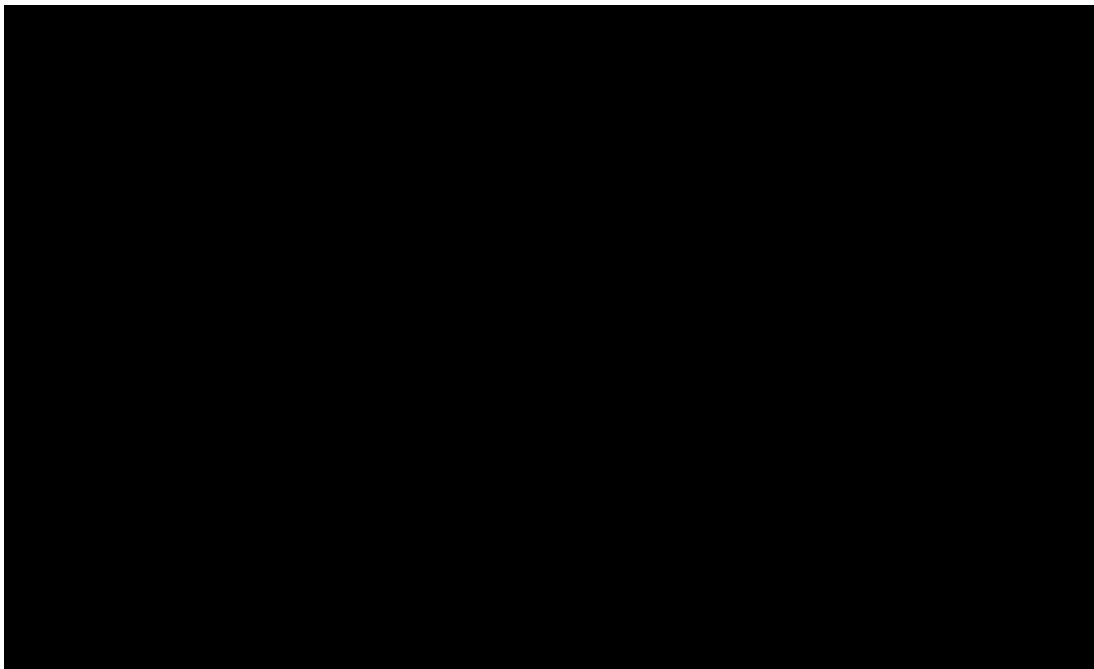
Failover Option 2—Failover to Alternate Data Center (Mirror Failover): In the event that an Agency wants to be protected against the failure of an origin site and is running a backup or alternate site, site failover can be directed to use the back-up site in the case that the primary is unavailable. Note that the back-up site may, at the discretion of the Agency, be different from the origin site—for example, a site containing reduced

functionality or content. Upon receiving a request for a piece of content that must be obtained from the primary site and determining that the primary site is unavailable, the edge server will obtain the requested content from the mirror site in a fashion invisible to the end user.

Failover Option 3—Failover to Edge Server: If the edge server needs to contact the origin server to fetch or revalidate content but cannot reach the origin server, it can be configured to serve the expired (most recent) version currently in cache. Agencies can configure the time it takes for the Qwest server to time-out its attempt to connect to the origin server and serve the most recent content instead.  depicts the Failover to Edge Server.

The needs of a particular Agency’s site and available infrastructure will determine which Site Failover option is appropriate. In all three scenarios, however, Qwest automatically detects whether the customer’s origin server is responding to requests and will detect when it is back online.

Potential Service Enhancements: Additional content delivery features, application accelerators, on-demand events, and performance



management tools can be provided. These include:

- **Flexible TTL and Time to Refresh Settings:** Agencies can define the TTL for every object or page, a designation that can be assigned in less than a minute. TTL can be set from “no store” (never cache) to seconds, minutes, hours, or days. The Agency can also direct not to cache certain objects or to check with the origin at every request for a particular object to see if it has been modified. A page often consists of 5 to 20 objects, and each can have its own custom TTL.
- **Access Control:** Access Control allows Agencies to limit access to content by integrating with authorization policies defined on an origin server.
- **Advanced Cache Control:** Advanced Cache Control enables EdgeSuite to increase the ability to store complex and dynamic content.
- **Content Targeting:** EdgeSuite Content Targeting enables Agencies to customize content to drive targeted business strategies online. The possible applications are limited only by imagination.
- **Download Manager:** Download Manager provides a simplified method of distributing, downloading, and installing digitized assets via the Internet. It can be used with websites that deliver content via SSL as well as with sites that require authentication before providing access to content. Download Manager is available as an add-on component for Agencies that use their websites to deliver digitized files such as software, movies, or other large objects.
- **Dynamic Content Assembly:** Dynamic Content Assembly enables Agencies to assemble and customize Web pages on Akamai edge servers, delivering personalized content reliably to every user, while minimizing the demands on centralized application servers.

- **Enhanced DNS:** Qwest’s Enhanced DNS provides a robust, reliable, and scalable solution to direct end-users to customer websites. It requires no change to existing DNS administration processes and provides unparalleled reliability, scalability, and performance of DNS resolution.
- **FTP:** Qwest’s FTP is a managed service that incorporates proprietary replication technology and global traffic management service using best-of-breed core storage equipment. The result is a scalable, high-performance and highly available storage and FTP Download service.
- [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] By using this fault-tolerant storage service, Agencies can make rich media content available to users on demand, anytime, and anywhere.
- **Secure Content Delivery:** SSL processing is extremely slow and often requires content providers to substantially overprovision sites to maintain performance and scalability. EdgeSuite Secure Content Delivery is a highly secure, outsourced solution that addresses the performance and security needs of customer SSL content, while reducing costs and complexity. It supports the reliable and secure delivery of SSL objects and pages and runs on a dedicated section of the Platform. EdgeSuite Secure Content Delivery offers the highest degree of physical security and is optimized for SSL traffic.
- **SureRoute:** This unique feature, available exclusively from Qwest, optimizes the delivery of all types of content—dynamic, static, cacheable, and uncacheable. It determines the optimal path between an Agency’s

origin site and Qwest’s edge servers, ensuring optimal performance and guaranteed delivery to every end-user, regardless of Internet conditions.

- **Tiered Distribution:** Tiered Distribution is offered specifically to enterprises that experience flash crowds or that offer a large number of sizeable files for download. EdgeSuite Tiered Distribution enables customers to effectively and quickly deliver content to end-users while minimizing the number of hits back to the origin website. With EdgeSuite Tiered Distribution, Agencies ensure high performance and dependability for their end users while reducing their Information Technology staff’s planning requirements and costs.

4.1.11.3.3 Network Modifications Required for CDNS Delivery (L.34.1.4.3(c))

No modifications to Qwest's or Akamai’s networks are required to deliver CDNS under the Networx program.

4.1.11.3.4 Qwest Experience with CDNS Delivery (L.34.1.4.3(d))

Qwest and Akamai have collaborated to deliver CDNS to both commercial and Government customers. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] Together, we offer a coordinated, proven capability to the Networx program.

Akamai is deployed in 11 of 15 Government Cabinet Agencies, has more than 40 Federal contracts, and was recognized by a trade publication in 2005 for delivering the 8 fastest Federal websites, demonstrating both market share and platform performance.

Qwest and Akamai have extensive experience with and understanding of the Government environment. [REDACTED] summarizes our CDNS experience.

Figure 4.1.11-10. Qwest CDNS Experience

Client	Qwest Products/Services	Results
[REDACTED]	EdgeSuite Enterprise	[REDACTED]
[REDACTED]	EdgeSuite Enterprise	[REDACTED]
[REDACTED]	EdgeSuite Enterprise, Netstorage	[REDACTED]
[REDACTED]	EdgeSuite Enterprise	[REDACTED]
[REDACTED]	EdgeSuite Enterprise	[REDACTED]
[REDACTED]	EdgeSuite Delivery	[REDACTED]
[REDACTED]	EdgeSuite Enterprise	[REDACTED]
[REDACTED]	EdgeSuite Enterprise, SureRoute; Site Shield	[REDACTED]
[REDACTED]	EdgeSuite Enterprise	[REDACTED]
[REDACTED]	EdgeSuite Enterprise, Enhanced DNS, FirstPoint	[REDACTED]

4.1.11.4 Robust Delivery of CDNS (L.34.1.4.4)

Qwest’s CDNS combines the industry leaders in IP connectivity and content delivery. We have examined the Networx traffic model and find that even the Year 10 requirements would be easily satisfied by our respective infrastructures. Our CDNS also provides a robust and reliable platform for the delivery of content to Agencies. Akamai has successfully expanded its CDNS infrastructure globally and demonstrated its ability to deliver service in the most challenging of network conditions. Likewise, Qwest’s IPS platform

employs redundant design throughout and is closely monitored for traffic growth and patterns to ensure a resilient and robust service capability.

4.1.11.4.1 Support of Government CDNS Traffic (L.34.1.4.4(a))

Over the course of the 10 years delineated in the Government’s pricing model, committed bandwidth for both domestic and globa [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

4.1.11.4.2 CDNS Measures and Engineering Practices (L.34.1.4.4(b))

Qwest’s CDNS alliance, Akamai, closely monitors traffic, plans for the future, and routinely upgrades and expands its platform capacity based on current and anticipated demand. In addition, Qwest’s centralized engineering team applies a consistent capacity management model to all data services. Qwest’s proactive assessment and enhancement of our network capacity ensures our clients that we will always be able to deliver their data, regardless of network conditions.

Our CDNS has built-in, automatic, self-healing properties, such as the ability to route around congested points, and to divert traffic away from data centers that are down. These fundamental engineering practices ensure resiliency in a dynamic environment.

4.1.11.5 CDNS Optimization and Interoperability (L.34.1.4.5)

Qwest CDNS understands the vital importance of service optimization and interoperability. The following sections describe our approach, methods, techniques, and vision for CDNS optimization and interoperability.

4.1.11.5.1 Qwest's Approach to Optimizing CDNS (L.34.1.4.5(a))

Qwest's CDNS platform optimizes content assembly and delivery to efficiently deliver Web content and applications from carefully located and load-balanced servers. The content delivery platform is connected with the clients' content generation infrastructure using optimal paths through the Internet and using intelligent routing algorithms supported by real-time network information. The delivery of content is then served by [REDACTED] edge servers that are deployed near all end users.

Intelligent Request Routing: Qwest's CDNS platform uses patented Internet monitoring software to maintain a comprehensive view of network health and sophisticated content-routing algorithms to route users to the optimal servers on the platform.

We employ a variety of techniques for Internet topology discovery and for measurement of up-to-the-minute latency, loss, and bandwidth metrics to a variety of points on the Internet. These network performance measurements are then combined with detailed load, "liveness," and capacity information from our servers to arrive at mapping decisions for end users. As a result, every end user is mapped to a nearby server that is lightly loaded and that maximizes performance for the relevant application. Manifest as an instantaneous decision at DNS resolution time, our patented network-routing algorithms find the best edge server for each request. This ability to optimize load and performance is unique to our CDNS platform.

High Performance Communications: The Qwest CDNS platform has highly optimized communications between edge servers, as well as between edge and origin servers, to ensure that content and data are always readily available from all edge servers. Two of the core communications systems are SureRoute and Metadata Transmission.

SureRoute identifies alternate paths from our edge server to the origin server and uses those alternatives to improve performance of content delivery. Using both Border Gateway Protocol (BGP) and alternate routes using our edge servers, real-time performance measurements are used to determine the fastest route, allowing the user to bypass network congestion to which BGP has no ability to react.

The Metadata Transmission System is a highly scalable and reliable system to transmit Agency configurations (metadata) to edge servers. Unique aspects of this infrastructure are its application of Sure Route for high-performance routing to edge servers, robust mechanisms of replicating data submitted to our content delivery platform, and the ability to transport data to the entire content delivery network very rapidly.

Network Management and Monitoring: To ensure ongoing optimization of this diverse and distributed platform, Qwest has built a comprehensive set of tools to administer a network configuration and heterogeneous state efficiently, enable easy modular modification and addition of software components, and scale and fully automate the software installation process. The NOC uses proprietary, secure, scalable, real-time data collection mechanisms to enable efficient and responsive monitoring of the platform. If a problem is detected, our fault-tolerant architecture takes over, automatically switching from one edge server to another. Our NOC personnel investigate the cause.

Proactive Performance Monitoring: In addition to the NOC, Qwest has a variety of software and infrastructure that provides detailed information used to ensure optimal performance for end users, as well as for continual analysis and optimization of the CDNS algorithms and network. Examples include data collected from Akamai's distributed agents for HTTP and HyperText Transfer Protocol Secure testing; Akamai's proprietary, patented

agents and technology for testing streams from all major formats; and network protocol level statistics logged by Akamai servers.

4.1.11.5.2 Qwest's Approach to Optimizing Network Architecture for CDNS (L.34.1.4.5(b))

The technology behind Akamai's CDNS is the Mapping Process that continuously monitors Internet conditions and routes users to the optimum edge servers [REDACTED]. Users benefit from the best performance possible.

4.1.11.5.3 Qwest's Approach to Access Optimization for CDNS (L.34.1.4.5(c))

Our CDNS approach is driven by the Mapping Process algorithms described in Section 4.1.11.5.2—algorithms that were initially developed at the Massachusetts Institute of Technology by the founders of Akamai. Akamai's content delivery servers are deployed in more than 1,100 ISP networks, ensuring close proximity to large concentrations of diverse customers and enabling us to handle their requests efficiently.

Akamai has also made several enhancements to first and last mile access, such as SureRoute (optimum path determination between BGP and just routing traffic via edge servers), GNU Zip Compression, Prefetch, and Transmission Control Protocol Optimizations, to ensure better performance.

4.1.11.5.4 Qwest's Vision for CDNS Internetworking (L.34.1.4.5(d))

Qwest, the leader in the development of IP-based convergence, and Akamai, the world's leading IP delivery vehicle, firmly believe in a common, IP-centric architecture. Qwest and Akamai have implemented this vision. The foundation of the content delivery business lies in providing IP-based services that leverage common standards and network interoperability. Qwest's broad and deep solution set of IP-based service offerings ensures support for any CDNS or related requirement, ranging from the division to the department.

Qwest is well-positioned to support the continuing evolution toward IP convergence—delivering content around the world—to meet the ever-increasing demand for IP-based services.