

# WITS Program Service and Product Proposal for Dedicated Internet Access (DIA)



**Submitted To:**

General Services Administration  
Attention: Ms. Kimberly Bowie, Administrative Contracting Officer  
Room 6040  
301 Seventh Street, SW  
Washington, DC 20407  
(202) 708-6796

**Submitted By:**

Qwest Government Services, Inc.  
4250 North Fairfax Drive  
Arlington, VA 22203  
Audrey Hallett  
(703) 363-3077  
[audrey.hallett@qwest.com](mailto:audrey.hallett@qwest.com)

Qwest Proposal Number: FSQ2616

**January 29, 2004**

Qwest Corporation will not provide interLATA long distance voice services in Montana until Qwest is able to do so.

This document includes data that shall not be disclosed outside the Government and shall not be duplicated, used, or disclosed - in whole or in part - for any purpose other than to evaluate this service and product description. This restriction does not limit the Government's right to use information contained in this document if it is obtained from another source without restriction. The data subject to this restriction are contained on all sheets of this proposal.

## Table of Contents

<b>1</b>	<b>TECHNICAL RESPONSE .....</b>	<b>1</b>
1.1	COMPLIANCE CHECKLIST TABLE B-1 .....	1
1.2	REQUIRED NARRATIVE RESPONSES TABLE B-2 .....	15
1.2.1	Proposed System Architecture.....	16
1.2.1.1	Interconnecting with Serving Offices.....	25
1.2.1.2	Interconnecting with Local Exchange Network.....	25
1.2.1.3	Interconnecting with Government Networks.....	25
1.2.1.4	Internetworking with Other Service Providers.....	25
1.2.1.5	Providing Access to Commercial Telecom. Services.....	25
1.2.1.6	Economically Serving Small Customers .....	26
1.2.1.7	Maintaining Compatibility with Existing CPE .....	26
1.2.1.8	Addressing Scheme .....	26
1.2.1.9	News Feed.....	26
1.2.1.10	Access and Security.....	26
1.2.2	Quality of Proposed Services .....	26
1.2.3	Service Availability Intervals .....	27
1.2.4	Operational Support Systems .....	28
1.2.5	Draft Implementation Plan .....	37
1.2.6	Management and Operations Approach.....	38
1.2.7	Partnership with GSA .....	38
1.3	QWEST MANAGED ROUTER SERVICE.....	40
1.3.1	Network Profile.....	41
1.3.2	Continuous Monitoring .....	42
1.3.3	On-Line Network Reports .....	43
1.3.4	Fault Management.....	45
1.3.5	Configuration Management.....	46
1.3.6	Performance Management.....	47
1.3.7	Network Analysis.....	48
1.3.8	NMC Secure Web Interface .....	50
1.3.9	Network Management Center (NMC) .....	51
1.3.10	NMC Security .....	51
1.3.11	Description of Qwest-Furnished Equipment.....	52
<b>2.</b>	<b>PRICE RESPONSE .....</b>	<b>53</b>
<b>3.</b>	<b>RATE GROUP DEFINITION.....</b>	<b>54</b>
 <b>ATTACHMENT</b>		
<b>A:</b>	<b>SECTION H RECONCILIATION DOCUMENT .....</b>	<b>55</b>

## List of Figures

Figure 1: [REDACTED]	16
Figure 2: [REDACTED]	17
Figure 3: [REDACTED]	19
Figure 4: Qwest TeraPoP Architecture	20
Figure 5: IAS Customer Interfaces	22
Figure 6: Internet Statistics Report Selection Screen	30
Figure 7: Report Definition Screen	31
Figure 8: Internet At-a-Glance Report	31
Figure 9: Ticket List	32
Figure 10: Ticket Details	33
Figure 11: Create Trouble Ticket Interface Screen	34
Figure 12: Network Alarms	35
Figure 13: Network Alarm Detail	35
Figure 14: [REDACTED]	36
Figure 15: [REDACTED]	36
Figure 16: User Manager Screen	37

## List of Tables

Table B-1: Compliance Checklist	1
Table B-4.9: Stipulated Services and Products Compliance Checklist: IAS	9
Table B-2: Required Narrative Responses	15
Table 1: Qwest Communications Peering Overview	21
Table 2: IAS SDP Definition	23
Table 3: IAS UNI Interfaces	23
Table 4: Data Aggregation	44
Table 5: Managed Packet Filter Router Hardware Description	52

# 1 TECHNICAL RESPONSE

Qwest Government Services, Inc. (QGS), a wholly-owned subsidiary of Qwest Communications International, Inc. (QCII), is pleased to submit this product proposal to the General Services Administration (GSA) for Dedicated Internet Access (DIA) under the WITS2001 initiative in accordance with the WITS2001 Request for Proposal WTT-98-PW-N-0001 Consolidated Version dated September 28, 1999, and the WITS2001 Crossover Requirements dated January 11, 2002. This proposal provides Qwest Dedicated Internet Access and Qwest Managed Router Service. In order to meet all of the technical requirements set forth in Section C of the RFP, Qwest will provide future proposals to add Web Hosting, Dial Access, and VPN services.

This proposal is submitted with a companion WITS2001 Eligibility Proposal and is offered as a long distance modification to be made available under FTS2001 under Qwest's Seattle MAA, Contract GS00T02AHD004 awarded May 13, 2002. Qwest is fully qualified under the GSA MAA requirements and currently holds MAA contracts in Albuquerque, NM; Boise, ID; Denver, CO; Minneapolis, MN; Seattle, WA; and Salt Lake City, UT.

Qwest accepts the Section I provisions of WITS2001. Attachment A in this proposal contains the Section H Reconciliation Document.

## 1.1 Compliance Checklist Table B-1

An executed version of Table B-1, Compliance Checklist, is provided below. A column has been added to the table to acknowledge compliance or note that we concur with a pricing directive. Proposed pricing is provided in Section 2 in accordance with the requirements set forth in Table B-1.

Table B-4.9, Stipulated Services and Products Compliance Checklist: IAS, is also provided to indicate compliance with specific IAS technical requirements and provide a cross reference to the proposal.

**Table B-1, Compliance Checklist**

Rec. No.	Requirement	Requirements Reference	Compliance
1	The contractor shall provide specified price schedules for provisioning required services and features for the life of the contract.	B.1 Pricing Overview	Qwest will comply
2	The contractor shall furnish all personnel, services, and equipment necessary to perform the requirements set forth in the contract.	B.1.1 Provisions	Qwest will comply
3	All service orders under this contract shall be priced in accordance with the price schedules of this section.	B.1.2 Pricing of Orders	Qwest will comply
4	The contractor shall propose fixed-price schedules for each product and service proposed for each applicable year of the contract modification. The prices for services defined in the price tables shall not include Federal, state, or local taxes defined in Section H.14 that are in effect on the contract modification date, the Associated Government Fee defined in Section H.25, or the regulatory charges	B.1.2 Pricing of Orders H.25 WITS2001 Associated Government Fee(s) H.28 Regulatory Passthroughs 2.3.2.1 Changes to WITS2001 RFP Technical Requirements	Qwest will comply

This document includes data that shall not be disclosed outside the Government and shall not be duplicated, used, or disclosed - in whole or in part - for any purpose other than to evaluate this service and product description. This restriction does not limit the Government's right to use information contained in this document if it is obtained from another source without restriction. The data subject to this restriction are contained on all sheets of this proposal.

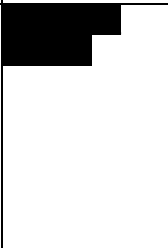
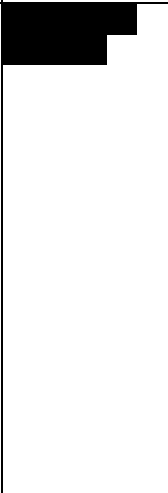
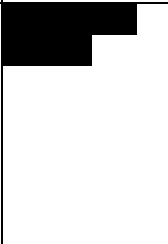
Rec. No.	Requirement	Requirements Reference	Compliance
	defined in Section H.28. The contractor shall provide in Table B-0.6 any taxes or regulatory passthroughs that may appear on a WITS Program invoice that are in existence at the time of the award of the contract modification. Offerors shall use the jurisdictional rates in existence at the time of proposal submission for all remaining years of the contract modification.		
5	All price tables shall be effective at the time of the contract modification. If the contract is modified effective between October 1 and March 31 of a given fiscal year, price tables for contract modification pricing for the first year shall be effective through September 30 of that fiscal year. If the contract is modified between April 1 and September 30 of a given fiscal year, price tables for that contract modification for that year shall be effective through September 30 of the following fiscal year. Price tables for the remaining years shall be on a Government fiscal year basis.	B.1.2 Pricing of Orders 2.3.2.1 Changes to WITS2001 RFP Technical Rqts	
6	Proposed prices on the first effective price table (within a particular contract year) for any service, feature, or other charge shall not increase on the second effective price table (for the subsequent fiscal year) if the first effective price table is in force for less than six months.	B.1.2 Pricing of Orders	
7	Prices provided in the proposal shall not increase within a fiscal year but may increase from fiscal year to fiscal year.	B.1.2 Pricing of Orders	
8	The offeror shall collect taxes, as applicable to the monthly WITS Program charges, from the agencies or GSA for subsequent distribution to the applicable jurisdiction. Until the offeror distributes collected taxes to the jurisdictions, such monies shall be deposited in interest-bearing escrow accounts. The contractor shall establish such interest bearing escrow accounts on behalf of the Government, specifically and only for the payment of taxes associated with WITS Program sales and services. One hundred percent of the accrued interest from such escrow accounts shall be remitted to the Government as a direct payment on a quarterly basis.	B.1.2 Pricing of Orders 2.3.2.1 Changes to WITS2001 RFP Technical Rqts	
9	All prices on a row of a price table shall carry a "start" date, which is the date when the prices on that row become effective. These prices shall remain in effect through their listed "stop" date or until the prices are changed by a contract modification. When prices are revised by a contract modification, the newly inserted rows shall become effective by their listed start dates, and the pricing rows that are being replaced shall carry a "replaced" date, the date when the contract modification will become effective. The listing of a price-replaced	B.1.2 Pricing of Orders	

Rec. No.	Requirement	Requirements Reference	Compliance
	date shall always identify a row that is being replaced by a contract modification.		
10	The offeror shall propose a Contract Line Item Number (CLIN) for each proposed charge (except taxes, the Associated Government Fee defined in Section H.25, the regulatory passthroughs defined in Table B-0.6, and ODCs of less than \$50,000) using the CLIN format prescribed in Section B.2.1, footnote #1.	B.1.2 Pricing of Orders, H.25 WITS2001 Associated Government Fee(s) 2.3.2.1 Changes to WITS2001 RFP Technical Rqts	
11	Basic service is defined as that set of basic capabilities that are inherent within the base price and shall not be unbundled. Unless otherwise specified in this contract, basic service prices shall include the price to implement, operate, administer, and maintain WITS Program services; and establish and maintain appropriate interconnection arrangements with the local exchange network.	B.1.3 Price Categories 2.3.2.1 Changes to WITS2001 RFP Technical Rqts	
12	Referring to Figure C-4 of Section C.1.3, basic service prices also shall consist of a local access connection, local transport, and an Interexchange Carrier (IXC) access component.	B.1.3 Price Categories	
13	Basic service prices shall not contain any other charges, including taxes or the WITS Program Associated Government Fee that may apply. Pre-subscribed Inter-exchange Carrier charges (PICC), Subscriber Line Charges (SLCs), and Universal Service Fund (USF) obligations, or other regulatory commitments shall not be included in the basic service price but shall be itemized in Table B-0.6.	B.1.3 Price Categories 2.3.2.1 Changes to WITS2001 RFP Technical Rqts	
14	Table B-0.6 shall be completed and submitted with the offeror's proposal. Any other charges not included in this table as submitted by the offeror shall not be allowed for the term of this contract modification.	B.1.3 Price Categories 2.3.2.1 Changes to WITS2001 RFP Technical Rqts	
15	The contractor may also provide products and services that are within the scope of this contract but are not identified in the price tables. Charges for these services shall be considered "Other Direct Costs" (ODCs) and shall be established on an individual-case basis, in accordance with Section H.26 (Other Direct Costs).	B.1.3 Price Categories	
16	Time of Day. The Normal Business Day (NBD) is defined to extend from 7:00 a.m. to 7:00 p.m., Monday through Friday, excluding Federal holidays. Outside of Normal Business Day (ONBD) specifies all other times.	B.1.3.1 Price Sensitivity	
17	The geographic position of a customer's serving office and the IXC's Point of Presence (POP) shall be determined by their respective vertical and horizontal (V&H) coordinates. All distance measurements between serving offices shall be based on the airline distance between the locations involved. The distance between locations in miles shall be computed using the V&H coordinates	B.1.3.1 Price Sensitivity	

Rec. No.	Requirement	Requirements Reference	Compliance
	method set forth in the National Exchange Carrier Association (NECA), Inc., Tariff FCC No. 4. Fractions of a mile above one mile may be rounded up to the next whole mile before applying the rates.		
18	The V&H coordinates of the site, rather than its serving office, shall be the deciding factor in determining if the site is within the geographic scope of this contract; i.e., is within the WITS Program service area. Sites that are within the geographic scope but are connected to serving offices that are outside the geographic scope shall be billed as if they were connected to the nearest serving office within the WITS Program service area.	B.1.3.1 Price Sensitivity 2.3.2.1 Changes to WITS2001 RFP Technical Rqts	
19	The contractor may price proposed services using a maximum of 20 non-overlapping Rate Groups.	B.1.3.1 Price Sensitivity 3.5 Rate Groups	
20	The Government shall be able to issue service orders to serve a new building or to provide new services to an existing building using the prices established for that Rate Group.	B.1.3.1 Price Sensitivity 3.5 Rate Groups	
21	If the customer moves to a new Rate Group, the contractor shall change the Rate Group assignment at the time the move is completed, even if the customer's telephone number does not change (e.g., the customer may require Local Number Portability [LNP]).	B.1.3.1 Price Sensitivity 3.5 Rate Groups	
22	The Government requires flat-rate pricing for certain services, e.g., features, Directory Assistance, and CPE. For all other services, the offeror may specify the Rate Group within which the rates shall apply.	B.1.3.1 Price Sensitivity 3.5 Rate Groups	
23	The contractor shall propose one set of Rate Groups for all proposed services and products. The contractor is not required to provide all proposed services to each proposed Rate Group.	B.1.3.1 Price Sensitivity 3.5 Rate Groups	
24	The pricing for each service may include, unless otherwise stated, any appropriate combination of the following price elements: 2. Service Initiation Charge (SIC). This price element includes all one-time, initial charges (such as port-termination charges, if applicable) when a service, feature, or item of equipment is accepted.	B.1.3.2 Price Elements 2.3.2.1 Changes to WITS2001 RFP Technical Requirements	
25	The pricing for each service may include, unless otherwise stated, any appropriate combination of the following price elements: 3. Cancellation Charge (CC). The CC shall not exceed the SIC for that order when there is a SIC for that order.	B.1.3.2 Price Elements 2.3.2.1 Changes to WITS2001 RFP Technical Requirements	
26	The pricing for each service may include, unless otherwise stated, any appropriate combination of the following price elements: When there is no SIC charge, the CC shall be fair and reasonable. There shall be no CC when it is requested more than one week before the scheduled due date except in the cases of Video Teleconferencing Service and Audio Teleconferencing Service where users shall be permitted to cancel a teleconference 24 hours	B.1.3.2 Price Elements	

Rec. No.	Requirement	Requirements Reference	Compliance
	before the scheduled start time without incurring a CC.		
27	The pricing for each service may include, unless otherwise stated, any appropriate combination of the following price elements: 4. Disconnect Charge (DC). This price element includes one-time charges that may be incurred when a service is removed from service. The DC shall not exceed the SIC for that order.	B.1.3.2 Price Elements	
28	The Monthly Recurring Charge (MRC) shall begin on the date the service or equipment is accepted by the customer, in accordance with Section E (Inspection and Acceptance); end on the effective service disconnect date requested by the customer; and shall be prorated according to the number of days the service or equipment item is available.	B.1.3.2 Price Elements 2.3.2.1 Changes to WITS2001 RFP Technical Requirements	
29	The pricing for each service may include, unless otherwise stated, any appropriate combination of the following price elements: Usage charges shall not be sensitive to distance.	B.1.3.2 Price Elements	
30	The pricing for each service may include, unless otherwise stated, any appropriate combination of the following price elements: 12. Finance Charges. The contractor shall provide financing for any nonrecurring charges incurred under the WITS Program contract modification including SIC charges and Customer Premises Equipment (CPE) charges. This financing shall be available under the following terms: a) The period of the loan, at the customer's option, shall range from three months to sixty months, in increments of one month.	B.1.3.2 Price Elements 2.3.2.1 Changes to WITS2001 RFP Technical Rqts	
31	The pricing for each service may include, unless otherwise stated, any appropriate combination of the following price elements: This financing shall be available under the following terms: There shall be no required down payment. However, if the Government chooses to make a down payment, it shall be able to do so without penalty.	B.1.3.2 Price Elements	
32	The pricing for each service may include, unless otherwise stated, any appropriate combination of the following price elements: This financing shall be available under the following terms: c) There shall be no required points to acquire the loan.	B.1.3.2 Price Elements	
33	The pricing for each service may include, unless otherwise stated, any appropriate combination of the following price elements: This financing shall be available under the following terms: d) If the payback period of a loan extends beyond the termination date of the WITS Program contract modification, the loan shall be repaid in accordance with Section H.27 (Lease Termination).	B.1.3.2 Price Elements 2.3.2.1 Changes to WITS2001 RFP Technical Rqts	
34	The pricing for each service may include, unless	B.1.3.2 Price Elements	

Rec. No.	Requirement	Requirements Reference	Compliance
	otherwise stated, any appropriate combination of the following price elements: This financing shall be available under the following terms: e) If the contractor financing is used to purchase CPE, then title to that CPE shall transfer to the customer upon acceptance of the CPE and the contractor shall retain a security interest in that CPE until the loan has been repaid.		
35	The pricing for each service may include, unless otherwise stated, any appropriate combination of the following price elements: This financing shall be available under the following terms: f) The customer may buy out the loan in whole or in part at any time, and there shall be no prepayment penalty. In no case shall the amount of the buyout exceed the unpaid balance.	B.1.3.2 Price Elements	
36	The pricing for each service may include, unless otherwise stated, any appropriate combination of the following price elements: This financing shall be available under the following terms: g) The Monthly Payment Factor, as a function of the number of monthly payments, (2 < N < 61), and the monthly interest rate I, shall be: Monthly Payment Factor = $I / (1 - [1 + I]^{-N})$ The value of the Monthly Payment Factor used to calculate the required monthly payment shall be rounded to five decimal places.	B.1.3.2 Price Elements	
37	The pricing for each service may include, unless otherwise stated, any appropriate combination of the following price elements: This financing shall be available under the following terms: h) The required Monthly Payment of the item, exclusive of taxes, shall be the product of its capital cost and the above Monthly Payment Factor.	B.1.3.2 Price Elements	
38	The pricing for each service may include, unless otherwise stated, any appropriate combination of the following price elements: This financing shall be available under the following terms: i) The monthly interest rate for existing loans shall be fixed over the duration of each WITS2001 loan. The maximum monthly interest rate, I, that the contractor shall charge for new loans may be changed once a month after contract award in accordance with the formula: $I \leq (\text{Treasury Constant Maturity Rate} + \text{Margin}) / 12$ , where Treasury Constant Maturity Rate = The most recent monthly Treasury Constant Maturity rate published in the Federal Reserve Statistical Release G.13 ( <a href="http://www.federalreserve.gov/release/g13">http://www.federalreserve.gov/release/g13</a> ) U.S. Treasury Constant Maturities having the same duration of the prospective new loan. Note that the contractor may charge less than this maximum interest rate on any new loan but may not charge more. The contractor shall inform the GSA	B.1.3.2 Price Elements 2.3.2.1 Changes to WITS2001 RFP Technical Rqts	

Rec. No.	Requirement	Requirements Reference	Compliance
	<p>Administrative Contracting Officer of a change in the value of I within five business days after publication of Release G.13 or wait until the next month. The other term in this upper bound is: Margin = The annualized percentage amount above the Treasury Constant Maturity Rate required by the contractor to provide the required financing. The Margin shall be negotiated prior to contract award and shall remain fixed through the life of the WITS2001 contract. The offeror shall list in Table B-2 the Margin above Treasury Constant Maturity Rate that will be required as a function of the duration of a new loan. When the duration of the loan is between three and 60 months but is not the same as any of the values quoted in Table B-2 or Release G.13 for U.S. Treasury Constant Maturities, the contractor shall establish the values of I and M through a process of linear interpolation, based on the interest rates for U.S. Treasury Constant Maturities quoted in Release G.13 and margins quoted in Table B-2 having durations just below and just above the duration of the loan in question.</p>		
39	<p>WITS Program services shall be priced as follows: The price of installation shall be the sum of the SIC charges for local access, features, inside wiring (if required), and CPE (if required). The Monthly Recurring Charge shall be the sum of the MRCs associated with local access, features, and CPE (if required). For DTS only, there may be an MRC associated with the local transport component.</p>	<p>B.1.4 Instructions for Pricing 2.3.2.1 Changes in WITS2001 RFP Management and Operations Rqts</p>	
40	<p>The contractor shall provide all prices in the format and structure defined herein. Although the contractor may not propose any additional price elements not included in the defined format and structure, he or she is not required to use each price element available. Where charges do not vary by year, time-of-day, etc., the contractor's price entries for each similar element shall be the same. Where the contractor's charges do not vary by usage or distance, or there is no SIC or MRC or hourly charge, price entries shall be set to zero. The price items that are "not separately priced" and are included as part of the basic service shall be identified in the price tables as "NSP." Price items that are "not applicable" or "not allowed" are identified by the Government as "N/A."</p>	<p>B.1.4 Instructions for Pricing</p>	
41	<p>Items that are "Not Commercially Available," as this term is defined in Section J.12 of the RFP, or "Not Available" from the contractor during the contract year under consideration for other reasons shall be identified as "NCA" or "NA." Such entries will be marked "red" in the price tables to remind the offeror to provide supporting evidence in a document entitled Items That Are Not Commercially Available</p>	<p>B.1.4 Instructions for Pricing 2.3.2.1 Changes to WITS2001 RFP Technical Rqts</p>	

Rec. No.	Requirement	Requirements Reference	Compliance
	or Not Available for Other Reasons.		
42	The contractor shall provide a document, entitled Instructions for Pricing, that is available on the WITS Program Web site and provides detailed procedures for applying the contractor's price tables. The document shall provide the capability for a user to compare services of interest (e.g., VTS provided via CSD or DTS) without the need to understand the complexity of the underlying price components. It shall also provide the user with the information necessary to understand these price components.	B.1.4 Instructions for Pricing 2.3.2.1 Changes in WITS2001 RFP Technical Rqts	
43	The contractor's Instructions for Pricing shall be updated as necessary so that any prices provided in this document remain equivalent to the actual component prices provided in the price tables of the contract.	B.1.4 Instructions for Pricing	
44	Any service delivered under this contract, for which a price is not specifically identified by the contractor, shall be considered to be included in the price of another item or provided at no cost to the Government. However, the contract may be amended to add CLINs to properly deliver a product or service if there has been an omission.	B.1.5 Service Prices All Inclusive	
45	When the Government requires an analog SVS or BRI SDP to be located on customer premises at a point other than the MPOP and the inside wiring is unsatisfactory, the contractor will incur additional costs. The Government has established CLINs for the inside wiring in Section B.10.1, assuming the existing inside wiring is unsatisfactory but there is a satisfactory access from the MPOP to the SDP. Otherwise, inside wiring shall be priced on an individual case basis.	B.10. Additional Price Tables	
46	Prices for the necessary network termination equipment shall be provided as a function of the service and the type of CPE. For example, the contractor may have to provide a router if the customer orders FRS to interface with an Ethernet LAN.	B.10. Additional Price Tables	
47	In Section B.10.3, CLINs for other charges that may be incurred under the WITS Program contract modification shall be priced. In Sections B.10.4 and B.10.5, CLINs for required network equipment and CPE shall be priced.	B.10. Additional Price Tables 2.3.2.1 Changes to WITS2001 RFP Technical Rqts	
48	Table B-42 pertains to the vertical wiring from the MPOP to the Intermediate Distribution Frame (IDF), including the MPOP frames, cross-connects, and terminations; and Table B-48 pertains to the horizontal wiring from the IDF to the SDP, including IDF frames, cross-connects, and terminations. These tables shall be used to price the connection from the MPOP to the SDP as a function of the type of Inside Distribution Cable (IDC) used and the distance. The wiring shall meet the specifications of	B.10.1 Inside Wiring	

Rec. No.	Requirement	Requirements Reference	Compliance
	Section C.2.1.2 (Inside Wiring).		
49	The contractor shall interface with certain generic CPE types that do not have the native protocol and/or interface of the service under consideration (e.g., FRS, ATM, or SMD). The contractor shall provide prices for the Contractor-UNI-to-Client-UNI Conversion devices specified in Table B-44. If a DSU/CSU is required, it shall be provided as CPE and priced in accordance with Table B-48 (Purchase, Installation, Deinstallation, and Maintenance of CPE).	B.10.2 Contractor UNI to Client UNI Conversion 2.3.2.1 Changes to WITS2001 RFP Technical Rqts	
50	The contractor shall price other charges in the format shown in Table B-45, in accordance with the guidelines of Section B.1.3.	B.10.3 Other Charges	
51	Table B-46 describes how National Security and Emergency Preparedness (NS/EP) features shall be priced.	B.10.3 Other Charges	

Table B-4.9 below indicates compliance with specific IAS technical requirements and provides a cross-reference to the proposal response.

**Table B-4.9, Stipulated Services and Products Compliance Checklist: IAS**

Rec. No.	Requirement	Requirements Reference	Comply? (Yes/No)	Proposal Reference
1	The connection from the customer's SDP to the contractor's IAS serving office shall be priced separately using the appropriate WITS Program service (e.g., SVS, CSD, DTS, FRS, ATM, SMD, DSL, or wireless).	B.9 IAS 2.3.2.1 Changes to WITS2001 RFP Technical Rqts		1.2.1
2	IAS ports shall be priced in Table B-39 as a function of the peak data rate(s) that the offeror proposes to support.	B.9.1 UNI, 2.3.2 Changes to RFP Rqts, 3.4 Price Response		2.0
3	The Internet Access Service features shall be priced in accordance with Tables B-40 and B-41.	B.9.2 Features, 3.4 Price Response		2.0
4	IAS shall allow customers to interconnect CPE using the TCP/IP protocol suite and interoperate with other Government networks, such as the FTS2001 Internet Protocol Internetworking Service (IPS), CINEMA, Energy Sciences Network (ESNet), DISN (as needed and in accordance with security policy), and the public Internet Service Provider (ISP) networks.	C.2.9 Internet Access Service (IAS)		1.2.1
5	The contractor shall provide IAS ports at the peak data rates specified by the customer and shall use appropriate WITS Program services (e.g., dial-up SVS analog data service, dial-up ISDN, DTS, FRS, ATM, or SMD) to connect customers' SDPs to the contractor's IAS service office(s).	C.2.9.1 Basic Service Capabilities 2.3.2.1 Changes in WITS2001 RFP Technical Rqts		

Rec. No.	Requirement	Requirements Reference	Comply? (Yes/No)	Proposal Reference
6	These access circuits shall support TCP/IP-based applications that conform with the specifications of the Internet Standards (STDs) and the Request for Comments (RFCs) of the Internet Engineering Task Force (IETF).	C.2.9.1 Basic Service Capabilities	■	1.2.1
7	The following capabilities shall be provided as part of the basic service: 1. Unlimited access to the Internet 24 hours a day, 7 days a week.	C.2.9.1 Basic Service Capabilities	■	1.2.1
8	The following capabilities shall be provided as part of the basic service:2. Two or more redundant paths from the contractor's network to the Internet, each at the level of DS3 or higher.	C.2.9.1 Basic Service Capabilities	■	1.2.1
9	The following capabilities shall be provided as part of the basic service:3. Established public peering arrangements from the contractor's network to the Internet, such as at the Commercial Internet eXchange (CIX) and the Merit Access Exchange (MAE) East Network Access Point (NAP).	C.2.9.1 Basic Service Capabilities	■	1.2.1
10	The following capabilities shall be provided as part of the basic service:4. Private peering arrangements established from the contractor's network with redundant links to connect to its private peering partners.	C.2.9.1 Basic Service Capabilities	■	1.2.1
11	The following capabilities shall be provided as part of the basic service:5. Access control provided by the contractor's network to ensure that the only incoming connections to WITS Program IAS SDPs are from authorized users.	C.2.9.1 Basic Service Capabilities 2.3.2.1 Changes in WITS2001 RFP Technical Rqts	■	1.2.1
12	The following capabilities shall be provided as part of the basic service:7. Support for the Government assigned and InterNIC registered IP addresses and domain names.	C.2.9.1 Basic Service Capabilities	■	1.2.1
13	The following capabilities shall be provided as part of the basic service:8. Primary and Secondary Domain Name Service to provide an authoritative name server for the customer's IAS.	C.2.9.1 Basic Service Capabilities	■	1.2.1
14	The contractor shall provide the following features:3. Electronic Mail Service. The contractor shall provide and manage individual mail accounts using Simple Message Transfer Protocol (SMTP), Post Office Protocol (POP), and Internet Messaging Access Protocol (IMAP) standards. The e-mail service shall support Multipurpose Internet Mail Extension (MIME) for application-specific binary attachments.	C.2.9.2 Features	■	
15	The contractor shall provide the following features:4. Web Hosting. The contractor shall provide a Web hosting service to host Government web pages. The Web hosting	C.2.9.2 Features	■	

Rec. No.	Requirement	Requirements Reference	Comply? (Yes/No)	Proposal Reference
	service shall be accessible 24 hours per day, seven days per week via: a) Shared server(s) and/or b) Dedicated server(s)			
16	The contractor shall provide the following features:5. Web Authoring. The contractor shall provide an hourly rate to assist the Government in the development of Web pages and services.	C.2.9.2 Features		
17	The contractor shall provide the following features:7. Firewall Security Service. The contractor shall provide a firewall service which shall provide a completely transparent access process, including firewalls, management tools, integrity checkers, and intruder alarms. The firewall system shall be 100% Internet compatible. Individual IAS circuits may have different requirements for the Firewall Security Service feature. Offerors may propose additional CLINs (see Section B.10.6) for such firewall capabilities as virus scanning, site-to-site encryption, or url/java/active-x filtering. Such features will be evaluated for reasonableness.	C.2.9.2 Features 2.3.2.1 Changes to WITS2001 RFP Technical Rqts		1.3
18	The contractor shall provide the following features:8. Border Gateway Protocol (BGP). The contractor shall provide support for the border gateway protocol for WITS Program customers with registered Autonomous System (AS) numbers.	C.2.9.2 Features 2.3.2.1 Changes to WITS2001 RFP Technical Rqts		1.2.1
19	The contractor shall provide the following features:11. Network News Transfer Protocol (NNTP) News Feed. The contractor shall provide as a feature a Usenet news feed and shall describe the Usenet NNTP news feeds that will be provided in its technical proposal. WITS Program customers shall be able to choose whether to access the contractor's news feed server or to have the news feeds downloaded by the contractor to the customer's server.	C.2.9.2 Features 2.3.2.1 Changes to WITS2001 RFP Technical Rqts		1.2.1
20	The contractor shall provide the following features:13. Periodic Reports. The contractor shall provide the capability to deliver special reports detailing the performance of IAS connections for individual customers in accordance with Sections G.2.2.2 and G.2.2.3. The periodic reports described in Section G.2.1.7 shall include IAS activity and shall be provided as part of the basic service.	C.2.9.2 Features 2.3.2.1 Changes to WITS2001 RFP Technical Rqts		1.2.1
21	The contractor shall provide the following features:15. Dialup backup of dedicated ports. Transmission shall be provided separately using:	C.2.9.2 Features		

Rec. No.	Requirement	Requirements Reference	Comply? (Yes/No)	Proposal Reference
	a) SVS at a rate of 56 kb/s			
22	The contractor shall provide the following features:15. Dialup backup of dedicated ports. Transmission shall be provided separately using: b) ISDN BRI at a peak data rate of 64 kb/s	C.2.9.2 Features		
23	The contractor shall provide the following features:15. Dialup backup of dedicated ports. Transmission shall be provided separately using: c) ISDN BRI at a peak data rate of 128 kb/s	C.2.9.2 Features		
24	The contractor shall provide the following features:16. Electronic Directory Service. The contractor's Electronic Directory Service feature, at a minimum, shall provide: a) The e-mail address of WITS Program IAS subscribers, b) International white page directory service, and c) Support of the Lightweight Directory Access Protocol (LDAP) (RFC 1588).	C.2.9.2 Features 2.3.2.1 Changes to WITS2001 RFP Technical Rqts		
25	The contractor shall provide the following features:18. Service Level Guarantee. If the customer experiences an outage of at least 30 minutes in any 24-hour period, that customer shall receive one day's service credit.	C.2.9.2 Features		1.2.2
26	The following additional features shall support the customer's intranet service requirements: 1. Intranet Access Control Facilities to ensure that only authorized users are allowed on the customer's intranet.	C.2.9.2 Features		1.2.1
27	The following additional features shall support the customer's intranet service requirements:2. Service Assurance. This feature shall improve the availability of the customer's intranet connections as specified below by using such approaches as automatic restoration and reconfiguration: a) Availability: At least 99.7 percent, calculated	C.2.9.2 Features		1.2.2

Rec. No.	Requirement	Requirements Reference	Comply? (Yes/No)	Proposal Reference
	as described in Section C.2.1.10.4 b) Trouble identification: Less than 20 minutes c) Time to restore: Less than 2 hours			
28	5. The contractor's infrastructure shall support best commercial practices against unauthorized access and threats from hacker, criminal, and terrorist activities. In addition, the contractor's infrastructure security shall comply with the OMB Circular A-130, which requires adequate security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.	C.2.9.3 Performance	■	1.2.1
29	6. Customer technical support shall be provided 24 hours per day, seven days per week. Support shall be available by toll-free phone and e-mail.	C.2.9.3 Performance	■	1.2.4
30	7. The contractor shall monitor the customer's connections and traffic 24 hours per day, seven days per week.	C.2.9.3 Performance	■	1.2.4
31	8. Continuity of Operation. The contractor shall provide disaster recovery to ensure that the Government's IAS is restored in cases of natural or other disaster situations. The contractor shall maintain and test the disaster recovery capability and include a description in the Contingency Plan (Sections C.6.4 and G.2.1.19).	C.2.9.3 Performance	■	1.2.1
32	9. Offerors shall propose a Service Level agreement regarding IAS in their proposal. Areas of interest to the Government include, but are not limited to, the throughput, response time, latency, rate of premature disconnects, and the service availability. The service availability shall be measured in accordance with Section C.2.1.10.4, and the other parameters shall be measured between any two SDPs located in the WITS Program service area. Offerors shall submit data characterizing their current IAS performance in their proposal. For each parameter reported, the measurement approach, reporting procedure, and approach for dealing with performance shortfalls shall be described. The contractor shall negotiate a Service Level Agreement with the Government prior to contract award. The contractor also shall negotiate individual Service Level Agreements to meet agency-specific requirements if requested by the GSA ACO.	C.2.9.3 Performance 2.3.2.1 Changes in WITS2001 RFP Technical Rqts	■	1.2.2
33	The contractor shall provide, at a minimum, IAS ports that support the following peak data rates: 56 kb/s via dial-up service	C.2.9.4.1 Line-Side Interfaces	■	

Rec. No.	Requirement	Requirements Reference	Comply? (Yes/No)	Proposal Reference
34	The contractor shall provide, at a minimum, IAS ports that support the following peak data rates: 64 kb/s via dial-up service	C.2.9.4.1 Line-Side Interfaces		
35	The contractor shall provide, at a minimum, IAS ports that support the following peak data rates: 128 kb/s via dial-up service	C.2.9.4.1 Line-Side Interfaces		
36	The contractor shall provide, at a minimum, IAS ports that support the following peak data rates: 56/64 kb/s	C.2.9.4.1 Line-Side Interfaces		1.2.1
37	The contractor shall provide, at a minimum, IAS ports that support the following peak data rates: 128 kb/s	C.2.9.4.1 Line-Side Interfaces		1.2.1
38	The contractor shall provide, at a minimum, IAS ports that support the following peak data rates: 256 kb/s	C.2.9.4.1 Line-Side Interfaces		1.2.1
39	The contractor shall provide, at a minimum, IAS ports that support the following peak data rates: 512 kb/s	C.2.9.4.1 Line-Side Interfaces		1.2.1
40	The contractor shall provide, at a minimum, IAS ports that support the following peak data rates: 768 kb/s	C.2.9.4.1 Line-Side Interfaces		1.2.1
41	The contractor shall provide, at a minimum, IAS ports that support the following peak data rates: 1.536 Mb/s	C.2.9.4.1 Line-Side Interfaces		1.2.1
42	The contractor shall provide, at a minimum, IAS ports that support the following peak data rates: 4 Mb/s	C.2.9.4.1 Line-Side Interfaces		1.2.1
43	The contractor shall provide, at a minimum, IAS ports that support the following peak data rates: 10 Mb/s	C.2.9.4.1 Line-Side Interfaces		1.2.1
44	The contractor shall provide, at a minimum, IAS ports that support the following peak data rates: 16 Mb/s	C.2.9.4.1 Line-Side Interfaces		1.2.1
45	The contractor shall provide, at a minimum, IAS ports that support the following peak data rates: 34 Mb/s	C.2.9.4.1 Line-Side Interfaces		1.2.1
46	The contractor shall provide, at a minimum, IAS ports that support the following peak data rates: 45 Mb/s	C.2.9.4.1 Line-Side Interfaces		1.2.1
47	The contractor shall provide, at a minimum, IAS ports that support the following peak data rates: 100Mb/s	C.2.9.4.1 Line-Side Interfaces		1.2.1
48	The contractor shall provide, at a minimum, IAS ports that support the following peak data rates: 155Mb/s	C.2.9.4.1 Line-Side Interfaces		1.2.1

## 1.2 Required Narrative Responses Table B-2

Table B-2, Required Narrative Responses, is repeated below. It contains a proposal reference that indicates the number of the paragraph in this volume that addresses the requirement.

**Table B-2: Required Narrative Responses**

Record No.	Requirements Reference	Requirement	Proposal Reference
1	C.2 L.27.1.3, Items 3a) and 3d) through 3f)	The contractor shall describe the system architecture proposed for providing the proposed services or products to customers in the WITS Program service area, including the approach for: <ol style="list-style-type: none"> <li>1. Interconnecting with the contractor-provided serving offices, with the local exchange network, and with Government networks.</li> <li>2. Internetworking with other service providers.</li> <li>3. Providing access to all commercial telecommunications services that are now available or that become commercially available within the WITS Program service area throughout the life of the contract modification.</li> <li>4. Meeting the scalability and robustness requirements (Sections C.2.1.10.5 and C.2.1.10.2).</li> <li>5. Economically serving small customers.</li> <li>6. Maintaining compatibility with existing WITS Program CPE.</li> </ol>	1.2.1
2	C.2 C.4 L.27.1.3, Items 2a) and 2b)	The contractor shall describe the quality of the proposed services and products with respect to the specifications of Sections C.2, C.4, and other quality of service metrics used by the contractor. If Switched Voice Service or Circuit Switched Data Service is proposed, the contractor shall describe the approach proposed to provide service throughout the WITS Program service area.	1.2.2
3	C.3.2.3.2	The contractor shall specify standard, expedited, and emergency service availability intervals for the services and products proposed.	1.2.3
4	C.3.3 L.27.2.3.1, Item 1	The contractor shall describe any major changes planned in its operational support systems and indicate when they will be available.	1.2.4
5	C.3.3 C.6.1 C.6.4 L.27.2.3.1, Item 2b)	The contractor shall provide a draft Implementation Plan that describes how the proposed service will be implemented at existing and new WITS Program locations, how the plan will be updated to account for site-specific variations, how the Government will be kept informed of the status of implementation activities, and how the contractor will maintain and restore service during an emergency.	1.2.5
6	C.3 L.27.2.3.1, Item 2	The contractor shall describe any other major changes that are planned in its management and operations approach to meet WITS Program requirements and indicate when they will be completed.	1.2.6
7	C.7 1.4	The contractor shall offer any suggestions he or she may have to establish and maintain an effective partnership relationship with GSA.	1.2.7

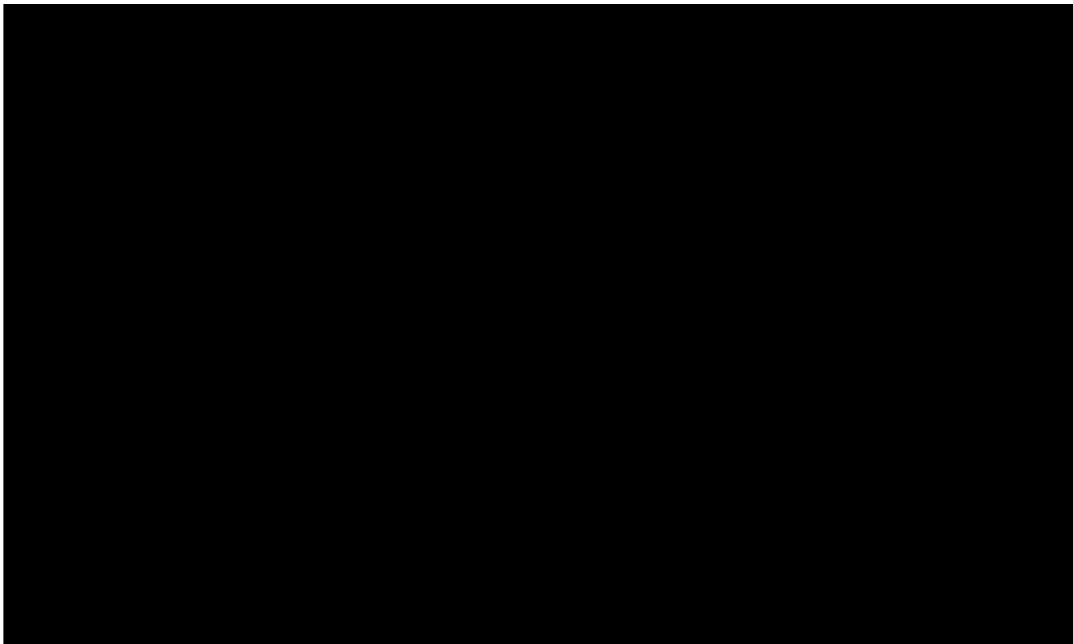
### 1.2.1 Proposed System Architecture

Qwest proposes to provide Dedicated Internet Access Service (DIA) to support Federal users in the National Capital Region. The IAS service will be provided over an in-place fiber optic infrastructure already installed in the Washington DC area.

#### Qwest Backbone Network for WITS

The fiber optic infrastructure that will provide the IAS consists of the Qwest Nationwide Fiber Optic Network and the Qwest Local Access Metropolitan Area Network installed in the DC area. Qwest has an in-place IP network infrastructure that resides on the Qwest Nationwide Network and a Local Access Washington Area Network. **Figure 1,**

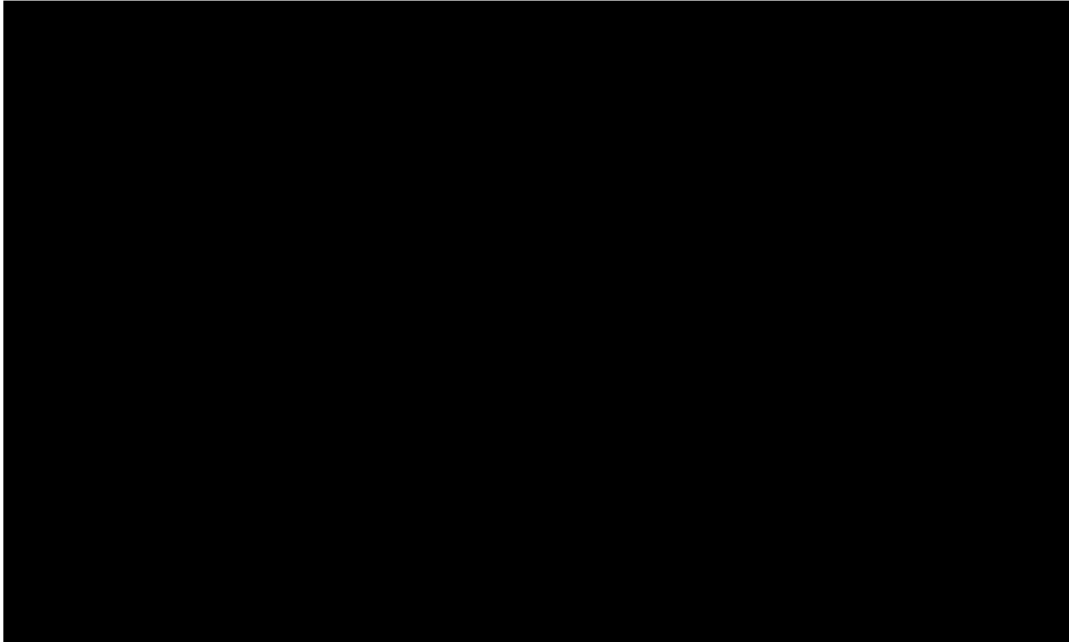
, depicts the Qwest network that will serve the WITS customer base.



**Figure 1:** 

Qwest has built the world's most advanced network from the ground up. Utilizing the latest in optical fiber, opto-electronics and data networking technologies, Qwest provides the most cost-effective and reliable communication services available today. Using state-of-the-art Dense Wavelength Division Multiplexing (DWDM) OC-192 transmission equipment, each of Qwest's 48 fibers along its route can carry over 600 Gbps today. The Qwest Nationwide Network uses a four-fiber, bi-directional line switched ring (4F-BLSR) SONET architecture. This self-healing network design virtually eliminates network downtime for customers ensuring ultra-high availability.

Qwest's [REDACTED] illustrated in **Figure 2**, [REDACTED] spans approximately 20,000 route miles in the United States. Qwest engineers designed our network utilizing Lucent's state-of-the-art fiber, Nortel transmission electronics to meet the needs of data transmission demands of the future.



**Figure 2:** [REDACTED]

Qwest's nationwide network is almost entirely located on privately owned railroad right-of-ways (ROWs). Qwest has buried two High-Density Polyethylene (HDPE) conduits along each route to a depth of approximately four feet and four feet from the railroad track. To expedite conduit installation, Qwest uses a state-of-the-art rail plow to efficiently lay the conduit. Not only does the rail plow bury the conduit, it also buries a locator tape two feet above the conduit to indicate that conduit and fiber are in the ground. Qwest worked to a very aggressive schedule to lay approximately 20,000 miles of conduit in less than three years. The current fiber cable occupies only *one-fourth* of the capacity of the buried conduit. Planning for the future, Qwest installed two conduits providing room for future expansion in fiber count and fiber technology.

Qwest's comprehensive approach when building the Macro Capacity Fiber Optic Network allowed us to utilize Nortel transport equipment with its Dense Wavelength Division Multiplex feature. DWDM allows Qwest to simultaneously send sixteen separate wavelengths on the same fiber at OC-192 (10 Gbps) for a total of 160 Gbps per fiber. In the near future, Qwest will be able to increase the capacity of the fiber to 32 wavelengths without major equipment upgrades. The Qwest Nationwide Network is composed of multiple rings that are connected by multiple Transfer PoPs located on common points of intersecting rings. [REDACTED] is located directly

on a major ring of the Qwest Fiber backbone. There are a number of Qwest primary PoPs located in [REDACTED].

The Qwest Local Access Metropolitan Area Network provides secure, high-speed local access connections that transport traditional Qwest communications products to the Qwest backbone. It provides direct broadband access to large organizations with bandwidth-intensive applications such as bundled data and voice, and those that require high-capacity connectivity between multiple sites within a city and to our fiber optic network. Qwest offers a variety of access speeds from DS1 (1.544 Mbps) to OC-48 (2.4 Gbps). Qwest has included a detailed description of the network infrastructure in the WITS Eligibility proposal.

Qwest proposes to provide IAS to Federal customers in the National Capital Region served by the WITS contract. The service offers worldwide IP connectivity and Internet Access. The service will utilize the Qwest Nationwide IP Network for IP transport and access to Internet public and private peering points. Access to Federal sites will be via Qwest Local Access or Local Exchange Carriers (LECs) in the Washington DC. Federal sites will be connected to the [REDACTED] Qwest Nationwide Network.

Qwest already has Qwest Local Access installed in many facilities in the Washington DC area including the [REDACTED]. Qwest also has agreements and infrastructure in place to connect Washington DC customers to the Qwest Network using connections provided by [REDACTED]

The [REDACTED] is illustrated in **Figure 3**, [REDACTED]. The network is superimposed on the Qwest SONET ring backbone and consists of [REDACTED] interconnected IP TeraPoPs that serve every LATA in the Continental United States.  
[REDACTED]

---

Figure 3: [REDACTED]

Each TeraPoP is configured as shown in **Figure 4, Qwest TeraPoP Architecture**. This architecture provides a fully path diverse route between each TeraPoP and at least two other TeraPoPs on the nationwide network.

To ensure availability in excess of [REDACTED] on the IP Backbone, Qwest utilizes:

- ▶ MPLS Fast Reroute – Layer 3 protection to ensure redundancy
- ▶ Auto-Protect Switching (APS) – Provided by redundant core IP backbone routers with optical connections between them.
- ▶ Ultra Reliable Power and Cooling – Telco Grade Buildings with battery backup and power generators
- ▶ Geographically Diverse Peering – Multiple paths to other IP networks with ability to dynamically choose the highest quality path

Qwest currently supports over [REDACTED] peering arrangements across Europe and North America and maintains peering agreements with all major national Internet service providers to exchange traffic at public Network Access Points (NAPs). We also exchange traffic at private peering locations throughout our infrastructure with national and international Internet service providers, making Qwest one of the largest international Internet backbone providers worldwide.

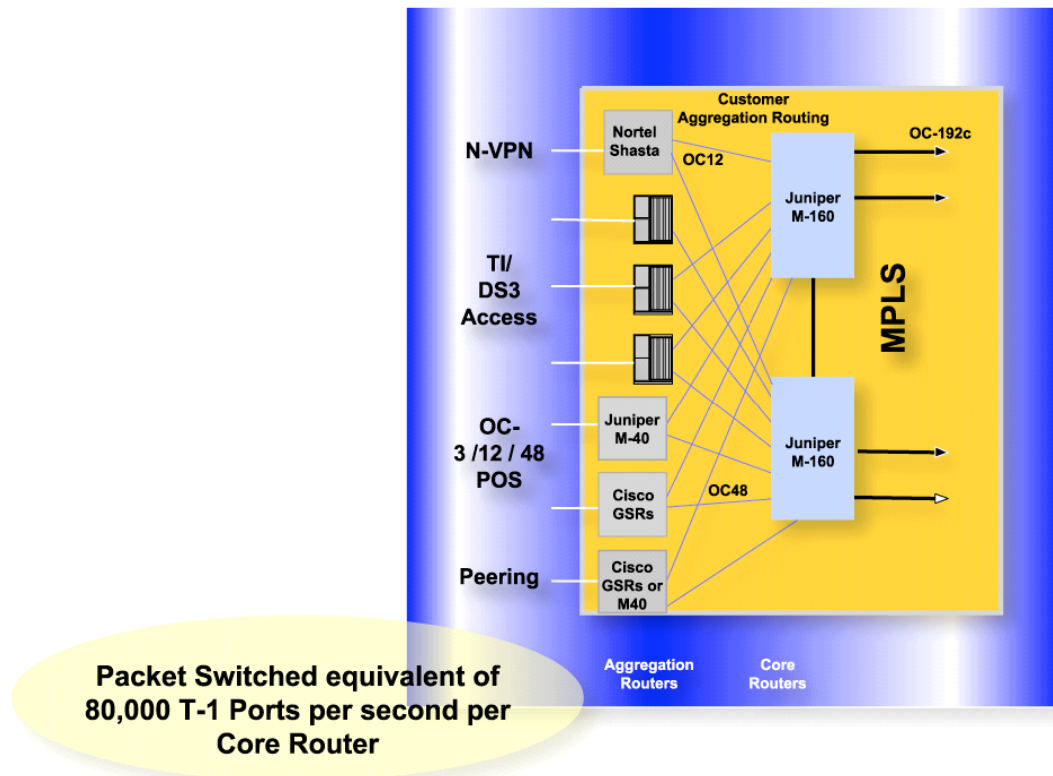


Figure 4: Qwest TeraPoP Architecture

Qwest also utilizes “Cold Potato” routing that keeps requests on the Qwest backbone to the peering point closest to the target Internet site. Most competitive Internet Access networks utilize “Hot Potato” routing to move the traffic off of their network at the nearest peering point to minimize traffic on their network. Qwest uses “Cold Potato” routing to provide maximum access speed to all sites, especially European sites, and to help ensure that we maintain our guaranteed SLA performance levels.

### BGP Service and Peering Requirements

Qwest provides Intermediate System to Intermediate System (IS-IS) as the interior routing protocol on the Qwest IP network, with mBGP as the external gateway routing protocol. The Qwest network is able to support high-speed IP tunneling across the network. Qwest maintains peering agreements with all major national Internet service providers to exchange traffic at public Network Access Points (NAPs).



In order to enable the service, each site must connect to the service through an integrated access device, access concentrator or router. **Figure 5, IAS Customer Interfaces**, illustrates the interfaces available at customer locations to provide connectivity to provide a wide array of connections at various speeds.

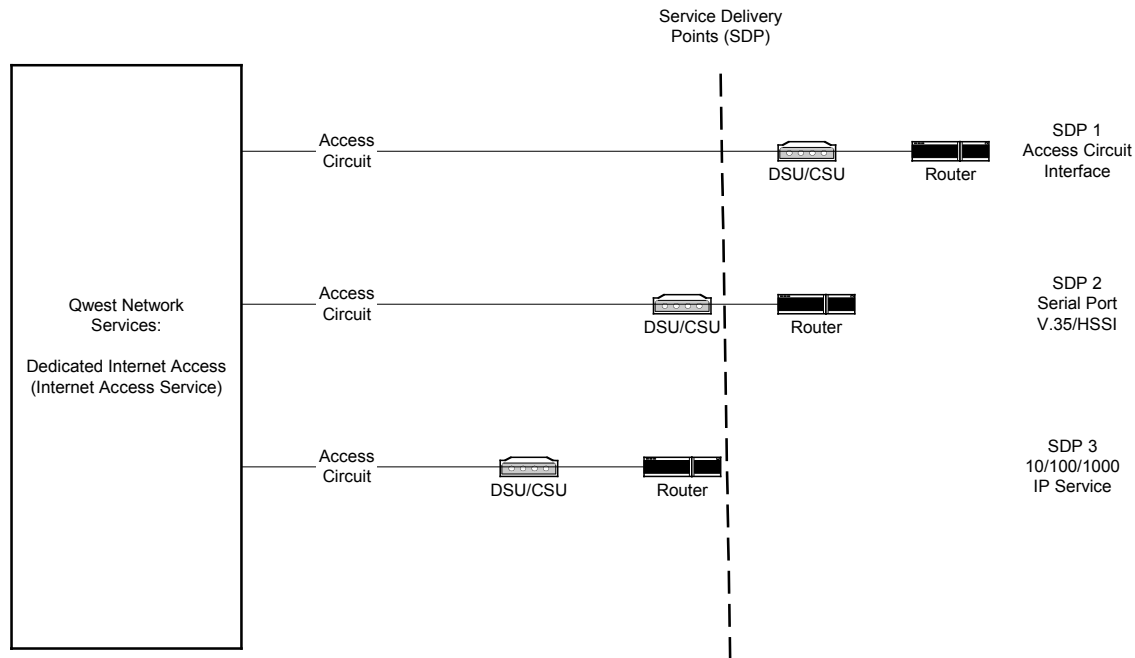


Figure 5: IAS Customer Interfaces

For normal IAS, Qwest can supply the following User Network Interfaces (UNIs) Service Delivery Points (SDPs): RJ-48, V.35, HISSI, Coax, FC or SC fiber or BaseT Ethernet. The SDPs are specified in Figure 5.

User to Network Interfaces (UNIs) are defined as service delivery points for the termination of Qwest network services at user locations. In order to enable the service, each site must connect to the service through a Qwest provided UNI.

UNIs are the interfaces through which the customer receives the traffic at the SDP. UNIs are defined at speeds between Fractional T1 and OC12 for IAS service. The tables below define the different SDPs, service speeds and corresponding UNIs. UNIs will consist of metallic, coax, optical, serial or 10/100 BaseT Ethernet. The SDPs categorized into SDP 1, SDP 2 or SDP 3. SDP 1 defines the interface with no customer premises equipment provided. SDP 2 defines a serial interface that is either V.35 or HSSI as required. SDP 3 defines a 10/100 BaseT Ethernet interface that is provided by a Cisco router or equivalent.

Interface definitions are provided in **Table 2, IAS SDP Definition**.

**Table 2: IAS SDP Definition**

<b>SDP</b>	<b>Description</b>
SDP 1	Defines the standard demarcation provided by the access provider which is an RJ48 for T1/FT1, coax for DS3 and optical for OCn services.
SDP 2	V.35 for T1/FT1 services are provided through an integrated access device. HSSI interface is provided by an access multiplexer or DSU/CSU 44.736Mbps. There is no UNI 2 defined for OCn services. All units are stand-alone requiring AC power at the customer location.
SDP 3	Provides a 10/100/1000 BaseT Ethernet interface through a router located at the customer location. The router contains the DSU/CSU functionality. All units are stand alone requiring AC power at the customer location.

Interfaces to be provided are summarized in **Table 3, IAS UNI Interfaces**. The table indicates the appropriate SCIDs for non-recurring and monthly recurring charges associated with each IAS option.

**Table 3: IAS UNI Interfaces**

<b>Interface</b>	<b>Item description</b>
Metallic T1/FT1	RJ Type Interface
Coax DS3 IAS	Coaxial cable assembly
Optical OCn IAS	Optical cable assembly
v.35 T1/FT1	Kentrox 651 Satellite T1 DSU/CSU or equivalent
HISSI DS3	Kentrox T3/E3 IDSU Multi Rate AC, P/N 15951 or equivalent
10/100 T1/Tiered	LAN port on a Cisco 1721router or equivalent
10/100 NxT1/Tiered	LAN port on a Cisco 3640 router or equivalent
10/100 DS3/Tiered	LAN port on a Cisco 7204 or equivalent
10/100 OC3/Tiered	LAN port on a Cisco 7204 router or equivalent
10/100 OC12 /Tiered	LAN port on a Cisco 7204 router or equivalent
Gigabit Ethernet OC48 /Tiered	LAN port on a Cisco 7304 or equivalent

Qwest's IP network is monitored from the World Wide Data Operations Center (WDOC) in [REDACTED], on a 24 hours per day basis every day of the year. WDOC/NOC responsibilities include:

- ▶ Monitoring the state of the network and hosted systems, local or remote
- ▶ Reacting to downed or crippled conditions on monitored systems
- ▶ Handling open tickets
- ▶ Managing the backup operations of hosted clients

- ▶ Maintaining and controlling access into the NOC
- ▶ Adhering to cabling and hosted system standards
- ▶ Providing consultative services to pre-sales, installation/relationship management, and sales on an as-needed basis
- ▶ Managing project plans as they relate to handoffs from installation services, large moves, etc.
- ▶ Providing resources as needed within the Operations group for special projects as deemed necessary by management
- ▶ Providing a feedback mechanism to the internal groups for policy enhancements, systems enhancements, or suggestions to further increase customer satisfaction

The WITS Customer Service Center (CSC) will be a customer's first point of contact with Qwest. Trouble tickets can be called into the WITS CSC or can be entered into Qwest Control, a web based user interface that is described in the Eligibility Proposal. The WITS CSC will task the WDOC to respond to all trouble tickets to resolve problems. Network management, monitoring and trouble management will be performed by the IP Data Systems group with the WDOC.

Their responsibilities include:

- ▶ Serving as the conduit for all communications into either the WDOC, Relationship Management, Network Services, Engineering, and Sales within Qwest
- ▶ Opening [REDACTED] tickets for all customer outages, requests, and questions
- ▶ Serving as a customer advocate to ensure that all issues are resolved in a timely manner
- ▶ Managing the internal management escalation process
- ▶ Serving as the customer interface to communicate status on "pending/open" requests
- ▶ Communicating problem resolution to customers via the WITS CSC
- ▶ Serving as a communication liaison between all the groups within Qwest and customers through the WITS CSC
- ▶ Tracking and escalating all remedy issues as needed
- ▶ Fine tuning procedures to better suit customers' needs, within the rule sets established by Qwest Standard Operating Procedures
- ▶ Providing a feedback mechanism to the internal groups for policy enhancements, remedy enhancements, and any other suggestions to further increase customer satisfaction

The WDOC directs requests/problems to the appropriate Qwest service group as follows:

**First Level Support**—Problems/requests of all severity levels are initially routed to First Level Support (available 7x24x365).

**Technical Support**—Problems/requests that cannot be resolved via First Level Support are routed to Technical Support and/or, if appropriate, the applicable outside vendor. Technical Support is available on-site 8 AM-5 PM with personnel on call 7x24x365. The resolution of a problem focuses on the permanent repair or elimination of the cause of the problem, including a satisfactory explanation of the problem (and proposed resolution) back to First Level Support that remains the primary interface with the customer. If re-engineering is required, these services are provided at Qwest’s then-prevailing rates.

#### 1.2.1.1 Interconnecting with Serving Offices

Qwest has not proposed any hosting services as part of this initial IAS submittal. Qwest will submit a proposal for the balance of IAS functions in the near future that will provide web fileserver hosting in a Qwest CyberCenter. The proposed service does provide access to all Qwest CyberCenters.

#### 1.2.1.2 Interconnecting with Local Exchange Network

Qwest has interconnection agreements with other service providers in the Washington Capital region. We have numerous PoPs that provide interconnection between Qwest and other carriers including [REDACTED]. This provides Qwest with the capability to utilize these companies to provide connectivity between the Carrier and the nearest Qwest PoP to then provide IntraLATA services including IAS to the locations.

#### 1.2.1.3 Interconnecting with Government Networks

The Qwest IAS service connects with multiple private and public peering points. The system will connect to all commercial telecommunications services that are now available or that become commercially available within the WITS Program service area throughout the life of the contract modification provided they are accessible via the Internet.

#### 1.2.1.4 Internetworking with Other Service Providers

Qwest has interconnection agreements with other service providers in the Washington Capital region. We have numerous PoPs that provide interconnection between Qwest and other carriers including [REDACTED]. This provides Qwest with the capability to utilize these companies to provide connectivity between the Carrier and the nearest Qwest PoP to then provide IntraLATA services including IAS to the locations. In addition, we maintain peering points with numerous Internet Service Providers as summarized in **Table 1, Qwest Communications Peering Overview**.

#### 1.2.1.5 Providing Access to Commercial Telecom. Services

Qwest has access to Commercial Telecommunications services via the numerous peering points described in **Table 1, Qwest Communications Peering Overview**.

### Scalability and Robustness

The proposed IAS is available at the following speeds:

T-1/FT-1	Tiered/OC-3
NxT-1	Tiered/OC-12
Tiered/DS-3	Tiered/OC-48

Users can scale systems up or down via a change to the level of service ordered and a change to the UNI that connects the SDP to the network as outlined in **Table 3, IAS UNI Interfaces**. If an IAS connection is made to Qwest via a LEC, the bandwidth of the LEC connection may have to be increased or decreased.

#### 1.2.1.6 Economically Serving Small Customers

Qwest can provide IAS to large and small businesses at economical prices. Qwest has established relationships with LECs in the Washington DC area including

The in-place contracts and in-place PoP transfer points enable Qwest to provide the most cost effective service to any size organization.

#### 1.2.1.7 Maintaining Compatibility with Existing CPE

The Qwest offering includes three types of UNIs to connect to existing facilities. These include RJ, coax and fiber optic interfaces that easily interface with existing CPE. All Qwest UNIs are open standards based.

#### 1.2.1.8 Addressing Scheme

Qwest will support the Government assigned and InterNIC registered IP addresses and domain names. When using BGP Qwest will advertise the addresses that belong to the Government as required. It is the responsibility of the Government to SWIP Government owned addresses to their users.

Qwest Primary and Secondary DNS will provide authoritative name servers for the customer's IAS. This is configurable by the customer through Qwest Source and can be modified by the customer to add or delete Qwest provided authoritative name servers.

#### 1.2.1.9 News Feed

Qwest News Feed allows customers to request news feed services through Qwest and the service may provide a full or partial feed to your news server. Customers can specify a subset of news groups to be included in the feed. Qwest is running a The news feed service is configurable by the customer through Qwest Source.

#### 1.2.1.10 Access and Security

Within the Qwest network infrastructure, we provide filtering for Telnet and SNMP access to the Backbone routers, BGP access-lists to permit or deny the incurrence or propagation out of network advertisements, per-customer prefix filters to only accept their network advertisements, Blocking of Private AS advertisements, ACL's denying private IP address ranges both in and out. In the event of a DoS attack, we will implement temporary filters to stop the attack on the edge routers.

### 1.2.2 Quality of Proposed Services

Qwest has an established SLA for Domestic IAS Service.

[REDACTED]

[REDACTED] of the Monthly Recurring Charge for not meeting specified levels of Network Availability, Latency or packet delivery and [REDACTED] of credit for each instance where Qwest fails to notify a customer of a service outage within [REDACTED] of that occurrence. The target time to restore is [REDACTED].

Details for the proposed service are summarized below as extracted from the Qwest Global Internet Service Level Agreement.

**NETWORK AVAILABILITY**

Region	GOAL	REMEDY
[REDACTED]	[REDACTED]	[REDACTED]

**LATENCY**

Region: Intra U.S.	GOAL	ACTUAL LATENCY = REMEDY	
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

Region: Intra U.S.	GOAL	ACTUAL PACKET DELIVERY = REMEDY	
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

**REPORTING**

Region:	GOAL	REMEDY
[REDACTED]	[REDACTED]	[REDACTED]

**Components Included** - All components of the Qwest IP Network and the components of Qwest’s network partners in certain locations (e.g., PoPs, Routers, Circuits) are covered by this SLA, but local access/connection facilities used to access the Qwest IP Network or partner networks (i.e., the local loop or tail circuits) and any Qwest-provided UNIs and inside wiring are not. The Intra-U.S. region is limited to components of Qwest’s continental U.S. IP Network and the GSP Network, if applicable. The Intra Europe and Intra Asia-Pacific regions are limited to the relevant Qwest or partner network PoPs located in any particular Tier 1, Tier 2, or Tier 3 location.

**Measurement** – Network Availability. Network Availability is based on “Network Downtime,” which exists when a particular Customer IAS port (the "Affected Service") is unable to transmit and receive data and such failure is recorded in the trouble ticket system. Network Downtime is measured from the time the trouble ticket is opened to the time the Affected Service is again able to transmit and receive data.

**1.2.3 Service Availability Intervals**

The typical service interval to install IAS is 30-60 days using LEC provided connections to the nearest Qwest PoP location. In the event a customer wishes to utilize the Qwest Local Access Network, Qwest will evaluate feasibility and schedule required to bring Qwest Local Access into

the customer location. Qwest Local Access adds a fiber connection between a government location and the nearest Qwest Local Access route. The cable is actually spliced into the existing network making the government site a PoP on the Qwest Local Access network. This has the advantage of provide a bi-directional path from the government facility. In many cases we offer a path diverse route into a site to ensure maximum availability. If a customer is already in a location served by Qwest Local Access, service availability is [REDACTED].

#### 1.2.4 Operational Support Systems

The proposed IAS service will be supported by the WDOC in [REDACTED] on a 24 hours per day basis every day of the year. These are large, secure, disaster resilient facilities that reside directly on the Qwest backbone network and have fully redundant, route diverse connections to the network. The primary support system for IAS is Qwest Control<sup>sm</sup>.

Qwest Control is a Customer Network Management System that will be provided to WITS2001 IAS customers to view performance statistics and track the trouble ticket management process. A key part of Qwest Control is the ability of a customer to directly enter and monitor the status of trouble tickets. This virtually eliminates the confusion about how to report problems to Qwest as well as improving the quality of status information reported back to a customer. Please see <https://control.qwest.com> to see a demonstration of Qwest Control that will provide the look and feel of the system.

Qwest Control is a proprietary web-based application that provides customers with complete management control over a broad range of Qwest services including DIA, NVPN, ATM and Frame Relay services. Qwest Control allows customers to access a wide variety of network management and reporting tools via a secure website. All a customer needs to manage their communications with Qwest Control is a PC with Internet access, a certified browser, an enterprise ID, user name and password. The application is best viewed at 1024x768 resolution with 256+ colors. In order to use Qwest Control user PCs must be equipped with Microsoft Windows 95, 98 or NT and one of the following Web browsers:

- ▶ Microsoft Internet Explorer 5.0 or higher
- ▶ Netscape Navigator 4.08 or higher
- ▶ Netscape Communicator 4.7 or higher with the following settings:
  - Enabled cookies
  - Enabled Java
  - Enabled JavaScript
  - 40 Bit or 128 Bit SSL encryption

Qwest Control provides the following features and benefits:

- ▶ Saves money – Qwest Control can potentially reduce costs by eliminating the need for expensive, dedicated network management workstations. Qwest Control gives users the ability to monitor network usage and respond quickly to changing needs resulting in a streamlined network management process.

- ▶ Saves time – Qwest Control can save time by integrating communications network management tools in one easily accessible Web site. Qwest Control streamlines processes by eliminating the need for customers to work through their account team to generate reports or call toll-free numbers to access information about their networks.
- ▶ Manages networks efficiently – Qwest Control allows customers to efficiently manage their networks via real-time monitoring and trouble management tools ensuring rapid problem identification and resolution.
- ▶ Safeguards data – Qwest Control protects information with a level of security that customers demand. Qwest Control ensures privacy of customer network data through built-in security features including an account ID, unique user IDs and passwords for each employee.
- ▶ Resolves trouble – Customers can create and track trouble tickets on their Qwest network services. Qwest Control ensures timely resolution of problems by allowing customers to quickly isolate network problems and open trouble tickets. Customers also have the ability to track the status of opened tickets in real-time.


Qwest Control provides a comprehensive set of communications management tools, including:

- ▶ Statistics Manager - Allows customers to view historical and real-time network statistics, and create detailed reports.
- ▶ Trouble Manager - Enables customers to create and track the status of trouble tickets.
- ▶ Status Manager - Immediately reports network or service failures via an alarms list and interactive network map, keeping customers aware of the status and performance of their network. Customers can jump directly to Configuration and Trouble information from the network status map.
- ▶ Configuration Manager - Enables customers to view current network element configuration and manage network groups and service users.
- ▶ System Administration Manager - Allows customers to create and manage secure administrative profiles for their enterprise users.

### **Statistics Manager**

The Qwest Control Statistics Manager, available for DIA, NVPN, ATM and Frame Relay services, enables customers to view historical and real-time network statistics, and create detailed reports. ATM and Frame Relay customers can create performance and usage reports for Ports and PVCs for the last 90 days.

Users can select the appropriate Statistics Manager Service by selecting one of the blue boxes at the top of the screen. Service category statistics are provided by the Qwest Control Statistics Manager. The screen in Figure 6 below is used to select the type of report desired.


Friday, February 2, 2001

Control

HOME eBILLING INTERNET FRAME RELAY ATM VNS TOLL-FREE

Merger Notice

ABOUT CONFIGURATION TROUBLE MANAGEMENT STATISTICS

## Internet Statistics Report Selection

Internet > Statistics Report Selection

Qwest Control customers can generate various types of reports to monitor the health of their IP network components.

**Dedicated Internet Access(DIA)**

**At-a-Glance Reports**  
You can either view previously generated At-a-Glance Reports or generate your own reports on your Access Circuit.

**Trend Reports**  
You can either view previously generated Trend Reports or generate your own reports on your Access Circuit.

**Billing Reports**  
Currently available for Burstable Billing customers, these reports show a graphical representation of circuit usage during past billing cycles.

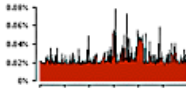
**Dedicated Hosting(DH)**

**At-a-Glance Reports**  
You can either view previously generated At-a-Glance Reports or generate your own reports on your Access Circuit.


**Trend Reports**  
You can either view previously generated Trend Reports or generate your own reports on your Access Circuit.

**Qwest IP Network Statistics**  
Monitor the latest statistics on our network including latency, packet loss, and availability.

**Sample At-a-Glance Report**



**Sample Trend Report**



**At-a-Glance Report** This report provides a one page summary of important performance indicators for a specific Access Circuit during a specified period of time. It also displays charts depicting indicators such as bandwidth utilization, volume in bytes, and element type-specific errors. It provides a global view of your network configuration.

**Trend Report** This report displays the behavior of variables that are specific to the Access Circuit. It allows you to generate reports on up to ten variables for a single Access Circuit or on a single variable, such as bandwidth utilization, for up to ten Access Circuits.

**Billing Report** Currently available for Burstable Billing customers, these reports show a graphical representation of circuit usage during past billing cycles. Data can also be downloaded in text format for further desktop analysis.

Figure 6: Internet Statistics Report Selection Screen

Reports can be daily, weekly, monthly or between specified date ranges. Users can select circuits to be evaluated as shown in **Figure 7** below. An example Statistics Report is shown in **Figure 8**.

Figure 7: Report Definition Screen

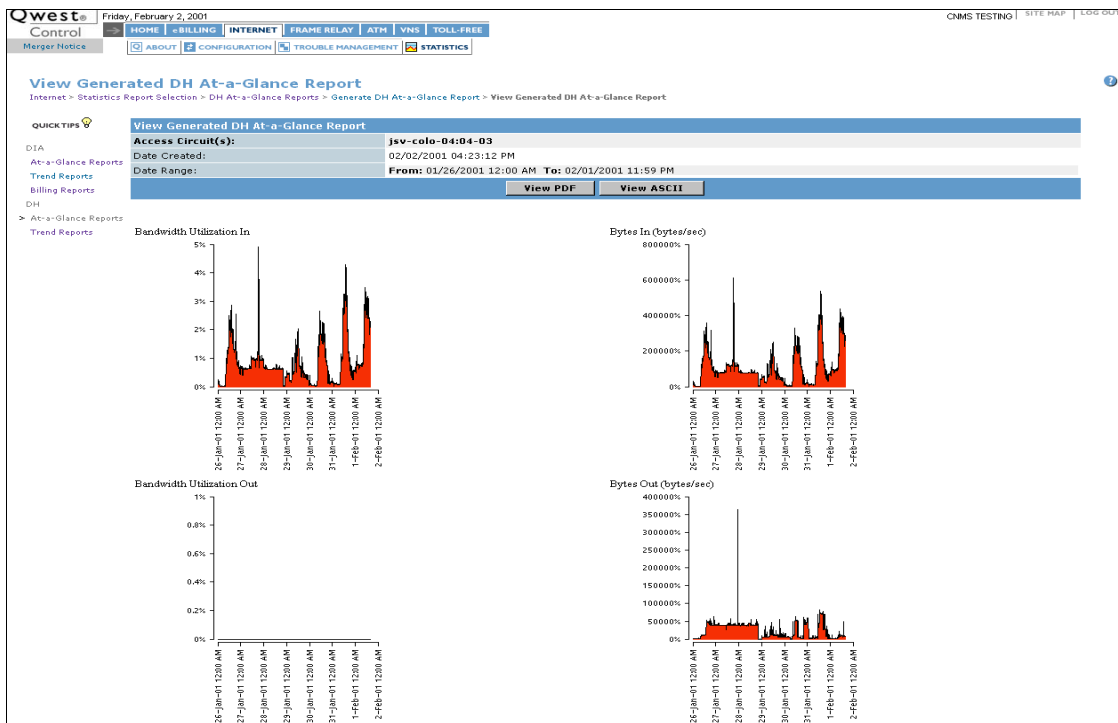


Figure 8: Internet At-a-Glance Report

## Trouble Manager

The Qwest Control trouble manager enables WITS2001 customers to create trouble tickets online and view a summarized list of all open trouble tickets including those opened in Qwest Control or those opened by Qwest Customer Care. In addition, customers can view all trouble tickets that have been closed in the last ten days. The trouble manager is available for ATM and Frame Relay Services. **Figure 9, Ticket List**, presents a sample screen illustrating all of the current tickets open for a specific customer.

The screenshot shows the Qwest Control web interface. At the top, there is a navigation bar with links for HOME, BILLING, INTERNET, FRAME RELAY, ATM, VNS, WORLDCARD, and TOLL FREE. Below this is a secondary navigation bar with ABOUT, CONFIGURATION, TROUBLE MANAGEMENT (highlighted), and STATISTICS. The main content area is titled "Trouble Management" and includes a "QUICK TIPS" icon. A table titled "Trouble Management - Tickets" is displayed, with a "+ Create Ticket" button in the top right corner. The table has columns for Ticket #, Service Type, Component/Problem Type, Service Id, Status, Date Opened, and Last Status Date. There are seven rows of ticket data, each with a magnifying glass icon in the right margin.

Ticket #	Service Type	Component/Problem Type	Service Id	Status	Date Opened	Last Status Date
NTM000000004469	NetVPN/Shasta	Policy Management	DS1-185213547	Open	06/21/2000 02:17:37 PM EDT	06/21/2000 05:26:01 PM EDT
NTM000000004471	NetVPN/Shasta	Request	DS3-155598459	Assigned	06/22/2000 11:10:54 PM EDT	06/23/2000 02:23:15 PM EDT
NTM000000004473	NetVPN/Shasta	Request	DS3-155598402	Open	06/24/2000 09:15:15 PM EDT	06/24/2000 12:31:10 PM EDT
NTM000000004484	NetVPN/Shasta	Network	DS1-160348523	Open	06/26/2000 05:21:42 PM EDT	06/26/2000 05:21:42 PM EDT
NTM000000004485	MDNS MFW-VPN	Policy Management	MFW-155598403	Open	06/26/2000 05:22:16 PM EDT	06/26/2000 05:22:16 PM EDT
NTM000000004506	MDNS MFW-VPN	Troubleshoot	MFW-155598402	Assigned	06/27/2000 02:19:59 PM EDT	06/27/2000 02:19:59 PM EDT
NTM000000005372	MDNS MFW-VPN	Policy Management	MFW-155598404	Assigned	06/29/2000 04:15:48 PM EDT	06/29/2000 04:15:48 PM EDT

Figure 9: Ticket List

The Trouble Ticket is used to track activities such as customer requests for adds and drops, and changes to network or security policies in addition to tracking circuit issues.

The user can be provided with detailed information about any of the tickets by clicking on the desired trouble ticket line on the screen. **Figure 10, Ticket Details**, provides a sample screen showing the type of detail provided for each ticket.

**Qwest Control** | Wednesday, January 10, 2001 | TESTING | SITE MAP | LOG

HOME | BILLING | **INTERNET** | FRAME RELAY | ATM | VNS | TOLL-FREE

Merger Notice | ABOUT | CONFIGURATION | **TROUBLE MANAGEMENT** | STATISTICS

### Ticket Details

Internet > Trouble Management > Ticket Details

**QUICK TIPS**

View Tickets  
Create Ticket

Trouble Management - Ticket Details	
<b>Ticket Details</b>	
Trouble Ticket ID:	NTM000000000419
Status:	Assigned
Service Type:	Dedicated
Component/Problem Type:	Circuit
Service Id:	6515
Service Name:	205.171.60.206
Date Opened:	07/25/2000 05:49:41 PM EDT
Last Status Date:	07/25/2000 05:49:41 PM EDT
Symptom:	Degraded
Problem Description:	Bill Crisco called from the Sandpiper NOC stating that the server on IP: 216.206.188.216 is down and would like someone to check the physical layer to make sure that the cable is not loose. If no problem appears with the physical connection he is requesting that the machine be powercycled. Bill's manager is Jason Raber. The primary responsibilities are gonna be handled in London because the schedule is going to be switched. Sandpiper's ticket # is 38274. Matthew or Linda will be the contact in England.
Case Type:	Trouble
Priority:	Business - Medium
<b>Contact Information:</b>	
Primary Contact:	Ben Hanner
Phone:	7033634249
E-mail:	Ben.Hanner@qwest.com

**Done**

Figure 10: Ticket Details

The Trouble Manager can also be used to create a trouble ticket to identify a network problem, or to request a change in policy, an add or a drop, or information. A sample ticket is illustrated in **Figure 11, Create Trouble Ticket Interface Screen**.

**Figure 11: Create Trouble Ticket Interface Screen**

### Status Manager

The Qwest Control Status Manager provides customers with the following information for WITS2001 services:

- ▶ Real-time alarm information for their network elements
- ▶ Alarm history
- ▶ A color-coded network map (also a part of the configuration manager) as a quick reference to network status

**Figure 12, Network Alarms**, is a sample screen of Network Alarms. The alarms are automatically generated by the DIA, NVPN, ATM or Frame Relay Monitoring System. The screen indicates the status and date of each alarm for a selected time period. The user can use this screen to create a trouble ticket and to see detail as shown in **Figure 13: Network Alarm Detail**.

This system is used by the Qwest Maintenance Team to create trouble tickets, it is not the responsibility of the WITS2001 customer.

**Filter Alarms by Status and Date**

Alarm Status: Open  
Report Period: 3/9/2000 - 4/8/2000  
Severity Level: Warning Minor Major Critical  
Alarm Status: Open Closed

Time	Type	Component Name
Mar 13 2000 16:38:23	LPORT_DOWN	UNI_TVE---_DS3-1919066
Mar 15 2000 00:06:02	LPORT_DOWN	UNI_DFD---_DS3-1526198
Mar 16 2000 20:31:38	LPORT_DOWN	UNI_DFD---_DS3-1526198
Mar 19 2000 11:46:35	LPORT_DOWN	UNI_TVE---_DS3-191906
Mar 19 2000 11:46:35	LPORT_DOWN	UNI_TVE---_DS3-191906
Mar 19 2000 11:48:57	LPORT_DOWN	UNI_TVE---_DS3-191906
Mar 19 2000 11:48:57	LPORT_DOWN	UNI_TVE---_DS3-191906
Mar 28 2000 00:26:43	LPORT_DOWN	UNI_TVE---_DS3-191906
Mar 28 2000 00:29:06	LPORT_DOWN	UNI_TVE---_DS3-191906
Mar 28 2000 04:46:28	LPORT_DOWN	UNI_TVE---_DS3-191906
Mar 29 2000 00:55:40	LPORT_DOWN	UNI_TVE---_DS3-191906
Mar 31 2000 16:13:44	LPORT_DOWN	UNI_TVE---_DS3-191906

**Click the magnifying glass to view alarm details or the yellow note to create a trouble ticket**

Figure 12: Network Alarms

**Alarm Details**  
Frame Relay > Status > Alarm Details

Component Information	
Component Name:	HT9TH21151
Qwest ID:	UNI_HIJ-FRFR000-6270
Component Type:	LPORT

Alarm Information	
Alarm Logged Time:	Jan 30 2001 15:02:36
Alarm Open Time:	Jan 30 2001 15:01:21
Status:	Open
Severity:	Minor
Type:	LPORT_DOWN
Description:	Logical Port Down Alarm occurred

Done

Figure 13: Network Alarm Detail

In addition, alarms can be displayed graphically as depicted in Figure 14: [REDACTED]

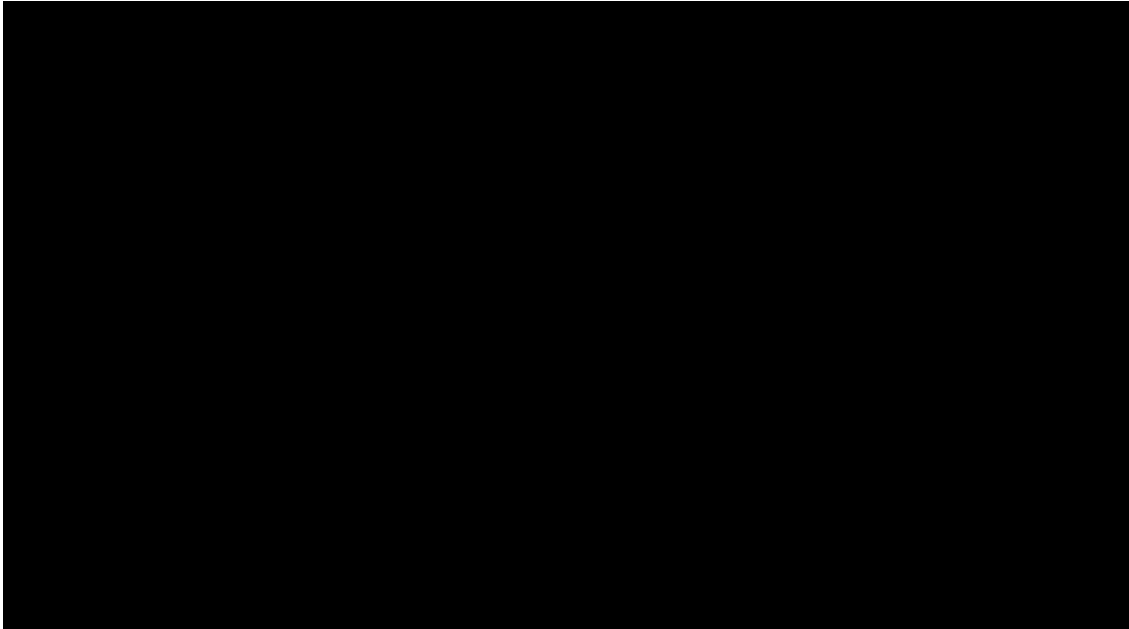


Figure 14: [Redacted]

### Configuration Manager

The Configuration Manager is a tool that can provide network snapshots, summarized network lists, and network element details. The configuration manager helps keep critical network information organized at your fingertips. It is available to support all WITS2001 services.

**Figure 15,** [Redacted], shows the screen that provides an access to IAS Configuration information. It provides information about all of circuits as well as performance statistics plus a link to a network map for the network.

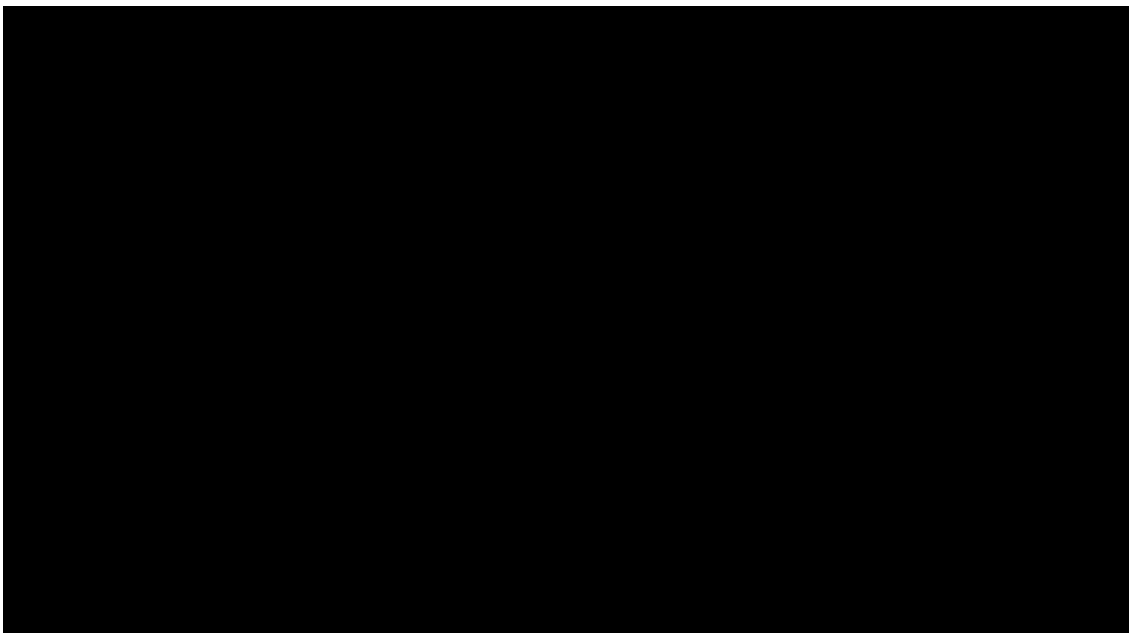


Figure 15: [Redacted]

## System Administrator Manager

The System Administrative (SA) Manager is the command center of Qwest Control for the customers use. The SA manager provides System Administrators to:

- ▶ Add new users
- ▶ Create customized roles
- ▶ Audit users' actions

With the SA manager, users can be provided just the right level of access to keep your network running smoothly through the secure environment of Qwest Control.

Figure 16 shows the user manager screen used to add user accounts, create and manage custom roles, audit user activity, modify or reset passwords, and add or delete components to the system.

System Administration - Manage Users

Home > System Administration - Manage Users

QUICK TIPS 1-50 of 60

ALL FIRST PREVIOUS NEXT

First Name	Last Name	User ID	Roles
Jackson	Children	userjp1	[Icons]
Jackson	yarlagadda	user6789	[Icons]
sriini	Varlagadda	user45678	[Icons]
8xx	user	user16b	[Icons]
DIA	user	user16a	[Icons]
first	user	user1	[Icons]
Rachel	Sullivan	testmast	[Icons]
Testers	Testers	testers	[Icons]
A	test	tester1	[Icons]
bart	simpson	test5	[Icons]
john	smith	test4	[Icons]
lester	tester	test3	[Icons]
Test	Hope	test2	[Icons]
elaine	benice	test1	[Icons]
HAMRICK	TERESA	TERESAH	[Icons]
erinivas	yarlagadda	tempuser3	[Icons]

Manage Users  
View details, modify, reset passwords, delete, assign components

Add users & accounts, Create & manage custom roles, Audit user activity

Figure 16: User Manager Screen

### 1.2.5 Draft Implementation Plan

The proposed service is a commercial service available on the Qwest Nationwide Network. In order to install the service, a service request must be submitted to Qwest. The service request will provide Qwest with the SDP information required including the appropriate feature(s) required to process the request. The entire price will consist of a Non Recurring Charge (NRC) for installation and equipment provision and a Monthly Recurring Charge (MRC) for services and features. The service is provided on a fixed MRC, it is not a usage-based product. The timeline for implementation varies depending upon the size of the project and the availability of local loop facilities. Once Qwest receives sufficient information to develop a quote and produce

a network design, the typical interval for presentation of quote and said design to the customer is ten days. The interval period for network implementation begins upon receipt of a valid purchase order and receipt of all technical information required from the customer. Typical interval for T1 services is [REDACTED] days and for DS-3, [REDACTED]. If facilities are not available Qwest will provide an estimated interval on an individual case basis (ICB). The interval is the time normally required by Qwest or other local service providers to design and install the local loops. Once installed, Qwest will run an end-to-end performance validation using automated performance testing through Qwest Control.

### 1.2.6 Management and Operations Approach

The management approach for IAS is described in the WITS2001 Eligibility Proposal and in Section 1.2.1 of this proposal. No change to that approach is necessary or planned.

Qwest's IP network is managed, monitored and maintained from the Qwest WDOC [REDACTED] on a 24 hours per day basis every day of the year. The Qwest WDOC in Ballston will manage the actual operation of the IAS and will interface with WITS2001 clients through the Customer Service Center (CSC) described in the Eligibility Proposal.

### 1.2.7 Partnership with GSA

Qwest has provided a Marketing Plan in the WITS2001 Eligibility Proposal. This plan outlines a process whereby Qwest will partner with GSA to ensure the success of the proposed service and of the WITS2001 contracting vehicle. Some highlights of the plan are summarized below.

Immediately upon a contract award for IAS service, a dedicated WITS2001 Marketing Team from Qwest Government Services Division (GSD) will contact the GSA/NCR to establish a marketing kick-off meeting to be held within the first two weeks after award. The goal of the meeting is to review this draft Marketing Plan, agree to any revisions, and set resources in motion to grow the existing customer base, as well as introduce new products and services under the contract now and in the future. For successful marketing and sales, the Qwest and GSA teams must work as a true partnership, so frequent, scheduled communications in the form of meetings or reports, or informal daily calls, are the backbone of this marketing plan.

The GSD Marketing Team will participate in program, operations and sales reviews to ensure that WITS2001 marketing is based on a broad knowledge of the entire program. Representatives of the Qwest Marketing Team will continue to participate in WITS2001 sales and program reviews on a regular basis, providing input and feedback to the Qwest/GSA marketing team.

#### Sales Activity

The GSD Marketing Team will work with GSA to set sales goals based on market variables and customer base. The GSD Marketing Team will compile and assess sales metrics including Total Revenue, Lines of service, and New Service Development. From these metrics, Qwest and GSA will forecast sales achievement for two quarters: i.e., plus 3 months, plus 6 months.

Along with the WITS2001 account team, a representative from the GSD Marketing Team will participate in Qwest GSD weekly and quarterly sales reviews specifically to maintain WITS2001

contract visibility amongst the sales force and executive management. It will be the responsibility of the GSD Marketing Team to identify and facilitate resolution of any sales-related issues.

### **Marketing Activity**

The GSD Marketing Team will proactively conduct the WITS2001 marketing program. This includes a wide range of activities, including:

1. Trade Shows
2. Events
3. Field Marketing
4. Customer Outreach
5. Media
6. Training
7. GSD WITS2001 Website
8. Market Intelligence
9. Monthly WITS2001 Marketing Team Updates
10. Quarterly WITS2001 Marketing Team Meetings

### **Trade Shows and Events**

The GSD Marketing Team and GSA will review an initial list of trade shows and events to develop a schedule featuring WITS2001. Joint effort between Qwest and GSA will result in wider market impact. Qwest GSD traditionally participates in two to three big trade shows per year, including the GSA FTS Networking Conference. GSD also participates in many smaller agency or federal market-segment specific shows. These have proven to be very effective as they offer smaller, more informational, one-on-one discussion opportunities with federal customers. The GSD Marketing Team proposes highlighting the WITS2001 contract in the Qwest GSD booth with a large display specifically for the program, along with knowledgeable account managers and WITS2001 customer collateral. The GSD Marketing Team would also seek to position and staff WITS2001 speakers and panelists as appropriate during the conferences.

In addition to trade show, the GSD Marketing Team will seek to feature WITS2001 in local area events. GSD currently participates in a wide variety of events that afford the opportunity to highlight specific contracts, products, the company, and trends in the market. The GSD Marketing Team will work with GSA to maximize these forums to feature the benefits and details of WITS2001. Many of these events are sponsored by federal market associations and organizations. GSD participates in the top federal market industry/government associations and will seek to insert WITS2001 awareness into any emerging opportunities.

### **Customer Outreach**

The GSD Marketing Team and account managers will identify and support customer outreach opportunities as they arise. GSD account managers will alert the GSD Marketing Team of customer groups that would benefit from WITS2001 services. The GSD Marketing Team provides customer outreach activities on a regular basis and stands ready to promote a schedule of customer presentations, including Q&A sessions, for the WITS2001 contract. The focus of the WITS2001 outreach activities will vary depending on target customer requirements.

Initially, the GSA Marketing Team will develop an overview of WITS2001 and Qwest GSD offerings as an introduction for federal customers. This will include a WITS2001 brochure written and produced by the Qwest Marketing Team. The form of customer outreach may also include training, covering the contract itself, basic products and services, new products and services, and implementing enterprise solutions using the WITS2001 contract.

### Media

The GSD Marketing Team makes full use of federal market media outlets and intends to highlight the WITS2001 contract in major messaging. Upon contract award, GSD would seek to issue a press release in coordination with GSA press release about the new award. From this press release, the GSD Marketing Team would work with federal trade publications to get messaging out to market. Additionally, the GSD Marketing Team would make use of print and radio advertising in the local D.C. market to ensure that federal customers were aware of WITS2001 availability and benefits.

The GSD Marketing Team would also make use of the Internet channel, proposing on-line interviews with WITS2001 experts on web-streaming news channels as well as advertising on key web sites. WITS2001 pages will be added to Qwest's GSD (federal customer) web site and feature information from the Client's Guide as well as marketing focused areas for new or potential customers. This site will be maintained and updated as required to ensure that all new products and services are highlighted.

### 1.3 Qwest Managed Router Service

Qwest Managed Router Service can be provided with Qwest Dedicated Internet Access Service. Qwest Managed Router Service installs and manages a router that has been sized for the network services and it is compatible with customer requirements. The managed router can serve as a host for other WITS offerings. Qwest Managed Router Service will be provided through the Qwest Network Management Center (NMC).

Qwest Managed Router Service will provide Government users with the capability to have their data networks proactively managed by Qwest from a Qwest network management center and to provide packet filter routing service. This service provides the management of customer premise Cisco routers. The Managed Router Service supports a dial backup capability to provide a secondary method to access the router in the event the primary management path is disrupted. Qwest will provide the modem and it is the customer's responsibility to provide the business line adjacent to the router requiring the backup capability.

Qwest will provide the following as part of the Managed Router service:

- ▶ **Network profile** information including all relevant information about the managed portion of the network (e.g. network topology map and infrastructure inventory),
- ▶ **Continuous monitoring** of Routers and data transport network to ensure optimum performance and up-time,
- ▶ **On-line network reports** documenting the network, including bandwidth utilization, volume leaders, et cetera,

- ▶ **Fault management** to remotely isolate and respond to faults quickly and accurately, before the performance of the network can be compromised,
- ▶ **Configuration management** to ensure seamless network performance through backup, comparison and restoration of device configurations,
- ▶ **Performance management** including tidemark activities like threshold, counter and gauge definitions, to help achieve the data networking performance goals,
- ▶ **Network Analysis** of the data network performed by the designated Qwest NMC engineers.

In addition to these tasks, Government network administrators will be provided with a Secure Web Interface to the NMC to view the status of managed network through the routers. This system provides Government users with network information, including alarm information and summary reports, at the desktop using a standard Web browser.

### 1.3.1 Network Profile

Network profiling helps telecommunications managers keep track of facilities, devices and costs. Qwest NMC engineers will collect information about the network elements that are covered by the service. With the Information and Installation (I&I) at hand Qwest will create a profile of the network represented in a Network Inventory and Network Topology Maps.

As the network changes, the Qwest NMC personnel will perform updates to all components of the network profile. The network profile is accessible to the Government customer, along with other reports, by using a regular web browser and logging into the Qwest secured databases. For additional information on accessing the profile, please refer to Section 1.3.3, “On-Line Reports.”

#### Network Inventory

Upon receipt of service order for Qwest NMC engineers will conduct a detailed inventory on all devices to be included in the service. Additionally, remote diagnosis will be performed on the equipment to be managed. All information necessary to manage the network will be stored in these databases (e.g. site information and device maintenance providers with contract numbers and contact information).

#### Network Topology Map

After the NMC engineers complete the initial inventory, Government users will have access to a series of detailed network topology maps depicting all covered devices. The maps will be updated as devices are added to or deleted from the managed data network.

The NMC engineers use the topology maps to perform all network management tasks, including effective fault isolation and performance analysis. Additionally, Telecommunications managers can use these maps to perform capacity planning and to have an overall view and understanding of the network.

The topology maps are constructed using a set of specialized tools and time-tested processes. The maps are hierarchically organized into submaps, reflecting internetworks, networks and segments.

The highest level of Internet topology map shows the edge devices (e.g. routers or switches) as well as the links connecting them. At the next level down, Government users will be able to view the network submap, showing a collection of segments and connections such as routers, bridges, switches, and hubs. Additionally, the individual segment's topology will be represented, be it a bus, star or ring.

### **Trouble Ticket Summaries**

Qwest NMC engineers will utilize the a trouble ticketing system. This system records the symptoms, resources, diagnostics and resolution of all faults generated by the network.

### **1.3.2 Continuous Monitoring**

The NMC will proactively monitors the network, 24 hours a day, 7 days a week, 365 days of the year. The data networking equipment and transport are continuously monitored using customized tools to immediately detect faults and ensure optimum performance.

Detecting and isolating faults accurately and instantly is the main goal of the monitoring process. The first step in monitoring the network is to collect or capture the management data stored in the devices. The stored data/values are then used to:

- ▶ Trigger the Fault Management (FM) process (Before initiating the FM process, the data is correlated and filtered to determine the nature and level of the fault and discard irrelevant traps).
- ▶ Compare against stored thresholds and baseline information during the Performance Management process.
- ▶ Assemble the On-line Reports.

The SNMP polling mechanism is used by the NMC staff to collect the network management data from covered devices. The NMC polls devices every [REDACTED]. When one of the devices does not respond to the polls, or when the values returned by the devices exceed predefined thresholds, a fault condition is assumed. An alarm and a trouble ticket are then generated. (Thresholds are set through the Performance Management process).

Monitoring also includes the detection of faults by receiving and processing traps (unsolicited network management messages sent by networking devices). Traps will originate from the networking devices or from network alarms. From that point, the fault will be handled through the Qwest "Fault Management" process.

### **Filtering and Correlation**

The NMC uses filters to look at a single source of Network Management Information (NMI). Filtering rules are applied to check for thresholds, amounts of change or other factors. NMI that satisfy these criteria become events and are passed to other management tools and our engineers.

Fault correlation is the process by which several alarms are narrowed from a mass of problems to a root cause and side effects. The correlation capabilities built into the toolkit handles reports from multiple sources in parallel and sorts out more complicated situations. For example, a router failure has the following effect: the router failure may isolate a set of systems from the rest

of the network and thus degrading performance because of re-routing through longer paths or slower links. The router failure generates many events; correlation using the NMC toolkit sorts them out and identifies the likely cause. The flood of events is sorted and the most likely cause (in this case the router failure) is identified. The NMC engineers focus on the real fault and the result is higher network availability and service quality.

### Polls

The NMC management platforms poll for specific Management Information Base (MIB) objects and report alarms if the returned result does not match the expected value or has crossed a predefined threshold. An alarm is also generated if no response is received within the allotted time. Threshold values are based on the expertise of the NMC engineers, and are evaluated on an ongoing basis. Additionally, custom thresholds can be set to fit the individual needs. Some examples of items that are polled include:

- ▶ WAN and LAN physical interface utilization
- ▶ WAN and LAN physical interface error rate
- ▶ Interface unknown protocol
- ▶ Device memory utilization
- ▶ Device CPU utilization

### Traps

When the SNMP agent within one of the devices detects a fault (or when a threshold is exceeded) an unsolicited message is sent by that agent to a pre-configured NMC management platform, which then reports an alarm to the NMC engineers. Some examples of traps that will be acted upon by the NMC engineers are as follows:

- ▶ ColdStart - sent when the device has rebooted
- ▶ LinkDown - sent when the device detects that a physical interface has gone down
- ▶ LinkUp - sent when the device detects that a physical interface has come up
- ▶ AuthenticationFailure - sent when the device receives an SNMP query that contains an invalid community string

### 1.3.3 On-Line Network Reports

Network reports are automated and available to Government customers through a secure website. These reports facilitate NMC engineers in evaluating the performance of the network, allowing customers to make the most of existing resources and helping plan for future network growth.

In providing reports, it is the objective to provide customers the most information possible, with the highest possible granularity, in the simplest format. Reports are organized from a high level view of the network down to the smallest component, thus satisfying the needs of everyone in the organization.

Customers can access the reports at [REDACTED]. After receiving a welcome screen, the name and password must be entered to be able to proceed further. Reports

are available for viewing by the customer via any standard WWW browser. Government customers can also choose between the following report types:

- ▶ Daily: At the end of each day, daily reports are generated which contain data from the past 24 hours
- ▶ Custom: View reports for specific dates.

The On-line Reports system retains the data as shown in **Table 4, Data Aggregation.**

**Table 4, Data Aggregation**

AGE	GRANULARITY
1 to 30 days	As polled ( [REDACTED] interval) - pre-assembled daily reports
1 to 7 days	As polled ( [REDACTED] interval) - Custom reports
8 to 42 days	Aggregated to [REDACTED] increments - Custom reports
43 to 364 days	Aggregated to [REDACTED] increments - Custom reports

The following are examples of reports that are available to customers and to the NMC engineers for proactive analysis. A more detailed description of each report is available on line.

### LAN/WAN Reports

The first group of reports is viewed by clicking on the LAN/WAN Reports option on the main “reports” menu.

- ▶ **Exception Detail Report** - This report is available on a daily or weekly basis. It lists elements/devices that have exceeded the set threshold. These thresholds are established by the customer and the NMC engineers. Telecommunications Managers can use this report to track the health of the network.
- ▶ **Multi-Variable Trend Reports** – From the Exception Detail Report customers can drill down into this report. It provides a list of which thresholds were exceeded.
- ▶ **Daily/Weekly Network Volume & Hourly/Daily Network Volume** - The Daily/Weekly Network Volume chart shows the total network volume in bytes or in percentage of bandwidth utilization for all reported elements or devices.
- ▶ **Daily/Weekly Volume vs. Baseline Chart** - This chart displays the volume in bytes or in percentage of bandwidth utilization for the reporting day for all of the elements.
- ▶ **Situations to Watch Chart** - The Situations to Watch chart lists the elements that are predicted to exceed, reach, or are closest to reaching a trend threshold. The report compares the data collected from the previous day to the Trend threshold calculated for each variable.
- ▶ **Volume Leaders Charts** - The Volume Leaders bar chart and table list the elements that had the highest volume for the previous day.
- ▶ **Health Index Leaders** - This chart lists the ten elements that received the highest Health Index values on the reported day.

- ▶ **Bandwidth Utilization Chart** - This chart displays the volume distribution for each element or device in the report, i.e., how much time an element spends in a particular bandwidth utilization range.
- ▶ **Bandwidth Trend Reports** - This report displays the bandwidth utilization for a network element or device.
- ▶ **Average Health Index Graph** - This graph displays the Health Index for all of the elements or devices in the report. If an element has errors, congestion, etc., it will be assigned points by the severity of the fault.

## Device Reports

The next group of reports is received by clicking on the Router Reports button on the first page.

1. **Daily/Weekly Network Volume & Hourly/Daily Network Volume** - The Daily/Weekly Network Volume chart shows the total volume for all reported devices in Frames, bytes, or percentage of bandwidth utilization.
2. **Bandwidth Utilization Chart** - The Bandwidth Utilization chart displays the average line utilization for each device. The average line utilization is calculated by summing the utilization (total number of bytes divided by throughput) of each interface and dividing that sum by the number of interfaces.
3. **Hourly/Daily Health Index & Situations to Watch Chart** - This chart displays the Health Index for the devices in the report by averaging the Health Index assigned to each device in the report.
4. **CPU Utilization Chart** - This chart displays the average CPU utilization for each device. For devices with multiple CPUs, the average CPU utilization is presented.

### 1.3.4 Fault Management

Fault management activities consist of analyses to isolate and correct unusual operational behaviors, including conditions such as deterioration of service and error situations. All fault management activities will be recorded in our trouble ticketing system for further analysis by the Qwest NMC staff of engineers. Qwest NMC engineers remotely isolate and respond to faults quickly and accurately, before the performance of the network can be compromised. The fault management process can be triggered by any of the following:

- ▶ Monitoring process: by devices not answering polls or by received traps.
- ▶ Performance Management: when the newly collected device information is outside of the thresholds and baselines set forth by our engineers.
- ▶ Network Analysis: by the discovery of uncomplimentary patterns or trends.

The following identifies the critical elements of the Fault Management Process.

### Event Severity

NMC engineers respond to network faults based on the event severity definitions outlined below. The engineers will classify alarms into three types: Critical, Moderate, and Minor, enabling them to restore the most critical faults first. In each case, the Network Management System (NMS) logs the event, creates an “event ticket,” and immediately notifies the on-duty NMC engineers by

NMC console message, pager, and/or Email, with as much additional alarm information as possible.

- ▶ Critical - A service-affecting situation has occurred and immediate action is required.
- ▶ Major - A significant, but not urgent condition exists, such as chronic intermittent interruptions or imminent service interruption.
- ▶ Minor - An atypical condition has arisen which requires investigation by the NSC engineer, but does not have any significant impact on the infrastructure.

### **Escalation Procedures**

The escalation procedures are extensive processes and procedures employed to handle any situation, fault or event that customers are likely to encounter. The following outlines the escalation procedures.

- ▶ The NMC Customer Engineers (CE) are responsible for the 24 by 7 monitoring of the networks; they are the first group notified in the event of a fault or event. They start assessing the situation no later than five minutes after receiving the initial alarm.
- ▶ If the fault is not critical, the CE will proceed to diagnose the network to find the cause of the alarm. The CE will email, page or phone the customer to keep them apprised of the situation. If the situation is not determined within ■ minutes, the CE will escalate to the SE.
- ▶ If the fault is critical, the CE will immediately notify the customer of the situation. The Government customer may designate up to three customer contacts per site. Furthermore, the event will be escalated to a Senior Engineer (SE) within ten minutes from the moment the alarm was generated. The CE will work with the SE to diagnose and solve the fault.
- ▶ If the SE has not solved or determined a solution for the fault within ■ minutes of the time they got involved, the SE will escalate to the transport provider, the device maintenance provider or the device manufacturer. The CE and SE will drive this process as the agent until the fault has been fixed.
- ▶ After one hour without a solution in sight, the NMC manager and the Tier 3 support manager will be notified.

### **1.3.5 Configuration Management**

Configuration management is the process of gathering information about the current network configuration. The data is stored for use in managing the restoration activities when an undesired change has been performed to one or more configurations, or if the configuration information is completely lost due to a hardware malfunction. As device manufacturers add remote configuration capabilities to their products, Qwest will certify these additional devices for Configuration Management support.

Configuration management includes functions to:

- ▶ Capture parameters that control the routine operation of the network,
- ▶ Associate names with managed objects and sets of managed objects,
- ▶ Collect information on demand about the current condition of the network,
- ▶ Obtain announcements of significant changes in the condition of the network.

The NMC collects the configuration of each supported device at regular intervals and compares it to the baseline configuration to determine whether any changes have taken place. Any anomalies will be discussed with the customer. The configuration will then be restored to its baseline, or, if the anomaly is determined to be appropriate, a new baseline will be established for the device.

In addition, the NMC engineers will perform reasonable and customary configuration changes on covered devices, such as those that the NMC's network analysis necessitates or that the customer requests. Any changes that affect a single device are included in the service.

### 1.3.6 Performance Management

Data communications network systems are composed of multiple complex components that must intercommunicate to share data and resources. It is critical to the effectiveness of an application that communication over the network remains within certain performance parameters.

Performance management serves as a useful tool to detect escalating error conditions before they happen, in order to resolve fault situations quickly. Data collected from the Monitoring process is logged into our custom-built databases and compared against the thresholds predefined between the customer and Qwest engineers.

As part of the proactive component of Managed Router Service, Qwest's specialized tools have been programmed to continuously evaluate key device and network health indicators, looking for escalating error conditions before they cause problems. This is accomplished by defining a set of threshold calculations using certain SNMP MIB variables. When the value of one of these calculations exceeds (or goes below) its defined threshold, the NMC customer engineers receive an alarm to notify them of a potential problem.

Qwest NMC engineers proactively and continuously look for potential faults. The net result for the customer is that faults are fixed before they are noticed and troubles are spotted before it causes network slowdowns or outages.

#### Thresholds

The central concept in thresholding is that devices are engineered to operate within certain ranges. When they are operating within those ranges, they need very little attention. The moment our tools detect that the preset threshold [REDACTED] has been exceeded, an alarm and a trouble ticket will be created to initiate the Fault Management process.

Another example would be an Ethernet segment that has a high level of errors due to poor physical infrastructure, such as old coaxial cabling in bad condition or excessive repeaters. In this case, the segment would be operational, but its performance would be affected.

Thresholds are set only on MIB values described in numeric terms, such as counters, gauges, integers and time ticks. NMC engineers use the data collected during the monitoring process to determine a range of values describing normal behavior for a MIB variable. Some examples of threshold values monitored by the NMC are:

- ▶ Average device CPU utilization
- ▶ Bandwidth utilization
- ▶ Congestion
- ▶ Frame rate
- ▶ Broadcast traffic levels
- ▶ Good/bad/abort/short Frames
- ▶ Packet discard occurrences
- ▶ Packet and traffic volume
- ▶ PVC data throughput versus committed information rate (supported by some devices)

### 1.3.7 Network Analysis

The expertise of Qwest NMC engineers is invaluable for solving potential problems before they occur. Our engineers manually analyze the network to uncover:

- ▶ Poor network response time and slow overall network performance.
- ▶ Excessive network downtime.
- ▶ Pinpoint inefficiencies, such as excessive retransmissions, time-outs, unexpected network hogs, and poor Frame sizing, so that the customer can make more informed decisions about moving to higher bandwidth network technologies or tuning the network.
- ▶ How routing protocols are operating and affect the overall performance of the network.
- ▶ How misconfigured devices usually masquerade as poor performance. Common examples include lack of filtering to eliminate unnecessary traffic like AppleTalk and Novell SAPs and Router Information Protocol (RIP).

The NMC Engineers also perform analyses to ensure that proposed changes will solve an immediate need, and that they will not adversely affect other user requirements. Additionally, our engineers will assist the customer in:

- ▶ Selecting the right custom thresholds for the different elements on the network.
- ▶ Designing the best strategy to deploy new client/server application. The rollout of new client/server applications often causes problems such as sluggish performance, poor response time, and even downtime.

- ▶ Determining which elements of the network to upgrade to improve response time for particular sites, users or applications.
- ▶ Selecting the best strategy to migrate and deploy new network technologies.
- ▶ Designing and testing the effectiveness of access lists.
- ▶ Determining the level of intelligence that must be embedded in the network to prevent congestion and fault tolerance.

Qwest NMC engineers analyze and correlate information about the network for up to ten hours for every 100 devices covered under Managed Router Service every month. During their analysis Qwest NMC engineers will study the following sources:

- ▶ Logs, detailing conversations with customers and the networking staff about performance complaints, expansion plans, planned changes, etc.
- ▶ On-line Reports, with emphasis on reports showing severe deviations from baselined information.
- ▶ Network Topology maps, to graphically correlate all the information about the network.
- ▶ Trouble Tickets and summaries, to determine whether any segments show excessive downtime. Additionally, Qwest NMC engineers analyze the information stored in the trouble ticketing system to pinpoint intermittent faults of CPE and transport, with discontinuous or fluctuating characteristics, and chronic faults whose trends are to cause increasingly severe faults.
- ▶ Network Event logs, to examine system state history.
- ▶ Configuration changes.
- ▶ Threshold information, to accommodate for changes on the network.
- ▶ Device logs, such as history information.
- ▶ Type of traffic that the network must support: voice, data, image, full motion video, or any mix of these.
- ▶ Types of protocols that must be supported (current and planned).
- ▶ Total number of nodes (current and planned).

### Baselines

Baselining is the process of taking snapshots of a network when it is healthy. This involves capturing data (during the monitoring process) over time to determine normal values of network statistics. Once a baseline is established, it can be compared to ongoing network behavior. This enables Qwest to spot anomalies and to solve impending problems before they turn into network catastrophes. This process allows customers and our engineers to:

- ▶ Understand network usage
- ▶ Identify network faults and eliminate them before they affect performance
- ▶ Plan for growth

- ▶ Determine system performance under normal and exceptional conditions

Baselines, like thresholds, can pinpoint future problems. Where they differ is that an element can be within the allowable threshold value, but it could be experiencing an uncharacteristic value. For example, a given link may have a threshold value of 56kb, but its baseline (normal behavior) is between 0 and 25kb. Qwest NMC engineers would note during their monthly analysis that during last month the link in question showed values between 5 and 42kb. This is very uncharacteristic for this link and would be enough reason to monitor this link even though the threshold value has not been exceeded.

### Installation and Inventory

The Installation and Inventory is the first step performed by Qwest NMC engineers when Managed Router Service is implemented. It is during this stage that modeling of the network into a toolset is accomplished to analyze the network based on initial data collected. During the “Initial On-site Technical Read-out” there is an opportunity for the customer to meet the designated lead engineers. The Installation and Inventory requires the heavy customer participation since it includes the following activities.

- ▶ Two engineers will be assigned to handle the network and lead all on-going performance trouble issues related to it. They are selected from our pool of seasoned networking experts according to their specialization to best support the device type mix.
- ▶ They determine the size and quantity of necessary PVCs to support the management traffic.
- ▶ Information about each device to be covered is gathered, including the manufacturer, model and serial numbers, location information, maintenance provider information (including contract number), software release number, logins and passwords, and SNMP community strings.
- ▶ Information is gathered about all the links touching the devices to be managed, including serial numbers and provider contact information.
- ▶ After all the prior steps have been completed, Qwest NMC engineers model the network into a “toolset”. During the modeling process, frequent participation from the networking personnel is required.
- ▶ Initial analysis of the network is performed.
- ▶ Logins and passwords are generated to allow the Government customer to access the On-line reports. We will create up to three logins for each covered devices. This will enable the personnel to have access to the On-line Reports and Network Profile.

### 1.3.8 NMC Secure Web Interface

Qwest will provide a secure web interface that will provide the status of the data network from the router perspective to provide a total network view between all the UNIs. Utilizing newly developed Internet technology, the Government user is able to see critical network conditions without having to analyze data, open more applications, or spend time searching for troublesome network situations. This system provides information about both the private and public switched network connections in a simple, secure and consistent format.

### 1.3.9 Network Management Center (NMC)

The NMC is the operation center where customers networks are managed and where the Qwest networking experts are located. The four components of the NMC are:

<b>Personnel</b>	The Qwest team of engineers is on the cutting edge of the industry, and two of these specialists are designated to serve the customer. Their mission is to make the network perform the way it was intended and take on the complex and continuous management tasks so the customer doesn't have to detect and correct potential problems before they occur.
<b>Tools</b>	The network management tools we use, including information technologies, architectures and applications, are best-in-class. Qwest engineers have gone a step farther, crafting highly-advanced tools, not available from any other vendor, to help manage the data network cohesively and comprehensively.
<b>Security</b>	The measures to protect the data and network against outside users.
<b>Service Redundancy</b>	Qwest Managed Router Service has implemented Service Redundancy measures to ensure a high availability service to the customer.

#### Personnel

The Qwest NMC staff is complete and well rounded, enabling coverage of all aspects of data network management. Qwest knew from experience that to construct a complete collective intelligence for Qwest Managed Router Service, we had to carefully determine the capabilities required of the NMC staff, then carefully choose people to fill those positions. Each staff member is a specialist and, collectively, they provide an incredible aggregate intelligence. The people in the NMC were chosen to provide a broad range of technical expertise to provide overlapping coverage and support.

As Managed Router service is enhanced to cover additional equipment and transport technologies, Qwest adds personnel who are trained and experienced in those areas. Additionally, NMC engineers and other personnel will continuously update their skills and knowledge. Each customer is assigned a senior and customer engineer, who will lead a team of data networking experts. This team will be responsible for managing the ongoing health of the data network, both proactively and reactively.

#### 1.3.10 NMC Security

To protect the data and network against outside users, we have implemented the following measures:

- ▶ The NMC links directly to the data network via a dedicated PVC.
- ▶ Access lists are used in the NSC POP and center routers to prohibit users from one network from accessing someone else's network.

- ▶ A firewall system has been implemented.
- ▶ A Secure Socket Layer (SSL) application has been implemented so data can be encrypted when a customer accesses the server to retrieve data.

To protect data and networks against internal intruders, the NMC is staffed by engineers dedicated to serving Managed Services customers. Information regarding the data network is confidential. There is no sharing of such information between NMC engineers and any other departments. Furthermore, we have deployed a secure shell (SSH) system, where each authorized user is given an electronic key that must be entered before they can access any of the systems or tools.

### Service Redundancy

Qwest has implemented Service Redundancy measures which include backup, redundant servers and applications, and an automatic E-mail and paging system.

#### *Backup*

All data and software running in the NMC are backed up on a continual basis.

#### *Redundant Servers and Applications*

The NMC utilizes full server duplexing for redundancy: Each of the applications that are essential to manage the infrastructure is run on two separate servers. When any hardware or software being used by the NSC fails, our engineers switch over to the alternate equipment.

### 1.3.11 Description of Qwest-Furnished Equipment

**Table 5, Managed Packet Filter Router Hardware Description**, indicates the router that will be installed at each SDP based on the WITS2001 service transport selected.

**Table 5, Managed Packet Filter Router Hardware Description**

	<b>Interface</b>	<b>Router For Managed Router Service</b>
	10/100 T1/Tiered	Cisco 1721 w/T1 interface
	10/100 NxT1/Tiered	Cisco 3640 w/NxT1 interface
	10/100 DS3/Tiered	Cisco 7204 w/DS-3 interface
	10/100 OC3 Tiered	Cisco 7204 w/OC3 interface
	Gigabit Ethernet OC-12/Tiered	Cisco 7204 with OC-12 interface
	Gigabit Ethernet OC48 Tiered	Cisco 7304 with OC48 interface

## 2. PRICE RESPONSE

### 3. RATE GROUP DEFINITION

## **Attachment A: Section H Reconciliation Document**

### Reconciliation Host Contract and WITS2001 Crossover Section H Provisions

The following Section H terms apply to Qwest services offered under the WITS2001 Crossover Program:

<b>WTT-98-PW-N-0001 Section H Terms</b>	<b>Title</b>	<b>GS00T02AHD0004 Section H Terms</b>	<b>Title</b>
H.1	Term of Contract		
H.2	Authorized Users		
		H.3	Minimum Dollar Guarantee and Maximum Contract Limitation (applies to host base contract services)
H.4	Disclosure of Information		
H.5	Internal Revenue Service (IRS): Disclosure of Information – Safeguards and Sanctions		
H.6	Price Management Mechanism – applicability shall be negotiated on a case by case basis for each service offering; in no event shall PMM apply to secondary carrier services provided by Qwest. The government and Qwest shall negotiate and reach mutual agreement as the any applicable comparison source information used in conducting the PMM.		
H.7	Price Reductions. Price reductions may be offered by agency location, and/or NPA/NXX.		
		H.9	Electronic Access to the Contract
H.9	Incentive Plan		
H.10	First paragraph of H.10 shall apply. Definition of out of service conditions and applicable service credits shall be negotiated on a service specific basis.		
		H.12	Tariff Filing Requirements
		H.13	New, Improved, Additional Services
H.13	Other Government Service Contracts and Contractors		
H.14	State and Local Taxes		
H.15	Small, Small Disadvantaged, and Women Owned Small Business Concerns Subcontracting Program Support		

<b>WTT-98-PW-N-0001 Section H Terms</b>	<b>Title</b>	<b>GS00T02AHD0004 Section H Terms</b>	<b>Title</b>
H.16	Contractor Performance		
H.17	News Releases		
H.18	Meetings/Conferences		
H.19	Permits		
		H.21	Contractor Provided Equipment
H.21	Fraud Prevention		
		H.23	Contractor's Liability Limitations
H.24	National Emergency		
H.25	WITS2001 Associated Government Fees		
H.26	Other Direct Costs (ODCs)		
H.28	Regulatory Passthroughs		
H.29	Special Requirements for Work in Areas Containing Asbestos		
H.30	Historic Buildings		
		H.32	Notice to Proceed