

1.3.2 Approach to Ensure Service Quality and Reliability

[L.34.1.3.2]

Agencies will interconnect to a network service provider offering reliable access options and peering and roaming arrangements with other service providers, as well as aggressive congestion and flow control strategies that ensure high-quality delivery of time-sensitive traffic.

With the continued convergence of applications, packet-switched network architecture (Internet protocol [IP]/multiprotocol label switching [MPLS]) will displace today's circuit-switched network architecture during the Networx contract timeframe. The architecture of the IP/MPLS-based network is designed to efficiently support the burst nature of packet (i.e., IP) traffic.

Independent of the network type, exceptional service performance must be delivered to support the Agencies' application requirements. The network architecture must be resilient and flexible to handle unpredicted traffic loads, or transmission and equipment failures. The design of the networks must incorporate redundant switching and transmission equipment, and use automated control mechanisms to manage traffic flow. Network capacity must be properly sized to handle anticipated and unanticipated capacity. The high performance of today's circuit-switched networks must transition into the growing IP/MPLS-based network.

As internal architecture of the network changes, so do service boundaries. Service performance is expanding to the service delivery point (SDP) from the network edge. Resilient and redundant access configurations are becoming essential to provide reliable service performance from the SDP to the network. As Agencies' applications converge, network access will also

converge into a few high-capacity access facilities from multiple low-capacity access facilities. The convergence of access only increases the need for resilient and reliable access solutions.

Service boundaries are extending beyond the network and into partner networks. No single contractor can offer a wholly-owned network infrastructure that reaches every location in the world. Some traffic will originate or terminate off the network (off-net). Performance must be maintained for traffic that is sent off-net for delivery, or originates off-net for delivery to Agencies. Careful partner selection is required to maintain performance for off-net traffic.

The convergence of applications onto an IP/MPLS infrastructure creates the challenge of maintaining quality of service for real-time traffic, such as voice and video. The statistical nature of an IP/MPLS network makes it difficult to control delay and jitter. Congestion and traffic management mechanisms are required in the network to provide the quality of service required by time-sensitive traffic. Delay and jitter must be closely managed.

In addition to the changing network architecture, the contract structure is changing with the transition to performance-based contracts. Performance-based contracts provide Agencies with the ability to simplify the contracting process, while providing the contractor additional flexibility to develop more creative solutions. Key to implementing performance-based contracts is verification of service performance. Through initial service performance verification and ongoing performance monitoring, Agencies can monitor service performance for adherence to contract parameters.

1.3.2.1 Service Quality and Reliability of the AT&T Network

The approaches, mechanisms, and practices to provide service quality and reliability are described in this section. Service quality and reliability are inherent in AT&T's network architecture. The network design principles that have provided exceptional service quality and reliability for voice and circuit switched customers have been applied to the IP/MPLS network design. AT&T's goal is to incorporate exceptional service performance into the IP/MPLS network design so service performance is seamless to the Agencies. **Table 1.3.2.1-1** provides an overview of AT&T's approach to service performance.

SECTION	DESCRIPTION
Section 1.3.2.a	Describes the characteristics and performance of the access solutions. AT&T's access solutions meet or exceed the industry best practices for performance. AT&T provides a broad portfolio of access options that allow the Agencies to implement high quality, resilient, and diverse access solutions.
Section 1.3.2.b	Describes peering and roaming arrangements with other service providers to carry or exchange traffic. Agencies' IP traffic flows directly to destination hosts or custom connections through more than [REDACTED] of private peering capacity with other Tier 1 Internet service providers (ISPs). Agencies' off-net IP traffic does not traverse multiple IP networks, which degrade service performance through increased latency and jitter. Global wireless roaming is enabled through general system for mobile communications (GSM) technology, which serves over one billion users in 200 countries over 600 networks. AT&T's wireless partner, Cingular, maintains high performance for off-net services, including close monitoring dropped calls, network availability, and service denial of roaming partners.
Section 1.3.2.c	Describes the congestion and flow control strategies for the network, demonstrating AT&T's ability to handle unpredicted traffic loads and unscheduled service outages. Agencies are provided reliable service because resiliency is incorporated into the AT&T network design by combining modeling and simulation with network monitoring. Automated systems in the network provide real-time flow control to manage unpredicted traffic loads and route traffic around unanticipated network outages. There are no single points of failure in the network because core nodes are designed to be single-link and single node survivable, and equipment redundancy exists at the trunk, switch, and card levels.
Section 1.3.2.d	Describes the approach to verify service performance meets or exceeds the key performance indicators/acceptable quality levels (KPIs/AQLs). To simplify the verification process, AT&T uses an automated testing platform called the common test platform. Performance data collection is automated through [REDACTED] which reports service performance online on a web-based interface.
Section 1.3.2.e	Describes approach to support time-sensitive traffic in an IP/MPLS network. Through careful network provisioning, traffic classification techniques, and traffic management mechanisms, Agencies' real-time traffic will be prioritized ahead of non-real-time traffic. Latency and [REDACTED]

Table 1.3.2.1-1: Response Summary for Section 1.3.2. Agencies obtain a high-quality, reliable service because AT&T leverages modeling and simulation tools, equipment redundancy, meticulous provisioning, automated performance monitoring, and management tools to verify and maintain service performance.

Agencies receive exceptional service quality and reliability by AT&T's use of modeling and simulation tools, equipment redundancy, meticulous provisioning, automated performance monitoring, and management tools.

1.3.2.a Access Arrangements Characteristics and Performance [L.34.1.3.2.a]

(a) Describe the characteristics and performance of the access arrangements that will connect to the offeror's backbone network(s) to ensure service quality and reliability. Describe how the performance is consistent with industry best practices. [L.34.1.3.2.a]

- *Every SDP requires a unique access arrangement with performance that is consistent with industry practices.*

The AT&T access services portfolio offers

flexible, cost-effective, reliable, and secure access solutions for Agencies' cost and performance network requirements with the focus on next-generation networking (**Figure 1.3.2.a-1**).

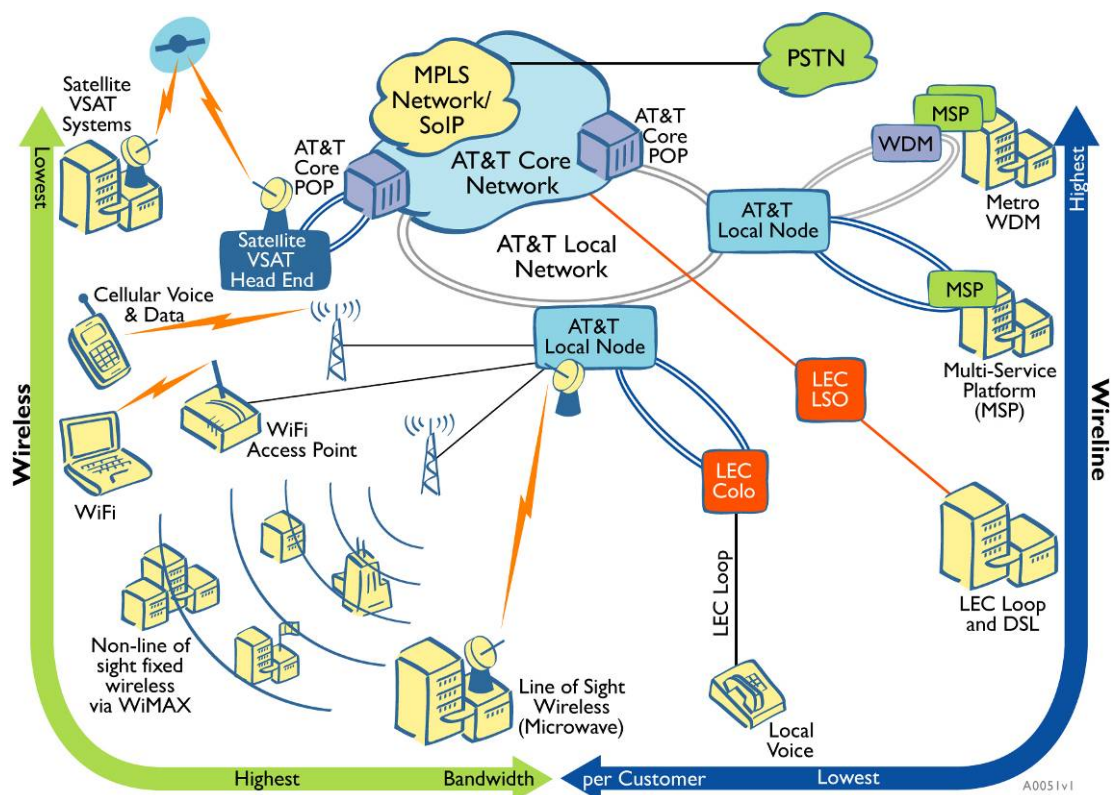












Figure 1.3.2.a-1: AT&T-Provided Local Access for Government Agencies. A broad range of network services are delivered using Access infrastructure tailored to the requirements of the service.

The access portfolio continues to evolve and ranges from low-speed leased circuits and dial-in access to wave division multiplex (WDM)-based metropolitan area networks (MANs), dark fiber turnkey solutions, and complete managed services. The current access solutions include: wireline access (MAN, local private line, dial, integrated access), broadband access (digital subscriber loop [DSL] access, Ethernet) wireless access (802.16-based broadband wireless), and satellite access services.

The managed access solutions for Agencies include the capabilities to analyze, model/simulate, design, deploy, deliver, and manage Agencies' access solutions. Wireline, broadband, wireless, and satellite solutions are available to match Agencies' unique requirements and further increase service reliability, availability, and flexibility.

The access arrangements can be considered interchangeable, meaning that any arrangement chosen will be able to deliver any type of service chosen by the Agency to the select SDP. **Table 1.3.2.a-1** summarizes the availability of access arrangements that AT&T provides for Agencies. The performance objectives of our service meet or exceed leading industry practices for service reliability.

ACCESS CATEGORY	ACCESS TYPE	AT&T ACCESS AVAILABILITY (NOTE 1)	LEADING INDUSTRY PRACTICES AVAILABILITY
Wireline	Point-of-presence (POP)-to-SDP Total Service – single path (routine)		99.9%
	POP-to-SDP Total Service – diverse paths (critical)		99.995%
	POP-to-SDP Coordinated Access – single path (routine)		99.5%
	POP-to-SDP Coordinated Access – diverse paths (critical)		99.995%
Broadband	xDSL		99.8%
	NMLI		99.9%
	Cable		
	FTTP		
Wireless	802.16 Broadband Wireless		99.9%
	802.16d/e WiMax		

	Free Space Optics		99.9%
	OFDM		99.95%
Satellite	VSAT		99.5%

Note 1: Data provided to present AT&T's historical performance to date.

Table 1.3.2.a-1: Service Availability for Access Arrangement Types. Agencies can select the access types that best suit its needs with confidence that access arrangement will provide quality connectivity between the AT&T POP and the Agency SDP that meets or exceeds industry best practices.

The characteristics of each access arrangement type are discussed in more detail in the following sections.

1.3.2.a.1 Wireline Access

AT&T is committed to offering our customers a variety of access types to obtain the most cost-effective wireline access service offered in the market.

Table 1.3.2.a-2 summarizes the types of wireline access arrangements that are available to Agencies:

WIRELINE SERVICE TYPE	FEATURE	BENEFIT	TECHNOLOGY
<ul style="list-style-type: none"> Agency-provide xLEC Access (Incumbent Local Exchange Carrier [ILEC] or Competitive Local Exchange Carrier [CLEC]) 	Baseline Service	Lower cost, Agency-managed	<ul style="list-style-type: none"> Synchronous optical network (SONET) Add-Drop Multiplexers (ADM) Multiservice Provisioning Platforms (MSPP)
<ul style="list-style-type: none"> AT&T-provided xLEC Access AT&T-provided Managed Access Ring (ACCU-Ring) 	Total or Coordinated Service Deployed by xLEC or AT&T Ring Architecture for Resilient Access	AT&T managed to provide high quality Deployed and monitored by AT&T	
<ul style="list-style-type: none"> AT&T Local Network Services AT&T UltraAvailable Access 	Fiber On-Net Locations Ring Architecture for Resilient Access Fiber On-Net Locations Interfaces include Native IT (ESCON, FICON, FC, GigE, D1, FDD1); Fiber Channel; DS-1/DS-3; OC-3, OC-12, OC-48, and OC-192; Fast Ethernet; D1 Video.		<ul style="list-style-type: none"> Metro Dense Wave Division Multiplexing (DWDM) Multiservice Provisioning Platforms (MSPP)

Table 1.3.2.a-2: Wireline Access Arrangement Summaries. Agencies select from a diverse set of high-quality wireline access arrangements to support their mission requirements.

The wireline access arrangement to connect to the AT&T backbone will be provided in two configurations, as described in **Table 1.3.2.a-3**.

WIRELINE ACCESS CONFIGURATIONS

- **Contractor Provided Access**
 - **Total Service** Access is provided to the Agency SDP as part of the AT&T local network services (LNS) network.
 - **Coordinated Service** Access to the Agency SDP arranged by way of a CLEC or the regional ILEC, where access connectivity by the AT&T LNS network is not feasible.
 - **Agency Provided Access**
 - **Baseline Service** Access from the Agency SDP to either the AT&T POP or a carrier-neutral hotel will be arranged using either the Agency dark fiber-based managed network or Agency- arranged CLEC or ILEC facilities.

Table 1.3.2.a-3: Wireline Access Configurations. Agencies have the flexibility to choose between contractor-provided or Agency-provided access configurations.

For on-net connectivity (local network services, on-net accruing, or UltraAvailable), the circuit goes through [REDACTED] and then is dropped off at the destination location (Agency SDP). The circuit is provisioned in a SONET ring configuration for transport protection. If a fiber cut occurs on the primary path, the circuit automatically switches to the back-up path.

To enhance the reliability of the access network, circuits are engineered to ride over diverse fiber routes that are separated horizontally a minimum of 50 feet and vertically a minimum of 3 feet. All fiber cables are installed in a duct of either high-density polyethylene (HDPE) inner duct or polyvinyl chloride (PVC) rigid duct.

Wireline access arrangement is available at speeds ranging from sub-DS0 to OC-192 and on three different service levels. **Table 1.3.2.a-4** describes the feature sets available for three different POP-to-SDP arrangements.

	Access Option	POP-TO-SDP TOTAL SERVICE	POP-TO-SDP COORDINATED ACCESS	POP ACCESS BASELINE SERVICE
•	Description	With POP-to-SDP total service, the access arrangement and all management services is provided between the Agency SDP and AT&T's POP, including design,	POP-to-SDP coordinated access allows AT&T to obtain local access connectivity from another provider as well as managing that	With POP access baseline service, Agencies provide their own access arrangements into AT&T's POP. Under POP access baseline service, Agencies handle their own service,

	ordering, installation, maintenance, and customer support.	service. AT&T oversees ordering, installation, maintenance, and customer support.	support, design, implementation, testing, and maintenance issues independently.
<ul style="list-style-type: none">• Access Connection	Agencies have the choice of a single or diverse dedicated physical connection into AT&T's POP, providing access to a wide array of voice and data services.		Agencies have their own managed, dedicated physical connection into AT&T's POP, providing access to a wide array of voice and data services.
<ul style="list-style-type: none">• Design and Engineering	Agencies benefit from the design of access solutions from the ground up, based on their unique information and performance requirements.		
<ul style="list-style-type: none">• Implementation	AT&T representative works closely with the Agency to plan and implement a timely and successful installation process, from design through testing and turn-up.		
<ul style="list-style-type: none">• Proactive Maintenance and Testing	AT&T monitors the Agency's access continuously, resolving any problems that occur as quickly as possible.		
<ul style="list-style-type: none">• Single Point of Contact	Agencies can contact their service center at any time through a single toll-free number where the technician the Agency talks to assumes ownership of any reported problem and takes steps to resolve it, providing the Agency with hourly updates until it is resolved.		
<ul style="list-style-type: none">• High Service Standards	AT&T provides Agencies with the exceptional reliability supported by the SONET- based architecture that will provide highly available services		

Table 1.3.2.a-4: POP-to-SDP Arrangements Available Feature Sets. Agencies can choose the POP-to-SDP Arrangement best suited to meet mission needs.

1.3.2.a.2 Broadband Access [L.34.1.3.2.a.2]

Broadband access is supported using DSL technology and native mode local area network (LAN) interconnect (NMLI). Each delivers Ethernet interfaces to the SDP demarcations. **Table 1.3.2.a-5** summarizes the broadband access options.

ACCESS DELIVERY TYPE	FEATURE	BENEFIT	TECHNOLOGY
• DSL Service	Offered in [REDACTED] in the contiguous United States (CONUS) region	Faster access to the Internet than is available from dial, integrated services digital network (ISDN), and low-speed fractional T1 service	Symmetric digital subscriber line asymmetric digital subscriber line ISDN digital subscriber line
• Native Mode LAN Interface Service - MAN	Ethernet handoffs cover [REDACTED] and [REDACTED]	Flexible service allows for varying levels of redundancy/diversity at Layer 1	[REDACTED]
• Native Mode LAN Service - WAN	approximately [REDACTED] with more than [REDACTED] on-net for broadband access	Enables LAN-to-LAN connectivity between Agency locations over the wide area network (WAN)	[REDACTED]

service delivery

Table 1.3.2.a-5: Broadband Access Arrangement Summaries. DSL and NMLI services offer Agencies high-speed access service with extensive coverage.

1.3.2.a.3 Wireless Access

Table 1.3.2.a-6 summarizes the types of wireless access arrangements that are available to Agencies.

ACCESS DELIVERY TYPE	FEATURES	BENEFIT	TECHNOLOGY
<ul style="list-style-type: none"> Microwave (802.16) 	<ul style="list-style-type: none"> T1, T3, and OC-3 bandwidths Protocol independent Available in [REDACTED] Encrypted transport Small, inexpensive antennas 	<ul style="list-style-type: none"> Agency-specific access solution Fast service deployment Diverse access solution – not wireline High-availability secure transport 	38 GHz licensed-spectrum; POP, line-of-site configurations
<ul style="list-style-type: none"> Fixed Satellite 	<ul style="list-style-type: none"> Dedicated (permanent) or ad hoc (reservation-based) satellite bandwidth Simplex (one-way) and duplex (two-way) transport to nearly any point on earth 	<ul style="list-style-type: none"> Global connectivity of remote SDPs to network POPs Immediate link establishment without need of local terrestrial networks 	<ul style="list-style-type: none"> C-Band: Uplink - 5.850 to 6.425 GHz; Downlink – 3.625 to 4.2 GHz; Bandwidth – 500 MHz Ku-Band: Uplink – 14 to 14.5 GHz; Downlink – 10.95 to 12.2 GHz; Bandwidth – 500MHz

Table 1.3.2.a-6: Wireless Access Arrangement Summaries. Wireless access provides access for Agencies with remote locations and diversity to Agencies with existing wireline, increasing their access resiliency.

The reliability, cost-effectiveness, flexibility, ease, and speed of deployment make wireless access a viable substitute or complement to wireline (fiber-based) solutions.

1.3.2.a.3.1 Future Broadband Wireless Offerings

AT&T continually investigates new broadband wireless technologies to be used within our network infrastructure. Technologies, such as free space optics, have been used by AT&T and our customers for several years, while WiMax is in testing to verify the technology will meet AT&T's demanding service quality standards. **Table 1.3.2.a-7** list possible future wireless services offerings AT&T is testing.

TECHNOLOGY	DESCRIPTION AND BENEFITS
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

	<ul style="list-style-type: none"> • Benefits from broad industry support
Free Space Optics	<ul style="list-style-type: none"> • Very hard to intercept – encryption still recommended
OFDM	<ul style="list-style-type: none"> • Suitable alternative for fiber when construction is not feasible

Table 1.3.2.a-7: [REDACTED] **Access Technologies.** [REDACTED]

Descriptions of future wireless access technologies are provided below.

1.3.2.a.3.1.1 [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Figure 1.3.2.a-2 [REDACTED]

Figure 1.3.2.a-2: Sample Architecture.

1.3.2.a.3.1.2 Space

1.3.2.a.3.1.3 [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

1.3.2.b Peering Relationships [L.34.1.3.2.b]

(b) Describe the arrangements that the offeror has with other service providers for carrying and exchanging traffic, including peering and "roaming" arrangements. Describe the impacts on quality and reliability of such arrangements. [L.34.1.3.2.b]

1.3.2.b.1 IP Peering

AT&T's peering goal is to provide excellent performance to all destinations in the Internet worldwide. AT&T's IP network is default-free," which means that traffic that leaves the AT&T U.S. IP network flows directly on peering connections or customer connections. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

1.3.2.b.1.1 U.S. Private IP Peering

Domestically, private peering is the most commonly used method of interconnection between major ISPs. As a Tier 1 ISP, AT&T has in place peering relationships with all major ISPs.

- *High-quality IP service requires that off-net IP traffic reach the destination host through the*

Peering with all major Tier 1 ISPs allows AT&T's IP network to pass off traffic bound for these other networks, or customers, on the shortest route, and as quickly and efficiently as possible. This translates into increased performance and a reduction in apparent latency to the end user.

Table 1.3.2.b-1 lists AT&T's private peering features and how they provide Agencies the benefits of interfacing with a Tier 1 provider.

PEERING FEATURE	IMPACT ON QUALITY & RELIABILITY	AGENCY BENEFIT
Default-Free Private Peering	IP routes are exchanged freely through private peering. Latency and packet loss are minimized by allowing AT&T to select optimal peering point to exchange traffic.	All traffic leaving AT&T U.S. IP network flows directly on peering or Agency connections, providing low-latency connections for Agency end users
Tier 1 ISP Peering	Provides higher quality, lower latency IP transport because majority of off-net traffic only traverses Tier 1 peering partner's network to reach destination host	AT&T has arrangements with other Tier 1 ISPs, which allow AT&T to keep network overhead low, translating to lower bottom line cost to Agencies
OC-12 and OC-48 private peering links at multiple, geographically dispersed locations	<ul style="list-style-type: none"> Latency and packet loss are minimized through multiple high-capacity peering-links Geographic diversity provides increased service reliability through alternative exchange points 	High-bandwidth private peering links at a minimum of three locations enables the most efficient traffic flow from AT&T IP network to other ISP networks, providing Agencies with superior network availability and minimum downtime

Table 1.3.2.b-1: Private Peering Features/Benefits. Agencies will receive high-quality and highly-reliable IP service from AT&T's private peering arrangements.

1.3.2.b.1.2 Domestic Peering Strategy

AT&T's peering architecture focuses on maintaining excellent performance to anywhere on the Internet by routing [REDACTED] of all Internet-bound traffic on private peering links and carefully managing capacity on these links so as [REDACTED] [REDACTED] Keeping usage low, and peering with other Tier 1 ISPs at [REDACTED] minimizes the chance of network congestion. This relates to increased IP-network availability for Agencies and their end users. **Figure 1.3.2.b-1** shows the domestic peering locations, including the number of connection links and total throughput.

Figure 1.3.2.b-1: Domestic Private Peering. [REDACTED]

1.3.2.b.1.3 Peering Diversity

AT&T peers at multiple locations with OCX facilities, [REDACTED]
[REDACTED] Peering at multiple, geographically-dispersed locations [REDACTED]
[REDACTED] enables a highly efficient traffic flow from the AT&T network to the other ISP networks. AT&T has led the industry in the installation of high-bandwidth private peering links and has numerous [REDACTED] private peering links in place throughout the U.S. These relationships provide Agencies with the bandwidth needed to support mission needs.

1.3.2.b.1.4 Global Peering

The AT&T global IP network is connected to other ISPs on massive private peering bandwidth. AT&T's global IP network reaches [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] AT&T's global IP peering

arrangements are discussed in further detail in Section 1.3.4, *Non-Domestic Services*.

1.3.2.b.1.5 Peer Monitoring

Agencies benefit from enhanced reliability of the AT&T IP backbone through development of a tool called PeerMon. PeerMon helps the AT&T IP backbone to be reachable throughout the Internet. Unique in the industry, PeerMon was developed to support the AT&T IP backbone and is always reachable throughout the Internet. Featured in the December 2000 issue of *Network Magazine*, PeerMon monitors route advertisements from key peers' networks, and compares them to the routes that AT&T advertised to verify the routes were not modified in the peer's network. While no ISP intends to cause routing problems in its own or other ISPs' networks, the complexity of the standard router interface makes it difficult to avoid mistakes.

1.3.2.b.2 Roaming

1.3.2.b.2.1 GSM Architecture and Roaming

- *Global mobility and roaming for Agency personnel is enabled through GSM technology, which serves over one billion users in 200 countries with over 600*

AT&T Networkx Team's Cingular network's architecture platform is based on GSM technology. GSM supports 79 percent of the world's mobile phones users, serving over one billion users in 200 countries over 600 networks. Using the AT&T/Cingular solution, Agencies' employees can roam onto more wireless networks than all other wireless technologies combined. GSM's architecture is specifically designed to streamline the roaming experience by incorporating a subscriber identity module (SIM) chip into the subscriber equipment. This chip uniquely identifies the user and associated home network to any visited networks. Roaming within North America is seamless, and requires no input from the subscriber.

When Agency subscribers are outside North America, the GSM architecture makes it possible to use multiband cellular devices to seamlessly roam on other networks throughout the world, even when those networks use different frequencies from those in North America

The economies of scale, captured by the GSM subscriber equipment market, have given rise to affordable multiband GSM phones. These phones allow Agency personnel to roam internationally with their normal, familiar handset. Agency users need not make special arrangements with foreign operators for international roaming service. Users' normal telephone number follows them and operates normally when registered on foreign networks. Compatible GSM networks on which Agency employees can roam are available in over 160 countries. Cingular carefully monitors the performance of their roaming partners, as described in **Table 1.3.2.b-2**.

PEERING PARTNER PERFORMANCE METRIC	DESCRIPTION
Dropped Calls	Measure of the digital calls dropped due to bit error rates, failed handoffs, or hardware failures. Dropped calls not to [REDACTED]
Service Denied	This customer perceived metric indicates that a valid subscriber attempts to correctly dial a valid number, and should have received a successful voice channel assignment, but did not. The metric is derived from access attempt failures above threshold and voice channel congestion. [REDACTED]
Network Availability	Total of all base station outages measured in hours divided by the total number of base stations times 24 hours [REDACTED]

Table 1.3.2.b-2: Peering Partner Performance Metrics. *Peering partners are under contractual agreement to provide service quality that meets or exceeds the Peering partner performance metrics.*

A list of non-domestic GSM network carrier bilateral agreements is presented in Appendix D, Bilateral and Other Carrier Agreements, Table D-2.

1.3.2.b.2.2 Data Service Roaming and Remote Access

Mobility and remote access is changing the way the Government does business with remote users and teleworkers. AT&T is building partnerships to provide the infrastructure for mobile data usage.

- Agency personnel require global remote access to their

Two virtual private networking (VPN) solutions are provided for remote users and teleworkers – AT&T VPN tunneling service (AVTS) and AT&T Network based IPVPN remote access service (ANIRA). Both services allow the remote users/teleworkers to enable a secure connection to their host application or corporate network through a variety of remote access options.

Both AVTS and ANIRA offer remote users the ability to build an IPSecurity (IPSec) tunnel back to a corporate server, allowing for encrypted, secure communications. AVTS also offers secure sockets layer (SSL) encryption for remote users for the purpose of securing web applications. In either case, remote users have a variety of access methods to connect to corporate networks and applications through AT&T's extensive dial access POP, arrangements to exchange traffic with broadband providers (cable and digital subscriber line [DSL]), and agreements with WiFi service providers. **Table 1.3.2.b-3** summarizes the data remote access options available to the Government.

**DATA ROAMING:
REMOTE ACCESS**

DESCRIPTION AND BENEFITS

Dial Access	Extended dial access, offered through third-party providers, expands roaming coverage
DSL Access	Offered in the CONUS region and in
Broadband Wireless - WiFi	Services at access points (also referred to as hot spots) in - giving Agency personnel the convenience and choice to connect at a broad range of locations.
Broadband Wireline - Ethernet	Through, over wired Ethernet locations accessible from worldwide. Mobile Agency data users will be able to connect on high-speed Ethernet, allowing the user to be more productive from a remote location.

Table 1.3.2.b-3: Data Roaming Remote Access. Agency personnel will remain connected, while roaming globally with AT&T's data roaming services. AT&T has partnered with service providers throughout the world to provide an extensive roaming footprint for our subscribers.

Regardless which form of remote access users choose, or which AT&T Networkx Team partner is providing the wireless link, all such connections to other AT&T IP services are set up and managed by one simple, unified software application—the AT&T global network client. When Agency personnel need to initiate a link to IP services while traveling, the global client provides an organized and familiar method for obtaining a remote connection.

From the AT&T global network client, Agency subscribers can create connections and manage any partner's access service that is locally available, including dial-up, ISDN, cellular, and broadband services, as well as 802.11 wireless networks as ingress to IP services. The client software even helps users locate hotspots, and provides feedback on the link status, quality, and signal strength.

1.3.2.c Congestion and Flow Control Strategy

[L.34.1.3.2.c]

(c) Describe the congestion and flow control strategy(ies), including control mechanisms, and redundant switch, router, base station, and transmissions facilities. Describe the flexibility inherent in the architectural design to handle predicted and unpredicted traffic loads. Also discuss the architectural ability to maintain service quality during switch, router, base station, and transmission failures. [L.34.1.3.2.c]

- *Network resiliency and reliability are especially critical to Government Agencies during emergency situations.*

Agencies require service providers who have well-designed, intelligent, and resilient networks to support the Federal Government's mission-critical

and routine needs. AT&T will provide Agencies with a reliable, high-quality network with a difference: it is the result of a deliberate approach to design in resilience at each layer of AT&T's worldwide infrastructure. Network resilience allows AT&T to handle congestion from unpredicted traffic volumes and link/node failures caused by extraordinary events that exceed normal design parameters. AT&T's congestion and flow control strategy provides service quality and reliability as follows:

- Design, build, and operate the network to deliver the capacity when and where customers need it.
- Use expert intelligence in tools and OSS to monitor and flexibly manage network usage for performance optimization.
- Implement an all-layer reliability and restoration capability to maintain service quality and protect against network failures.

AT&T's congestion and flow strategy are summarized in **Table 1.3.2.c-1**.

CONGESTION AND FLOW CONTROL STRATEGY

	<ul style="list-style-type: none"> • Modeling & Simulation 	<p>Network Modeling and Intelligent Operational Support Systems</p> <p>Intelligent modeling and simulation of network congestion and flow control provide a resilient and flexible network and service design.</p>
	<ul style="list-style-type: none"> • Network Monitoring and Feedback 	<p>Switch operational measurements are collected and compared against projected values. Models are refined and revalidated, and new control mechanisms, rules, configurations, facilities, and service changes are applied to the network, as required.</p>
	<ul style="list-style-type: none"> • Linear Transmission Systems 	<p>Transmission Network – Congestion and Flow Control Strategy</p> <p>Restoration and Provisioning Integrated Design System (RAPIDSM) and Fast Automatic Restoration (FASTARSM) systems correlate alarm data from network devices, reroute traffic based on prioritization and reserved available capacity, and support post-repair reversion to original facilities.</p>
	<ul style="list-style-type: none"> • SONET Transmission Systems 	<p>Two fibers of the four-fiber, bidirectional, line-switched rings (BLSR) are for protection, which provides self-healing restoration capabilities. In the event of failure, traffic is automatically switched to a fully redundant backup facility, typically in less than 60 milliseconds.</p>
	<ul style="list-style-type: none"> • Optical Network Systems 	<p>Each node is connected through a full mesh point-to-point network and uses an OSPF-based signaling and routing algorithm to develop a state map of neighboring nodes to automatically reroute traffic at ring-like speeds in the event of a node or link failure.</p>
	<ul style="list-style-type: none"> • Real-time Network Routing (RTNR) 	<p>Voice Network – Congestion and Flow Control Strategy</p> <p>4ESS central offices switches exchange real-time link status information to determine, on a call-by-call basis, the availability and network traffic load conditions of the direct and two-link routes to the destination, thereby minimizing blocking and call setup time.</p>
	<ul style="list-style-type: none"> • Global Network Operations (GNOC) 	<p>Restrictive, protective, and expansive network management call controls used by the GNOC over the 4ESS, edge, and local end-office switches to minimize congestion, when congestion exceeds RTNR capabilities.</p>
	<ul style="list-style-type: none"> • Mobile Switching Centers (MSC) 	<p>Wireless Network – Congestion and Flow Control Strategy</p> <p>Core network elements are load balanced and geographically separated to provide the highest availability, scalability, and reliability. Redundant hardware configurations allow network to reconfigure to bypass damaged equipment.</p>
	<ul style="list-style-type: none"> • Redundant Network Connections 	<p>Multiple DS1s connect base stations to a region. Two MSCs per region. Multiple diverse DS-3s connect a region to the asynchronous transfer mode (ATM) backbone transport network.</p>
	<ul style="list-style-type: none"> • Class of Service (CoS) 	<p>Data Network – Congestion and Flow Control Strategy</p> <p>AT&T offers our customers four classes of service and uses multiple priority and discard algorithms to differentiate services to our customers. This CoS is used at all routing platforms, rather than just at the edge of the network.</p>
	<ul style="list-style-type: none"> • Capacity Management 	<p>Proactive monitoring of backbone and peering links maintains traffic levels at or below 50% usage.</p>
	<ul style="list-style-type: none"> • Redundant Equipment 	<p>Redundant routers and switch configurations allow traffic to reroute if a node fails. All routers and switches have dual processors, redundant port cards, and dual power supplies</p>
	<ul style="list-style-type: none"> • Core Survivability 	<p>Network Resiliency</p> <p>Network core backbones are designed to be single-link and single-node survivable to the extent there are no single points of failure.</p>
	<ul style="list-style-type: none"> • Equipment Redundancy 	<p>Equipment redundancy at the trunk, switch, and card levels maintain service continuity in the event of congestion overloads or component failures.</p>
	<ul style="list-style-type: none"> • Separation of Functions 	<p>To improve network performance and reliability (i.e., separate data and control planes as in generalized multiprotocol label switching [GMPLS] or SS7)</p>
	<ul style="list-style-type: none"> • Certified Facilities and Equipment 	<p>Use of AT&T-owned facilities and infrastructure, when available, and of suppliers' facilities that meet service quality metrics and measurements, reliability, and diversity options, and offer competitive value.</p>

Table 1.3.2.c-1: Congestion and Flow Control Strategy. Agencies benefit from a comprehensive congestion and flow control strategy that allow the AT&T network to handle predicted and unpredicted traffic loads.

1.3.2.c.1 Congestion and Flow Control

AT&T's network reliability strategy is to design, deploy, and operate intelligently and cost-effectively primary and alternative facilities and functionality at each layer of its worldwide service infrastructure. This

- Current Analysis**
- "AT&T is the largest long-distance service provider in the U.S. and is the best-known brand name in telecommunications worldwide. AT&T has one of the most extensive and far-reaching networks in the world, supporting a wide portfolio of business and consumer voice, data and Internet services."
 - June 30, 2005

achieves support for routine and surge usage, so that its annualized network availability

approaches 99.999 percent. Network congestion generated by unpredicted traffic that exceeds planned capacity (and by link or node failures) scales in size, as a network expands beyond regional or national scope. Techniques to mitigate the effects of congestion through the use of flow controls or rerouting of excess traffic to

spare or unused network capacity is one dimension of a recovery response. A more layered and resilient approach is required for a global network.

1.3.2.c.2 Network Modeling and Intelligent Operational Support Systems

AT&T's approach to network design incorporates intelligent modeling and simulation tools to help build resiliency and flexibility into its networks. By running successive scenarios that progressively stress a network design in its ability to respond to varying levels of traffic, AT&T determines how to flexibly design and engineer a network to meet performance goals and customers' expectations for reliability.

As shown in **Figure 1.3.2.c-1**, AT&T's three loop network control model takes into consideration multiple complex factors (e.g., congestion from unpredicted traffic, facilities sizing, service reliability) and addresses how aspects of network control, capacity management, and planning affect network performance.

The intelligent modeling process

Figure 1.3.2.c-1: Network Model. AT&T's network model depicts how modeling and operational feedback of multiple complex factors play a role in superior network performance, reliability, and management.

continues after a network has been deployed and is operational. Operational measurements (OM) are collected and compared against projected values, and the models are refined and revalidated. As a result, the network control mechanisms, rules, configurations, and facilities are optimized to better support network congestion and managed flow control.

In addition to modeling and performance monitoring, AT&T's intelligent operational support systems (e.g., artificial intelligence, self-healing/self-identifying network elements, expert systems, rules-based processes) allow the network and operations support staff to respond faster to network congestion and flow control events. For example, congestion and flow control events can occur along several dimensions within the network, namely the element level, path level, and service level. Reporting and responding to

faults in isolation can affect other levels of the network and adversely impact the network congestion and flow control.

AT&T's OSS addresses the multidimensional aspect of the network through intelligent fault management correlation systems. These allow the Network Operations Center (NOC) to rapidly identify the root cause of related events and level of service impact, so a single ticket is generated with service impact information. Through the introduction of rules-based intelligence into tools and OSS, such as fault management correlation, AT&T significantly enhances its capability to handle predicted and unpredicted traffic loads.

1.3.2.c.3 Transmission Facilities Restoration Mechanisms

AT&T's transmission facilities consist of more than 77,000 route-miles, with 55,453 route-miles handling long-distance traffic, 21,887 route-miles supporting local services, and an additional 14,800 miles of the latest generation of fiber capable of supporting OC-768 (40 Gbps) traffic. With an intelligent optical network of more than 135 OC-192 nodes using full mesh point-to-point SONET, more than 8,900 SONET rings, and SONET linear chain systems, AT&T handles nearly 4.5 petabytes of traffic, including 2.3 petabytes of IP traffic every day.¹ To manage customers' network traffic reliably, AT&T uses intelligent systems – RAPID and FASTAR, SONET BLSR, intelligent optical network – that facilitate network self-healing to support Agencies' missions.

1.3.2.c.4 Switch Facilities and Routing/Congestion Mechanisms

To provide voice services, AT&T's long-distance network supports both circuit and packet switching for voice services. The network includes about 362 voice switches, including 156 local circuit switches deployed in 92 cities, 138 traditional longhaul central office switches, and 68 long-distance circuit

¹ Current Analysis, AT&T Company Assessment, June 30, 2005

switches that are packet (IP) capable. AT&T's global voice network carries more than 430 million local and long distance calls per day, more than 310 billion in annual minutes, and reaches over 230 countries. Congestion and call flow are dynamically managed through the RTNR system and manually through restrictive, protective, and expansive network call management controls implemented by the NOC. Expansive controls allow the routing to expand beyond the normal in-chain routing during failure or overflow conditions. Protective controls are used to control the spread of congestion in the network by restricting normal trunk access and overflow. Restrictive controls are used to limit the effects of network congestion and maintain network traffic throughout at high levels.

1.3.2.c.5 Wireless Routing/Congestion Mechanisms

AT&T Networkx Team's Cingular has a dedicated national ATM backbone and a wireless infrastructure of 32,000-plus base station subsystems (cell sites) to provide national GSM voice and general packet radio services/enabement and debugging of growing enterprises (GPRS/EDGE) data services to its 50 million subscribers. Service providers connect to Cingular by strictly controlled VPNs or dedicated network circuits. These are subject to intrusion detection/prevention at the edge of the network. Within its national network, core elements are load balanced and geographically separated to provide the highest availability, scalability, and reliability. Cingular uses a combination of T-spans, coaxial cable, fiber, and microwave links for transmission between cell sites and mobile switching centers (MSCs). The use of dedicated lines for landline links means they will not be affected by heavy non-wireless traffic during emergencies.

Extensive redundancy is designed into Cingular's MSCs, including redundant vital hardware. If a node failure occurs, the network is flexible enough to be

reconfigured to bypass damaged equipment. A minimum of two MSC call servers per region are deployed and geographically separated. A maximum of 200 node base stations (BS) per regional network center (RNC) are supported to limit geographical boundaries for single point of failure. Each node BS connects to one of Cingular's four geographically separated regional data centers (Schaumburg, Illinois; Bothell, Washington; Allen, Texas; and Atlanta, Georgia) on a pair of T1s for load balancing and reciprocal failover capability. RNCs are linked by multiple diverse DS-3s to the backbone ATM network, two national datacenters (NDC) and Cingular's Wireless Network Control Center (WNCC).

1.3.2.c.6 Router Facilities and Routing/Congestion Mechanisms

AT&T continues to expand its global IP/MPLS infrastructure to support a consistent set of services throughout the U.S. and more than 150 countries. The global IP/MPLS network is designed to exclude any single point of failure in the routers, switches, and multiplexers. If a single backbone facility fails, the network is engineered for sufficient capacity to reroute traffic to alternate facilities. All traffic transiting a failed node will be automatically rerouted around that node on alternate paths. Additionally, the IP/MPLS network design incorporates diverse facility connections, so the loss of a single cable will not bring the network down.

Within the AT&T global network (AGN), reliability is enhanced with redundant equipment. All routers and switches have dual processors, redundant port cards, and dual-power supplies. Service-affecting hardware elements are spared within the node and are fully operational. Redundant equipment configurations allow traffic to reroute in the event of a node failure.

AT&T proactively engages in capacity management to give IP networks time division multiplexing (TDM)-like reliability and manage congestion through

traffic engineering. AT&T's Network Operations proactively analyze three areas when performing capacity management associated with the global IP network: backbone and peering links, and access router port capacity, as summarized in **Table 1.3.2.c-2**.

AT&T CAPACITY MANAGEMENT

Operations Monitoring and Flexible Response

- **Backbone Links** Facilities are carefully monitored so when links reach a peak of 50% usage, AT&T's Network Operation teams perform extensive trend analyses to determine the need for routing adjustments (to shift traffic to less congested facilities) or for additional capacity.
- **Peering Links** To minimize the effects on network performance and congestion, AT&T deployed the first OC-48 peering circuit in late 2000, and now has several in service. AT&T has also developed partnerships with top ISPs to review traffic requirements and patterns, on a weekly basis, to plan jointly how to augment capacity in advance of traffic increases.
- **Access Router Ports** AT&T's maintains spare port capacity ranging from 15-30%, depending on the port size and geographic service growth forecasts to rapidly respond to customer needs.

Table 1.3.2.c-2: Capacity Management. *AT&T's capacity management allows AT&T network operations staff to perform traffic engineering to avoid, proactively, situations that increase the likelihood congestion.*

To provide high reliability, the capacity management organization runs a special AT&T-developed tool that performs a survivability analysis on the entire network's backbone links. This tool simulates potential facility failures and determines where traffic would be rerouted if a given link failed. This analysis enables the capacity management organization to provide sufficient capacity to survive a facility cut anywhere.

In addition to capacity management, AT&T implemented quality of service (QoS) within its IP/MPLS network to manage congestion and flow control associated with the emerging requirements to support real-time, delay-sensitive applications over IP. AT&T's approach to provide quality for time-sensitive traffic is described in Section 1.3.2.e, Approach to Ensure Time-Sensitive Traffic Quality.

1.3.2.c.7 Network Reliability and Restoration Capability

To enable Agencies to receive reliable service during a period of network congestion or in the event of a network failure, AT&T uses a layered protocol as an approach for complete protection (**Figure 1.3.2.c-2**).

Figure 1.3.2.c-2: AT&T Reliability Pyramid. *A layered protocol offers layered protection.*

1.3.2.d Approach to Perform Service Delivery Verification [L.34.1.3.2.d]

(d) Describe the offeror's approach to perform verification of individual services delivered under the contract, in particular the testing procedures to verify acceptable performance and Key Performance Indicator (KPI)/Acceptable Quality Level (AQL) compliance.] [L.34.1.3.2.d]

- The service verification facilitates performance-based

- *The service verification facilitates performance-based*

The first time a service is provided through the Network contract, the performance must be verified with the GSA and the Agencies. The service KPIs will be monitored to certify that the service performance complies with the AQL. ■

AT&T's approach to perform verification of Networx services is summarized in **Table 1.3.2.d-1**.

PERFORMANCE VERIFICATION ACTIVITIES	DESCRIPTION AND BENEFITS
Verification Testing	<p>Field Testing – Testing a service against previously developed test plans. Field testing include the following tests: field verification, network verification, network management verification, and service verification.</p> <p>██████████ – Integrated testing platform tool that automates a field test cycle, including performance and reliability.</p> <p>██████████ Provides real-time and historical performance reporting for AT&T services.</p>
Performance Verification Process	<p>Verification Process – Standard process followed to verify performance of an individual Networkx service.</p>
Network-Level Reports	<p>Network Performance – Real-time network performance statistics, such as delay or packet loss. Collected ██████████ by network performance monitoring system and displayed on a web interface.</p>

Table 1.3.2.d-1: Service Performance Verification. Verification of individual services is captured through the verification testing process. ██████████ or network-level reports provide tools to capture KPI data. Although verification starts when a service is first delivered, the process continues throughout the lifetime of the service.

1.3.2.d.1 Service Assurance Architecture

To maintain high-quality service and verify that service performance meets the KPIs, AT&T has implemented an integrated service assurance system. The architecture of the service assurance system (**Figure 1.3.2.d-1**), integrates fault monitoring and performance management with rules-based event processing, automated ticketing, and service testing. Each layer of the service assurance architecture is comprised of subcomponents that perform a specific role in maintaining service quality. The service assurance architecture components and subcomponents are described in **Table 1.3.2.d-2**.

Figure 1.3.2.d-1: Service Assurance Architecture.

SERVICE ASSURANCE ARCHITECTURE COMPONENT	DESCRIPTION
Network Elements (NE), Element Management System (EMS), and Collector Devices	<p>Network components that generate fault and performance data or respond to event processing commands:</p> <ul style="list-style-type: none"> • <i>Network Devices</i>: switches, routers, optical equipment • <i>Element Management Systems</i> • <i>Probes</i>: Performance management and fault monitoring collection devices in network
[REDACTED]	<p>Service Assurance component that provides fault monitoring, correlation and analysis capabilities:</p> <ul style="list-style-type: none"> • <i>Collection</i>: [REDACTED] • <i>Correlation & Analysis</i>: [REDACTED]
[REDACTED]	<p>Service Assurance component that provides performance monitoring, management, and reporting capabilities to verify KPIs:</p> <ul style="list-style-type: none"> • <i>Surveillance</i>: [REDACTED]

SERVICE ASSURANCE ARCHITECTURE COMPONENT	DESCRIPTION
[REDACTED]	<ul style="list-style-type: none"> • <i>Reporting:</i> [REDACTED] • <i>Planning & Control:</i> [REDACTED]
[REDACTED]	Service assurance component that provides ticket lifecycle management and status reporting: <ul style="list-style-type: none"> • <i>Automated Ticket Generation:</i> [REDACTED] • <i>Ticket Assignment:</i> [REDACTED]
[REDACTED]	Service Assurance component that provides automatic service testing, troubleshooting, and network diagnoses: <ul style="list-style-type: none"> • <i>Performance Verification:</i> [REDACTED] • <i>Test Coordination:</i> [REDACTED] • <i>In-service Testing:</i> [REDACTED]
[REDACTED]	Service Assurance component that provides business process automation: <ul style="list-style-type: none"> • <i>Process Automation:</i> [REDACTED] • <i>Event Processing:</i> [REDACTED]
[REDACTED]	Service Assurance component that provides inventory database of network equipment: <ul style="list-style-type: none"> • <i>Equipment Inventory & Data Warehouse:</i> [REDACTED]
Service Portals	Service Assurance components that provide user-friendly interface for reviewing fault and performance data: <ul style="list-style-type: none"> • [REDACTED] Internal web-based systems for reviewing service assurance data
[REDACTED]	[REDACTED]

Table 1.3.2.d-2: Service Assurance System. *Service Assurance is provided through a set of functional systems that act as a single integrated system to collect, analyze, correlate and report on network fault and performance events.*

The multicomponent service assurance system provides the foundation to quickly and effectively perform verification testing and ongoing performance monitoring for Networx services. Web-based service portals allow Agency personnel and AT&T Operations Teams to review the status of the network.

Through automated tools and experienced personnel, Agencies will obtain thorough verification of service performance.

1.3.2.d.2 Service Verification Testing

Service verification test (SVT) is part of field-testing (refer to **Table 1.3.2.d-1** [above]) of a service against the previously developed detailed test plan. SVT is a cycle of tests (e.g., functionality and security vulnerability discovery) that includes reliability and performance tests. AT&T uses its [REDACTED] [REDACTED] a single integrated testing platform, to provide common testing services supporting automation for both pre-service and in-service testing. The SVT is AT&T's methodology for delivering the services in accordance with the Networx-specified KPIs/AQLs.

1.3.2.d.3 Service Verification Process

The Networx RFP defines the process for verifying services against their KPIs. Sixty days after the notice to proceed (NTP), the GSA will receive a Verification Test Plan from AT&T. The Verification Test Plan will detail the standard test procedures used to verify the services, and describe the change procedure for adding service-specific test plan attachments.

Verification testing is performed at the time of initial service delivery to an Agency. Service acceptance testing follows verification testing, when the Verification Test Plan has been executed, and the results approved by the Government. Upon completion of the Verification Test Plan, AT&T must deliver the Service Order Completion Notification (SOCN).

Service verification testing is used to confirm KPIs meet or exceed required AQLs. If one or more of the specified KPIs for a delivered Networx service fails

to meet the associated AQL, then service delivery might be delayed until the specified performance levels are demonstrated. Even after service acceptance, if there is a period of unacceptable performance, service verification testing is performed to demonstrate that the service KPIs meet or exceed the associated AQL. **Figure 1.3.2.d-2** presents the service verification process.

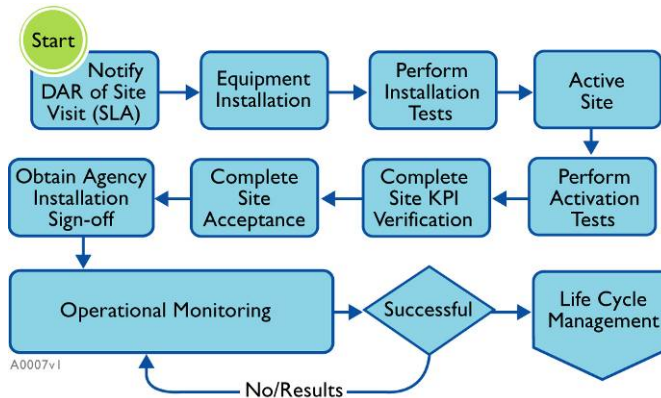


Figure 1.3.2.d-2: Service Verification Process. *Service verification process facilitates performance-based contracting by providing the Government the opportunity to verify that the KPIs of a service meet or exceed the AQLs.*

1.3.2.d.4 Performance Management Operations Support System

Key performance

verification monitors the network and services continuously and collect performance-related data in real-time. AT&T uses

██████ for service performance management integrating a number of tools for performance monitoring and reporting (Figure 1.3.2.d-3).

██████████ provides service-██
specific performance reports that verify service performance against the

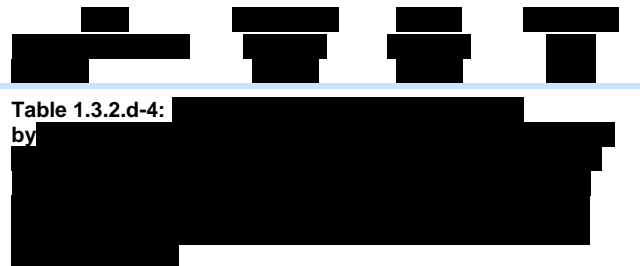
Figure 1.3.2.d-3: Performance Management

KPI/AQL. [REDACTED] provides both real-time and historical performance reports, which are available on a web interface (AT&T **BusinessDirect**). The [REDACTED] architecture components are described in **Table 1.3.2.d-3**.

COMPONENT	DESCRIPTION AND BENEFITS
[REDACTED] Collectors	<ul style="list-style-type: none"> Subcomponents that interact directly with the [REDACTED] Perform three main functions: performance measure collection, aggregation, and performance alert generation, based on analysis and thresholding of the individual measures.
[REDACTED] Real-Time Performance Surveillance Monitor	<ul style="list-style-type: none"> Provides aggregation point for performance alerts and cross-stream correlation, as well as any analysis required for predictive fault determination. Provides a performance surveillance graphical user interface (GUI). Supports analysis to aid trouble isolation and impact analysis.
[REDACTED] End-to-End Reports	<ul style="list-style-type: none"> Provides user interface for performance measures, in both aggregated and drill-down detail formats. Reports are service specific and present KPI/AQL metrics such as: availability, latency, data delivery, usage.

Table 1.3.2.d-3: Service Performance Verification. Verification of individual services is captured through the verification testing process that starts when a service is first delivered, but continues throughout the lifetime of the service. The [REDACTED] or network-level reports provide tools to capture KPI data.

An example of service verification, with respect to KPI/AQLs, is presented in **Table 1.3.2.d-4** for the network-based IP-VPN service.



1.3.2.d.5 Network Level Reports

Some KPIs/AQLs require that the performance of the overall network be measured. For example, latency is a KPI/AQL that is defined for the IPS service. Within [REDACTED], network performance statistics, such as latency, are calculated using a network performance-monitoring infrastructure – [REDACTED] – that collects data from the network every [REDACTED]. These are displayed on a web-based interface.

Figure 1.3.2.d-4 shows AT&T's current network performance IP site.

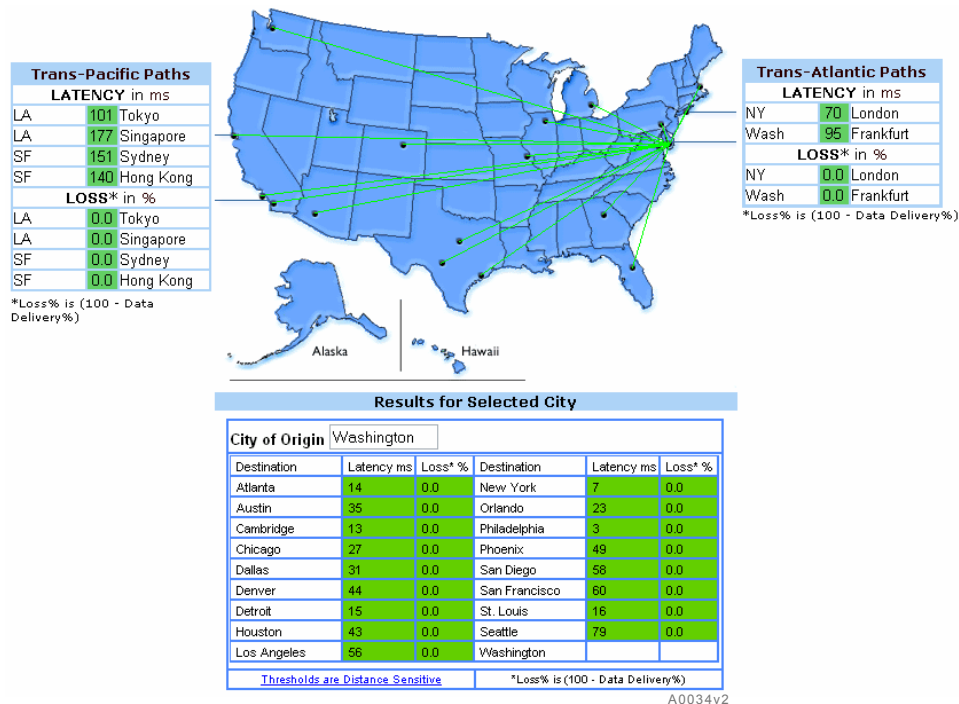


Figure 1.3.2.d-4: Global IP Network Performance Website. The interactive web interface provides verification engineers and Agency personnel with an easy-to-use tool for capturing network-level performance metrics for verification of IP-based services.

Unlike some ISPs who generate pings and trace routes from routers deployed within their IP networks, AT&T has built a separate network measurement infrastructure to measure the performance of its IP network. It more closely captures the real performance that customers experience using our services. For Internet services, AT&T measures the network latency and loss within its global IP network using dedicated measurement servers located in each of the [REDACTED] Data is collected and reported on every [REDACTED]

1.3.2.d.6 Service Performance Dashboard

Certain Networx services are designated as Service Level Agreement (SLA) services with aggregate-based performance metric(s) that will be monitored and reported on a monthly basis. To facilitate the service performance monitoring and SLA process, AT&T will provide the Agency with a monthly

performance dashboard that summarizes the service performance for each KPI.

The monthly performance dashboard allows an Agency to quickly assess if the service performance meets the AQL. **Figure 1.3.2.d-5** provides a sample performance dashboard.

1.3.2.e Approach for Time-Sensitive Traffic Quality

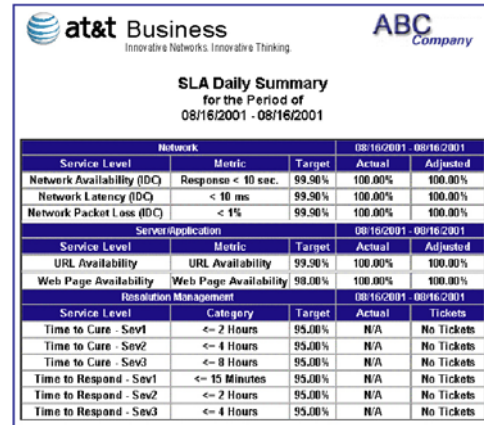
[L.34.1.3.2.e]

Describe the approach to ensure the quality of time-sensitive traffic (e.g., voice quality, video quality, video lip-synch) under different traffic patterns and load conditions on the offeror's network. [L.34.1.3.2.e]

As communications networks migrate to a statistical multiplexing (packet-based) architecture from a TDM (circuit-based) architecture, service quality of time-sensitive traffic must be maintained. In a TDM network, time-sensitive traffic is allocated with dedicated network resources, which enhance quality, but decrease network efficiency. In a statistical multiplexed network, the network resources are shared among all traffic types, which make the network more efficient, but potentially jeopardize service quality of time-sensitive traffic.

AT&T follows a well-defined strategy to provide service quality for time-sensitive-traffic in its statistically multiplexed IP/MPLS-based network. The three mechanisms implemented to support service quality for time-sensitive traffic are as follows:

- *Provisioning* – Continuously engineering the network transport facilities to provide ample capacity during peak periods of use



Network			08/16/2001 - 08/16/2001	
Service Level	Metric	Target	Actual	Adjusted
Network Availability (IDC)	Response < 10 sec.	99.90%	100.00%	100.00%
Network Latency (IDC)	< 10 ms	99.90%	100.00%	100.00%
Network Packet Loss (IDC)	< 1%	99.90%	100.00%	100.00%

Server Application			08/16/2001 - 08/16/2001	
Service Level	Metric	Target	Actual	Adjusted
URL Availability	URL Availability	99.90%	100.00%	100.00%
Web Page Availability	Web Page Availability	98.00%	100.00%	100.00%

Resolution Management			08/16/2001 - 08/16/2001	
Service Level	Category	Target	Actual	Tickets
Time to Cure - Sev1	<= 2 Hours	95.00%	N/A	No Tickets
Time to Cure - Sev2	<= 4 Hours	95.00%	N/A	No Tickets
Time to Cure - Sev3	<= 8 Hours	95.00%	N/A	No Tickets
Time to Respond - Sev1	<= 15 Minutes	95.00%	N/A	No Tickets
Time to Respond - Sev2	<= 2 Hours	95.00%	N/A	No Tickets
Time to Respond - Sev3	<= 4 Hours	95.00%	N/A	No Tickets

T0495v2

Figure 1.3.2.d-5: Performance Dashboard. The performance dashboard provides Agencies with a monthly snapshot of the KPIs for the 16 service-specific SLA services.

- *Time-sensitive traffic requires special treatment in an IP/MPLS-based network.*

- *Classifying* – Marking time-sensitive traffic as it enters the network to facilitate prioritization during transport
- *Traffic Management* – Mechanisms that allow time-sensitive traffic to avoid delays due to network congestion.

AT&T's approach for providing QoS is presented in **Figure 1.3.2.e-1** and **Table 1.3.2.e-1**.

Figure 1.3.2.e-1: Approach for Providing



APPROACH TO ENHANCE QUALITY OF TIME-SENSITIVE TRAFFIC

- **Provisioning – Designing the Network with Optimal Capacity to accommodate all Offered Services**



Dedicated team who proactively manages the various types of capacity associated with AT&T Global IP/MPLS network.

Analyze, correlate, and trend network statistics. Provides performance and capacity management reports to [REDACTED]. Compares trended measurements against engineering objectives and notifies [REDACTED] when capacity or performance thresholds are exceeded.

- **Mapping**



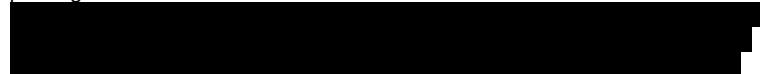
Classifying – Assignment of Packets Based Upon Priority

Process of assigning a packet or traffic flow to the appropriate service class and queue. Mapping is performed at the customer premise router/switch.



- **Traffic Management – Management of Traffic as It Enters and Traverses the Network**
- **Admission Control**

Proactive techniques that control the input of subscriber traffic to the Network. Network access can be explicitly and selectively denied to mitigate potential service degradation when inbound subscriber traffic exceeds the agreed rate. This prevents network from being overwhelmed by lower priority traffic that could impact the service quality of time-sensitive traffic. The most common admission control technique is policing.



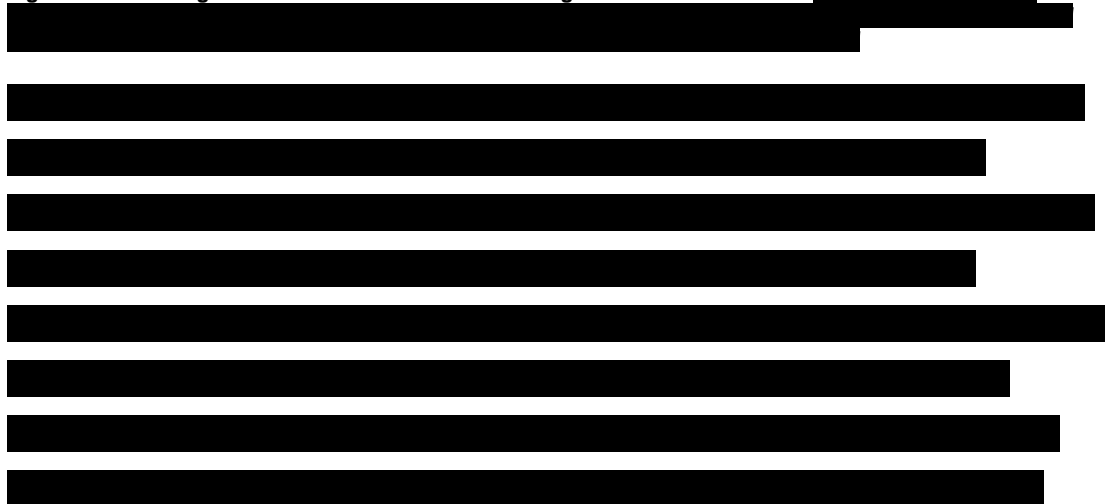
- **Queuing and Scheduling** Queuing and scheduling occurs within the switch or router equipment. Time-sensitive traffic is assigned priority as it traverses the switch/router equipment and the network. Traffic is also assigned to different queues, based on classification. The scheduler determines which queue a packet enters and when a packet exits a queue.
- **Congestion Control** MPLS network supports [REDACTED]

Table 1.3.2.e-1: Approach to Ensure Quality for Time-Sensitive Traffic. *Through capacity management, service classification and traffic management, time-sensitive traffic is provided the appropriate QoS.*

1.3.2.e.1 Time-sensitive Traffic in AT&T MPLS Network

AT&T's global IP core network infrastructure is based on MPLS technology that provides the framework to support CoS/QoS. **Figure 1.3.2.e-2** shows a high level view of CoS and QoS management across the network.

Figure 1.3.2.e-2: High-level View of CoS and QoS Management across Network. [REDACTED]



██ This provides Agencies with a cost-effective approach managing both bandwidth and performance levels.

Traffic classification for prioritization starts at the Agency's router, which identifies application traffic flows and assigns them to a specific network class. [REDACTED]

(Table 1.3.2.e-2).



Table 1.3.2.e-2: Class of Service Assignments.

(Table 1.3.2.e-3).

[illegible]

Table 1.3.2.e-3: Class of Service Profiles.

Figure 1.3.2.e-3,

Figure 1.3.2.e-3: Differentiated Services

Figure 1.3.2.e-4.

Figure 1.3.2.e-4: MPLS Header Encapsulation

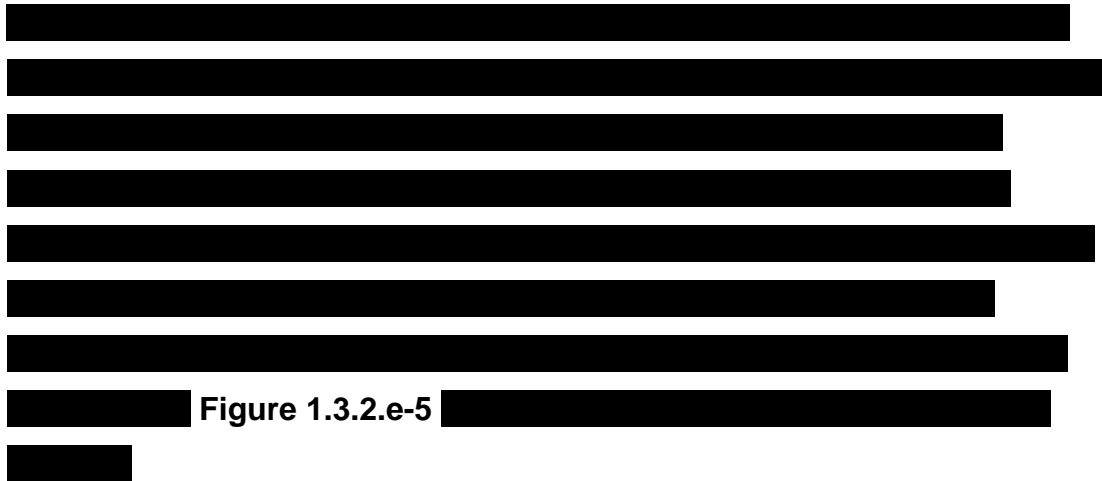




Figure 1.3.2.e-5: **Priority** 

When there is no congestion on the backbone trunks, there is no requirement for traffic management. 







 AT&T is confident that quality and service requirements for Networx's time-sensitive traffic will be satisfied.

