

1.3 Networx Architecture [L.34.1.3]

The General Services Administration (GSA) and the Interagency Management Council (IMC) designed the Federal Technology Service (FTS) Networx Program to provide Agencies with the best telecommunications and information systems services available over the next ten years. Because Networx Universal comprises 37 mandatory and 11 optional services and has a 10-year lifecycle, a contractor's network architecture will strongly influence its ability to provide Agencies with high-quality, full-service solutions for the duration of the contract. Architecture impacts every facet of a contractor's ability to support the Networx services.

The offeror shall describe the means by which its infrastructure will support the delivery of high quality, secure, and reliable Transport/IP/Optical, Management and Applications, Security, and Wireless Services. [L.34.1.3]

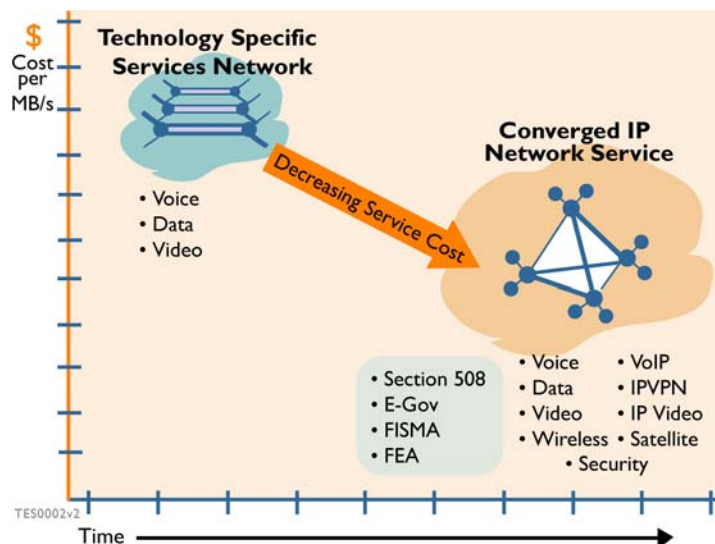


Figure 1.3-1: Converged Backbone Services. Agencies will receive Agency-specific solutions, migrate to emerging technologies, and reduce their total cost of operations by selecting a full-service vendor with a network that accommodates converged solutions and address FEA requirements and e-Gov initiatives.

Internet Protocol (IP) has emerged as the universal enterprise application protocol. The operational savings associated with converging voice traffic to the IP network will eliminate the traditional voice network altogether. Through convergence, Agencies may obtain lifecycle cost

benefits by bundling access services and converging backbone services (Figure 1.3-1). In addition to the lifecycle cost benefits, network convergence

provides the framework for implementing innovative integrated applications that allow Agencies to become increasingly citizen-centric, mission-focused, and responsive to new initiatives such as the Federal Enterprise Architecture (FEA). To harvest the convergence optimization, Agencies require service providers with a network architecture that embraces IP/MPLS converged networking.

As the Agencies' traffic migrates to a converged IP network, security becomes increasingly important. Service providers that follow leading security practices, protect their infrastructure from security threats, and mitigate cyber attacks will provide Agencies with a safe operating environment to perform their mission. A service provider's ability to identify security vulnerabilities and threats before they become a problem will differentiate them in the eyes of the Agencies. Increasingly, Agencies will view the service provider's network as an intelligent security device that provides continuous protection to their mission-critical applications.

Service quality and reliability are critical to the Agencies' success. The service provider's network architecture must be resilient and flexible to handle unexpected traffic loads or transmission and equipment failures. It must be scalable to maintain service performance as the network expands to reach service delivery points. Furthermore, service convergence creates the challenge of maintaining service quality for real-time traffic on an IP/MPLS network all the while service boundaries expand beyond the provider's network through roaming and peering agreements.

Service providers with a unified network infrastructure offer seamless global capabilities that provide Agencies a higher quality, end-to-end service portfolio with broad geographic coverage. For locations that are not on net, Agencies expect the service provider to act as a single-point of contact by

coordinating service arrangements with other service providers to extend in-country non-domestic reach. Agencies expect their provider to continue growing its non-domestic service to match their expanding missions.

When confronted with an actual or potential emergency, Government Agencies rely on the telecommunications infrastructure to mitigate the situation. Supporting the Government during an emergency situation requires prioritization of service providers' resources. In summary, a comprehensive National Security/Emergency Preparedness program is required for a focused response during emergency situations.

AT&T Network Architecture

As presented in **Figure 1.3-2**, AT&T provides Agencies a comprehensive Network Architecture that addresses security, quality and reliability, convergence, global reach, and emergency preparedness.



Figure 1.3-2: AT&T's Global Network Architecture

AT&T's Network Architecture

AT&T's network architecture offers the following benefits and features:

- Enables convergence through layered approach comprising an [REDACTED]
[REDACTED]
- Facilitates transition to IPv6 because it is transparently carried on the [REDACTED] like other multiservice applications.
- Offers dynamic access to services such as Voice over IP and web services through a [REDACTED]
[REDACTED] that is built on top of the MPLS core and the multiservice edge network.
- Enhances security of the Agencies' applications by [REDACTED]
[REDACTED] that continuously monitors both the AT&T network and the global Internet for security threats.
- Provides exceptional service performance and reliability through [REDACTED]
[REDACTED] in the network and automated systems for [REDACTED]
[REDACTED] to manage unpredicted traffic loads and alternate routing around unanticipated network outages.
- Facilitates Agencies' non-domestic expansion by providing virtually seamless service to more than [REDACTED] countries over a common MPLS core network
- Prepares Agencies to address emergency situations through a comprehensive NS/EP program that includes [REDACTED]
[REDACTED]
[REDACTED]
- Supports the Government's FEA vision of transformation by facilitating the use of technologies that contribute to mission performance by focusing on



AT&T takes Top Spot in Yankee Group's ranking of Telecommunications Providers. AT&T ranked number one by earning top scores in Corporate Reputation, Sales and Marketing, Technical Competence and Service and Support

--The Yankee Group

development of net-centric technologies to support solutions based on service oriented architecture (SOA) using standardized, web-adapted components

- Includes new wireless technologies in the architecture such as [REDACTED] and [REDACTED], with several networks already having built in wireless connectivity.
- Prepares for VoIP, data, and wireless seamless handoff with [REDACTED]
[REDACTED]
[REDACTED] architectures
- Incorporates [REDACTED] in investments since [REDACTED] towards infrastructure enhancements and global expansion.

The Networkx Architecture section, as summarized in **Table 1.3-1**, provides a detailed discussion of AT&T's approach to: infrastructure security; service quality and reliability; network architecture, convergence and interoperability; non-domestic services; national policy-based services, and common architecture components.

SECTION	DESCRIPTION
Section 1.3.1 Infrastructure Security	Describes AT&T approach to providing infrastructure security that protects the AT&T network and the Agencies' traffic. • Provides a description of AT&T's secure network infrastructure protection mechanisms: separation; automation; monitoring; control; testing; response; innovation • Describes how cyber attacks on Agencies are prevented through AT&T's network management and incident detection/response techniques • Outlines AT&T approach to upholding security best practices • Presents AT&T's perspective on anticipated future security enhancements • Describes AT&T skills and experience facilitating Certification and Accreditation (C&A) activities.
Section 1.3.2 Service Quality and Reliability	Describes AT&T approach to providing service quality and reliability. • Outlines AT&T's comprehensive access portfolio that meets or exceeds the industry best practices for performance. • Presents AT&T's peering architecture. Describes how IP traffic flows directly to destination hosts or custom connections through more than [REDACTED] of private peering capacity with other tier 1 ISPs. • Discusses how resiliency is incorporated in the AT&T network design by combining modeling and simulation with network monitoring. • Outlines the process to verify Key Performance Indicators (KPIs) through the collection and online reporting of performance data. • Describes the mechanisms that prioritize real-time traffic ahead of non-real time traffic as it traverses the network.

SECTION	DESCRIPTION
Section 1.3.3 Network Architecture, Convergence, Interoperability, and Evolution	Describes AT&T's network architecture, convergence, interoperability, and evolution approach. • Provides a description of the AT&T access systems and methodologies that provide Agencies with reliable access through redundant networking • Outlines the network transport and service layers • Discusses the support of existing interfaces and technologies as the network evolves to help support Agencies in their transition to future or emerging technologies • Presents AT&T's basic principles for introducing new technology into the network • Describes the AT&T applications aware networking (AAN) and services oriented architecture (SOA) • Describes the method used for mapping telephone and telephone systems IP addressing to E.164 addressing that are used in the PSTN • Discusses approach to migrate to IPv6 from IPv4
Section 1.3.4 Non-domestic Service	Describes AT&T's non-domestic service capabilities and network infrastructure. • Presents the arrangements AT&T has with non-domestic carriers to support roaming and off-net services • Details the non-domestic infrastructure security measures implemented by AT&T • Discusses AT&T's arrangements for interoperability of services between domestic and non-domestic locations • Outlines AT&T's planned expansion of its non-domestic facilities.
Section 1.3.5 National Policy- based Requirements	Describes AT&T's approach to satisfy NS/EP functionality and meet Section 508 provisions. • Presents AT&T's comprehensive NS/EP program that includes Government Emergency Telecommunications Services (GETS), Wireless Priority Services (WPS); Telecommunications Service Provisioning, and next-generation emergency telecommunications services • Details network hardening, separation and encryption mechanisms to protect the network signaling infrastructure and the Agencies' traffic • Outlines the redundant equipment configurations and resilient transport facilities that provide continuity of operations in the National Capital. • Presents the AT&T Team's experience with providing assistive technology solutions and training
Section 1.3.6 Common Architecture Components	Describes AT&T's architectural approach for optimizing Transport, IP, and Optical services. • Describes AT&T's network synchronization architecture, methods, and approach • Outlines engineering methods to optimize network access and transport • Details engineering strategies used to improve access performance • Provides AT&T's vision for service interworking over a common infrastructure

Table 1.3-1: Architecture Section Contents. *The overall AT&T network architecture aids Agencies in mission accomplishment today and AT&T's projects and methods to evolve the network will continue to assist them in the future.*

AT&T will deliver on its promise to perform. Our integrity, financial strength, rich portfolio of current and future products, contract management skills, and executive commitment—as well as those of our best-in-class teaming partners—will be at your service.