1.3.3 Approach to Network Architecture, Convergence, Interoperability, and Evolution [L.34.1.3.3]

The network infrastructure is evolving from multiple networks, systems, and processes into a unified service oriented architecture. Agencies benefit from architecture that includes both multiple protocol core routing and multiple service edge (MSE) transports built on top of solid optical transport foundation. This converged network architecture is based on industry-accepted standards and is designed for evolutionary changes such as IPv6 migration and next- generation internet protocol (IP)-based products like Voice over IP.

[redacted]The result of this migration will be a single network architecture built on standards-based layers that will supply Agencies with secure and reliable networking, telecommunications, office automation, and processing for e-Gov initiatives now and in the future.

[redacted]By supporting the legacy, current, and future network services in a single architecture, AT&T will provide Agencies with products that support convergence while maintaining service continuity, quality,

security, and interoperability. [redacted]

These network architectures and concepts along with their advantages are discussed in the sections as outlined in **Table 1.3.3-1** below, which reflects the AT&T approach to network architecture, convergence, interoperability, and evolution.

CONTENTS DESCRIPTION	
Section	***Discussion***
Section 1.3.3.a: Integrated Access	• Describes the approach for providing integrated access to locations that support customer applications with different performance requirements. • Provides a description of the AT&T access systems and methodologies that provide Agencies with reliable access through redundant networking. • Discusses access to multiple services over a reliable network architecture.
Section 1.3.3.b: Overall Network Architecture	• Descriptions of the network transport and service layers • References made to the edge technologies in Section 1.3.3.a • Management systems and security initiatives that are built into the network are also discussed.
Section 1.3.3.c: Technology Evolution	• The methods used to ensure interoperability with future services. • Support of existing interfaces and technologies as the network evolves to help support Agencies in their transition to future or emerging technologies.
Section 1.3.3.d: Introduction of technology	• Outlines the basic principles of engineering used to evolve the network • Discusses how new services based on new technologies remain robust and secure. • Describes the process that mitigates interoperability issues that typically surround the adoption of new technologies.
Section 1.3.3.e: PSTN Interconnect	• Describes the method used for mapping telephone and telephone systems' IP-addressing to E.164 addressing that are used in the PSTN. • Additional Public Switched Telephone Network (PSTN) interoperability, such as the use of gateways. • Discusses how AT&T will migrate to the intercarrier ENUM model once it is ready for commercial use.
Section 1.3.3.f:	• Discusses approach to providing a migration to IPv6 from IPv4. • Described how the network will carry Agencies IPv6 traffic as soon as they are ready to migrate. • Lists tools and topologies that will help Agencies transition from IPv4 to IPv6 without having to completely rethink their networking strategy.

Table 1.3.3-1: Section Contents Description. *This network architecture aids Agencies in mission accomplishment by providing products that support convergence while maintaining service continuity.*

Using the network architecture, systems, and services that are described in the following sections, Agencies will be able to depend on AT&T to assist mission completion as needed in a reliable, efficient, and secure manner.

(LOOK at Titles, first sentence and last sentence – Marketing Sentences; Review the Pictures – Generic Pictures)

1.3.3.a Approach to Providing Integrated Access [L.34.1.3.3.a]

(a) Describe the approach for providing integrated access to locations that support customer applications with different performance requirements (e.g., voice, data, and video). [L.34.1.3.3.a]

AT&T's network evolution strategy is the consolidation of today's multiple data and IP networks to a single, global, MPLS-enabled backbone over an intelligent optical core network. Coupled with the MPLS core is an edge network architecture that combines resilient access networks with multi-protocol/multi-service capabilities. This edge network architecture consists of two major edge components; the Multi-service Access (MSA), and the MSE that provides coupling to the MPLS Core. Listed in **Table 1.3.3.a-1** are the functions of each of the network systems.

COMPONENT	PROVIDES
Multi-Service Edge (MSE)	[redacted]
Multi-Service Access (MSA)	[redacted]
MPLS Core	[redacted]

Table 1.3.3.a-1: Multiple Access Strategies over a Single Resilient Network. *The use of the MSA and MSE offers Agencies the ability to connect multiple applications through single, managed underlying network architecture. This architecture interconnection to other Agencies also facilitates the adoption of new technologies.*

The basic architecture for an MSA/MSE configuration is shown in **Figure 1.3.3.a-1**. [redacted]

Figure 1.3.3.a-1: The MSE/MSA architecture provides resilient access to AT&T networks and services. *Using the available underlying network layers, Agencies are provided resilient access to transport and services using multiple network protocols. This is an important step in the converged network strategy that supports both the new and the old network types in a single system.*

1.3.3.a.1 Multi-Service Access (MSA)

The MSA refers to the network through which customers connect to AT&T's network services.

Key to this implementation is the support for protocol-independent virtual circuits through which the Agency accesses the multiprotocol transport core.

This new network architecture provides Agencies increased service flexibility and service performance. Agencies will be

able to evolve the service network types to match their ever-changing missions without completely re-engineering their network access.

[redacted]

1.3.3.a.2 Access Network Strategies

[redacted]This strategy allows AT&T to offer Agencies access interfaces that are managed at the network protocol level, with the underlying access network supporting redundancy and availability.

Worldwide, where metro fiber networks are not owned, AT&T creates a similar access level by leasing bandwidth from local exchange carriers (LEC) and foreign Postal Telephone and Telegraph (PTT) entities at the lowest possible network layer. [redacted]

[redacted]

[redacted]This allows AT&T to supply the upper layer communications product to the Agency with QoS, network reliability, and network availability supported at the same level as that of AT&T-owned access networks.

1.3.3.a.3 Multi-Service Edge (MSE)

The MSE will terminate customer access into the global packet network and provide all the service specific features for Layer 2 (e.g., FR/ATM) as well as Layer 3 (IP) services, and Time Division Multiplexing (TDM)-based services.

[redacted]

Figure 1.3.3.a-2 depicts how the MSE acts as the termination point, QoS arbitration system, and on-ramp to the MPLS core network. Additional functions within the MSE are the control of access, security functions, and protocol conversion for services like VoIP.

Figure 1.3.3.a-2: The MSE Physical and Virtual Elements. *The equipment handles the QoS and routing for IP, ATM and Frame Relay data within the MSE element. Additional edge functions that are included in a more virtual sense are the VoIP Border Edge and links to traditional 4E and 5E circuit switched voice.*

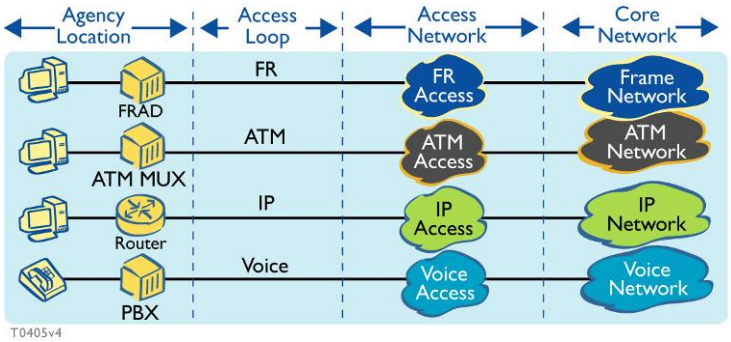
The use of the MSA/MSE combination allows Agencies to operate multiple applications over the same access arrangement. [redacted]

[redacted]

1.3.3.a.4 Network Evolution

The AT&T MSE/MSA access strategy is aligned with the evolution of network solutions currently under way throughout the industry. [redacted]

Figures 1.3.3.a-3 through **1.3.3.a-5** shows the evolution of networks towards using the MSE/MSA technology.



Traditional Networks- They are discrete in nature with access service and connectivity distinctly separated. Overhead bandwidth, which must be provisioned for each service, is managed separately by both the Agency and carrier.

Figure 1.3.3.a-3: Traditional Topology for Separate Service Types. *In this topology, individual access pipes lead to different backbone networks. This evolved from differing network types embedded in the communications products along with the natural industry progression to packet-based multiplexing and bandwidth management.*

Figure 1.3.3.a-4: The MSA/MSE Combination Used to Take Advantage of Access Network Bandwidth Reduction and Resiliency. [redacted]

Figure 1.3.3.a-5: Services are consolidated onto an IP Infrastructure. [redacted]

As shown the left of the figure, the MSA/MSE architecture is designed around delivering new converged services along with supporting legacy and transitional network services. Using the MSA/MSE architecture, Agencies will receive reliable multiprotocol, multiservice connectivity that provides access to the AT&T MPLS core network and SOA, as described in the following sections.

1.3.3.b Overall Network Architecture [L.34.1.3.3.b]

(b) Describe the overall network architecture and explain the benefits of this implementation. [L.34.1.3.3.b]

AT&T has developed a global network for government and commercial customers that is reliable, scalable, flexible, and intelligent. [redacted]

Figure 1.3.3.b-1 shows an exploded view of the converged networks architecture.

Figure 1.3.3.b-1: The AT&T Global network Architecture, is. *Agencies benefit from carrying products over a core network that is fast, reliable, and error free. Based on standards and use of inter-working layers, the network's goal is to provide customers with every type of service possible from a single-access mechanism standpoint.*

Table 1.3.3.b-1 provides a summary of AT&T's key architectural layers along with the scope, scale, and functionality of the physical, optical, and transport layers of the network. [redacted]

PHYSICAL, OPTICAL AND SONET LAYERS	
Layer	*Features and Functions*
Physical Layer	[redacted]
Optical Switching	[redacted]
Metro Optical Switching	[redacted]
SONET	[redacted]

Table 1.3.3.b-1: The lower layers provide the footprint and the resiliency to the remaining network layers. *Agencies with access to a variety of services from a single converged network architecture benefit by building on the physical layer with a standard set of optical and SONET systems.*

1.3.3.b.1 Network Reach and Capacity

[redacted] In addition to the owned physical plant, AT&T leases or partners with LECs, PTTs and other carriers to further expand its reach where needed. No other company has the worldwide coverage that AT&T offers. This means Agencies can connect more services in more places using AT&T.

The capacity of the network is governed by the makeup and reach of the physical topology. [redacted] The importance of this capacity is to provide enough transmission capability for the world's growing need for bandwidth, being able to provide in-network spare capacity for reroute on failure, and to provide packet-based protocols with a congestion-free operating environment.

1.3.3.b.2 Reliability

To make the best use of the redundant fiber paths that are built into the physical layer, AT&T has invested in systems that take advantage of automated redundancy at the lowest possible layer and then repeat the use of redundant networking throughout the layers, including the service layers. [redacted]

1.3.3.b.2.1 Optical

The AT&T fiber plant primarily consists of two distinct areas of operation. One is the long haul fiber, which serves to provide long distance transport both domestically and over seas. The other is the metro fiber, which supports campus network and intracity routes and ties POPs and interconnects together. [redacted]

[redacted]

Even with the multiple quantities per path, AT&T uses wave division multiplexing (WDM) to increase the capacity and resiliency of the fiber network. As shown in **Figure 1.3.3.b-2**, the WDM systems provide multiple optical interfaces available from a single fiber strand. In the AT&T WDM system several lambda are available for utilization by transmission equipment out of each equipment-facing WDM interface multiplex. This allows AT&T to interface multiple types of transmission equipment to a common WDM infrastructure which simplifies the operation of the Optical Electrical Optical (OEO) redundancy system that switches between redundant fiber routes.

Figure 1.3.3.b.-2: WDM Provides More Bandwidth. *Agencies benefit from a reduction in overall costs of bandwidth. Utilizing wave division multiplexing minimizes the amount of buried fiber needed to transport data and also reduces the number of costly long haul lasers.* [redacted]

[redacted]

(**Figure 1.3.3.b-3**) [redacted]

[redacted]

Figure 1.3.3.b-3 The Optical-Electrical Optical Switch [redacted]

[redacted]

1.3.3.b.2.2 SONET

[redacted] **Figure 1.3.3.b-4**. [redacted]

Figure 1.3.3.b-4. [redacted] Protection for Data Circuits. [redacted]

[redacted] **Figure 1.3.3.b-5** [redacted]

Figure 1.3.3.b-5 [redacted]

1.3.3.b.3 Circuit Switched Voice

The circuit switched voice network is the legacy voice network owned and operated by AT&T. **Table 1.3.3.b-2** outlines some of the features, capacities, and capabilities of the circuit switched voice network.

CIRCUIT SWITCHED	
Circuit Switched Network	[redacted]
Carrier Interconnect	[redacted]
Special Call Routing	[redacted]

Table 1.3.3.b-2: Circuit-Switched Voice Network. *The circuit-switched voice network includes both long-distance and local service switching and is fully integrated with the PSTN world wide.*

1.3.3.b.3.1 Network Disaster Recovery (NDR) Teams

One key element in the overall reliability of the network is the AT&T's Network Disaster Recovery (NDR) service. Starting in 1992 for voice systems disaster recovery, the NDR has grown into the industry-leading network disaster recovery service with more than [redacted] and a team of approximately [redacted] specialized in the physical recovery of the AT&T's infrastructure. Support for the NDR service is built into the network and has grown from a voice switch service into a NDR system. [redacted]

1.3.3.b.4 Upper Network Layers

Driven by IP-centric applications demand, IP-based services represent the fastest growing sectors of the AT&T network. Starting in 1999, AT&T began migrating its multiple networks to a single MPLS backbone/core network with multiprotocol, multiservice capabilities at the edge. AT&T is in the process of continuing

integrating Frame Relay, ATM, and Ethernet networks into the MPLS backbone. In addition to the combination of network services, new IP-based services such as VoIP are being built into the upper layers of the network. **Table 1.3.3.b-3** lists the major features and capabilities of the upper network layers.

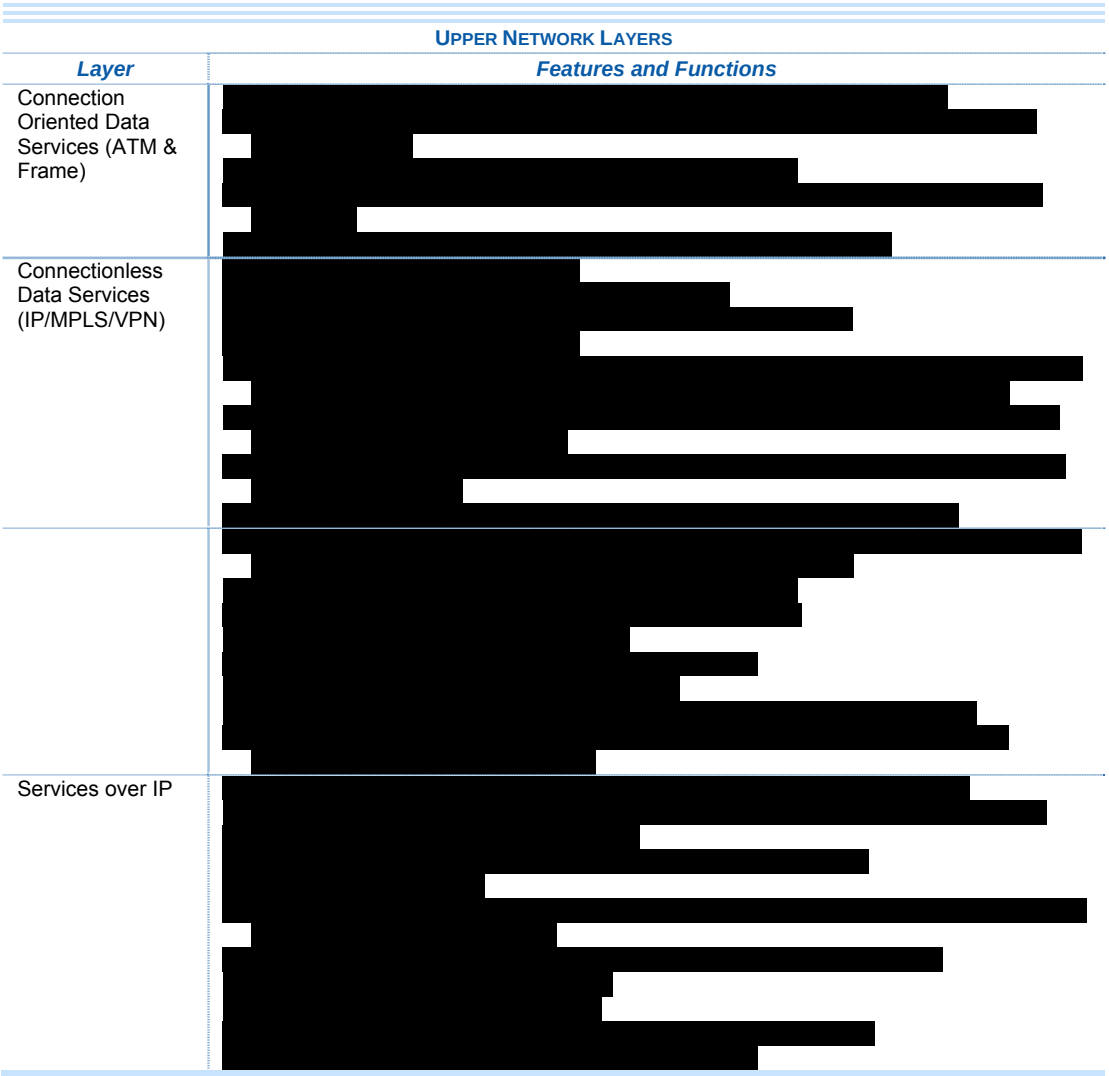


Table 1.3.3.b-3: Upper Layers Architecture for Performance and Service. *Agencies can depend on these upper layers to support and provide the communications, computing, and collaboration systems that are emerging in the industry. With services migrating to be served over IP, AT&T's upper layers are poised to offer services over IP with security and efficiency in a modular format that allows the grouping of modules to create new service systems.*

These upper layers are designed to support and provide emerging industry communications, computing, and collaboration systems in the industry

without eliminating the services on which Agencies have depended. This network is designed to provide transition from existing services to future needs and applications through the addition of application-aware elements over the high-performance MPLS core.

1.3.3.b.4.1 MPLS

The core of all AT&T network based services is migrating towards a MPLS) network that uses Label Distribution Protocol (LDP) to establish switching paths. The MPLS network allows for the transport of both connection-oriented and connectionless packet data freely across the same infrastructure regardless of the underlying protocol. [redacted] The MPLS network spans the worldwide AT&T footprint and provides the typical CONUS core routing performance characteristics as shown in **Table 1.3.3.b-4**.

METRIC	AT&T TARGET	TYPICAL OBSERVED MPLS CORE AVERAGES*		
		Month 1	*Month 2*	*Month 3*
CONUS Round Trip **Latency**	[redacted]	[redacted]	[redacted]	[redacted]
End-to-End **Packet Loss**	[redacted]	[redacted]	[redacted]	[redacted]
Network **Availability**	[redacted]	[redacted]	[redacted]	[redacted]
Packet **Jitter**	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]				

Table 1.3.3.b-4: MPLS Routing in the Packet Network core. *Once in the core, packet data is routed with a high level of performance and integrity. Agencies are able to move forward and focus on their mission instead of communication issues.*

In addition to the forwarding performance, MPLS offers RFC-2547bis Virtual Private Networks (VPN) without creating end-to-end tunnels or permanent virtual circuits. These virtual networks, that provide any-to- any connectivity within the network, can be offered directly to customers or be used to create

virtual service networks such as the one used for AT&T's Voice over IP (VoIP) products. The core MPLS network also features reliable high performance on-ramp through the access edge. Reliability between the access edge and core networks is provided using the access architecture shown in **Figure 1.3.3.b-6**.

Figure 1.3.3.b-6: Redundant Links Provide Reliability. *By utilizing the redundancy (dual links) built into the routing capabilities of the network, Agencies receive services that are reliable. As depicted In the model, a single failure does not affect the service since the entire route path shown can be followed to pass data.*

1.3.3.b.4.2 Services over IP

In the uppermost layers of the architecture are found the services over IP. The architecture is designed to support users of the services that generally require only a personal computer (PC) or an IP phone and a connection to the network. Service creation, the combining of different service components to create a new single service, is handled by the service creation layer in the network. **Table 1.3.3.b-5** describes the service offerings architected into the network.

ELEMENT	SERVICE OR FUNCTION
	VoIP
Call Routing	Call routing and PSTN access are built into the network [redacted]
IP Centrex	PBX-like services are built into the VoIP network [redacted]
Messaging	A choice of messaging [redacted]
Ad Hoc Collaboration (data, voice, video)	Systems that support collaboration services [redacted]

ELEMENT	SERVICE OR FUNCTION
	Network Hosting
Network Servers	Managed and unmanaged server space to house and process database, back office applications, and other business processes.
Content delivery	Web, streaming media, caching, and other content served to internet and intranet users.
Intelligent DNS	A domain name service (DNS) service that tracks network and systems performance then routes users to the most available content resource
Storage	Network-accessible storage media via IP or storage area network (SAN) to augment Agency storage needs. Storage can be selected as an addition to other SoIP products.
Utility Computing	Network- based computing for nearly any task or business process. Can be used to process common database elements and other functions that are shared among business entities.
Computing on demand	Computing and content delivery systems geared to handle seasonal and one time events.
Backup Services	Storage media, backup routines, vaulting, and data restoration services for both routine and critical data.

Table 1.3.3.b-5: Modular Service Nodes Adapt to Changing Agency Needs. *Using service modules that are architected into the network as individual elements and the surrounding network systems functions, along with open standards protocol access, special functions supporting Agencies ever-changing missions can be constructed on the fly.*

In general, SoIP service modules follow distributed and modular construction and are accessible using open protocol standards. This construction and standard access allows for combining of elements to create new products.

[redacted]

1.3.3.b.4.5 Interconnects With Extranets

The various distinct layers of the network, all operating as a single unit, provide a system that interconnects well with other carriers networks when needed. [redacted]

[redacted] The variety of network interconnects is shown in **Table 1.3.3.b-6**.

NETWORK	INTERCONNECT
IP Peering	Uses BGP and SONET at the POPs to interconnect to private peering points world wide
SS7	AT&T operates an extensive SS7 network that is an integral part of the world's call switching fabric. This network is also has gateways to VoIP.
PSTN interconnect	POP locations at every major carrier interconnect point in the U.S. as well as several international interconnects
Carrier Transport	Access and transport interfaces at sub-rate levels through OC-48 to every major carrier.
ATM/Frame to IP/MPLS	[redacted]
Cell Networks	AT&T carries data and voice for and is interconnected directly to the major cell networks
Cable/DSL	AT&T has interconnect and partnership agreements with cable and DSL broadband providers.
Satellite Networks	Linkage to major satellite carrier networks as well as several owned and operated earth stations.
Wireless Networking	[redacted]

Table 1.3.3.b-6: Inter-Working Networks. *By utilizing the layered architecture with a multiple service edge, Agencies are seamlessly interconnected to many types of networks that support a variety of services and missions. These networks include legacy networks, the Internet, and networks that are created by new technology (e.g., wireless access).*

Using an architecture that interconnects easily and natively supports multiple protocols and topologies, AT&T provides Agencies with all types of connectivity and service with its own and partner facilities as well as those of interconnected networks and systems.

1.3.3.b.5 Management and Security Architecture

Even the very best service delivery network architecture cannot function without solid systems management and provisioning. In addition, the vast interconnectivity and large customer base could pose some inherent security risks. To make network technology as usable as possible, AT&T has a standing design philosophy and architecture placing both management systems and security in the overall network architecture. [redacted]

[redacted] **Figure 1.3.3.b-7** shows the basic model of systems and service management along with the basic security elements.

Figure 1.3.3.b-7: Built-in Management and Security.. *Both security and management are process oriented, with network layers requiring different processes. The layers of the management and security systems abstract the differences, allowing for a more seamless and secure operation. This network architecture layers the management and security systems on top of the management network.*

Using the management systems architecture, AT&T combines the functions of provisioning, network monitoring, and service management using the three basic functions found in the element management systems (EMS), various network operations center (NOC), and unique product operations center (PNOC) systems. By using these distinct areas of operations AT&T initiates and combines services into new products quickly without upsetting the security that is designed into both the service and the management networks. Table 1.3.3.b-7 lists the basic architectural elements and functions of the management and security systems. (Note that the management systems architecture is both physical and logical.) The security architecture shown and discussed here is the logical extension of the overall security architecture.

FUNCTION	FUNCTIONAL ELEMENTS
Operations/ Management	• The management systems are architected in a modular fashion to match the modular construction of the service network. • All network systems and elements are managed from a dedicated secure management

FUNCTION	FUNCTIONAL ELEMENTS
	network. • EMS help abstract management data into a commonly collected set of parameters • EMS provide provisioning language interface to differing systems • Service provisioning uses several EMS elements to create a service form multiple network modules. • Network Operations receive operational data through EMS elements and correlate the data for a big picture view of the network. • Product operations provide a service level view that is a collection of data form many EMS and NOC elements. • Data collection and history storage allows customers to view product-based data and helps self-management of the services. • The service-creation layer uses the service provisioning from product operations along with the web portal to allow for ad hoc provisioning of new services created from modular service elements.
Security	• Separation – Networks are separated into trusted and untrusted domains. • Automation – Security processes are fully automated and can process data at full network loads • Monitoring – Each layer and element is monitored for both normal and under attack scenarios, allowing for security management overall as well as system by system. • Control – Access to systems and networks is controlled • Design and testing – Lab testing of risks and mitigations leads to secure network design • Response – Response teams act immediately when monitoring reports an event • Innovation and architecture – AT&T's approach to innovation in its architecture and design aims is to keep the network ahead of both intentional and accidental security threats.

Table 1.3.3.b-7: Management and Security Systems Work Together. *Agencies receive secure, reliable, and innovative products by utilizing the layered management architecture along with security systems that are designed and built into the network.*

By designing management and security into the network architecture, AT&T avoids outages and service function failures in both new and existing services. In addition, the modular deployment of management and security systems are designed to easily scale with the service elements and systems that create the services.

1.3.3.b.5.1 Operations Administration Management and Provisioning (OAM&P)

The layers management architecture allows AT&T to offer a holistic management, operations, administration, provisioning, and monitoring approach to customer applications and required customer networking. Datacenter resources to support these applications are accessed through a system that provides a single point of control through system integration.

The existing operations, administration, management and provisioning (OAM&P) systems, applications, and processes support very large-scale

infrastructure, network, and managed services. [redacted]

However, in order to support the unprecedented scope of Government IT and telecommunications requirements in Networx, AT&T is making a major investment in additional capabilities and functionalities for OAM&P systems.

1.3.3.b.5.2 Security Built Into the Network

AT&T network is evolving into a comprehensive security network that integrates the end-to-end physical, systems, and information security protection for each service, network and OAM&P element or component. This security network incorporates customer premise, network premise, data center, network access, and network-based security. Based on sophisticated security structures, processes, and unique security expertise, AT&T network security approach is proactive, detects attacks very early, and offers comprehensive security protection. See Section 1.3.1 for a complete discussion on security and security systems.

1.3.3.b.6 Standards-based Networking

The overall AT&T architecture is based on common standards from standards organizations such as IEEE, International Internet Engineering Task Force (IETF) and ITU-T. Adherence to standards allows for better interoperation with customers and extranets, network layers, and service nodes. In addition to interoperability, standards adherence allows AT&T to take advantage of the sum total of the telecommunications industry experience.

AT&T also plays an active role in the standards bodies, lending its many years of experience in networking and providing reliable high-capacity services to the process of standards development.

1.3.3.b.7 Technological Evolution

The overall AT&T core and edge network architecture is built to support evolutions in technology and service in two basic ways. [redacted] With this architecture, new customer-facing features and functionality can be added more quickly at the edge using the service agnostic core. This strategy is described in more detail in Section 1.3.3.d of this document.

1.3.3.c Network Evolution, Convergence, and Interoperability [L.34.1.3.3.c]

(c) Describe how the network architecture supports technological evolution, convergence, and ensures interoperability with present and future commercial networks. [L.34.1.3.3.c]

AT&T currently uses two basic methods to support technological evolution in two basic ways. [redacted]

THE CURRENT NETWORK ARCHITECTURE SUPPORTS THE ADDITION OF NEW

[redacted]

Using these two methods allows Agencies with investments in technologies to continue to utilize that investment while taking advantage of newer technology.

[redacted]

Table 1.3.3.c-1 outlines the basic elements and some of the current areas of effort in the AT&T network evolution.

NETWORK LAYER ARCHITECTURAL EVOLUTION	
Optical Network	
Technological Evolution	[redacted]
IP MPLS Core	
Technological Evolution	[redacted]

NETWORK LAYER ARCHITECTURAL EVOLUTION	
Convergence	[redacted]

Table 1.3.3.c-1: Network Evolution to Support Convergence. *Projects are constantly evolving to improve transport efficiency and provide access to converged services.*

In addition to the effort to improve the network core, AT&T is also adding layers of functionality to the network using SOA and AAN. [redacted] **Table 1.3.3.c-2** outlines the basic elements of the service layers architecture, including convergence and interoperability points.

SERVICE LAYER ARCHITECTURAL EVOLUTION	
Services Over IP	
Technological Evolution	[redacted]
Convergence	[redacted]
Interoperability	[redacted]
Application Infrastructure	
Technological Evolution	[redacted]
Convergence	[redacted]
Interoperability	[redacted]
Network Applications	
Technological Evolution	[redacted]
Convergence	[redacted]
Interoperability	[redacted]

SERVICE LAYER ARCHITECTURAL EVOLUTION	
Customer Applications infrastructure	
Technological Evolution	[redacted]
Convergence	[redacted]
Interoperability	[redacted]

Table 1.3.3.c-2: Services over IP and Applications Networking. [redacted]

1.3.3.c.1 Evolution of the Core

In an example of core network evolution, shown in **Figure 1.3.3.c-1**, the changes to the overall network architecture (refer to Section 1.3.3.b) include [redacted]

Figure 1.3.3.c-1: Next Generation Networks.

Figure 1.3.3.c-2

Figure 1.3.3.c-2: Continued Evolution from the Inside Out. [redacted]

1.3.3.c.2 Evolution of Interoperability at The Edge

[redacted]

[redacted]

Figure 1.3.3.c-3

[redacted]

Figure 1.3.3.c-3: MSE Configuration with IP Transport Services.

[redacted]

[redacted]

Figure 1.3.3.c-4 [redacted]

[redacted]

Figure 1.3.3.c-4: [redacted]
Telephone Systems

[redacted]

[redacted]

1.3.3.c.3 Access Mobility

In order to converge the networks and interoperate with both emerging and existing network topologies, the AT&T network architecture includes [redacted] (**Figure 1.3.3.c-5**). [redacted]

Figure 1.3.3.c-5: Addition and Convergence [redacted]

1.3.3.d Approach to Incorporate Emerging Technology [L.34.1.3.3.d]

(d) Describe the approach for incorporating into the offeror's network, infrastructure enhancements and emerging services that the offeror believes are likely to become commercially available in the timeframe covered by this acquisition, including a discussion of potential problems and solutions. [L.34.1.3.3.d]

[redacted]

To support this transformation, the AT&T network will require key infrastructure enhancements, and new services and capabilities during the Networx acquisition timeframe. This network transformation must be completed without service-impacting risks and without jeopardizing network reliability and functionality.

1.3.3.d.1 Approach for Enhancing the Network Infrastructure

[redacted]

When emerging technologies mature and become the new core, older technology interfaces are migrated to the edge for continued product support.

[redacted]

[redacted]

[redacted]**Figure 1.3.3.d-1** shows the flow of emerging technologies.

[redacted]

Figure 1.3.3.d-1: [redacted]

[redacted] Table 1.3.3.d-1

[redacted]

APPROACH FOR ENHANCING THE NETWORK INFRASTRUCTURE	
Approach	*Description*
[redacted]	[redacted]

Table 1.3.3.d-1: Key Network Enhancements and Emerging Services. [redacted]

1.3.3.d.2 Approach for Enhancing the Operational Support Systems

The operational support systems (OSS) infrastructure must be modified to accommodate emerging capabilities too. As with the network infrastructure, the introduction of emerging technology should not impact the capabilities of the existing network operations systems. The Network Operations team must continue to operate, administer, monitor, manage, and provision the network during the deployment of emerging technology or services. [redacted]

Changes to the OSS are limited to the EMS and provisioning system.

[redacted]

[redacted] **Figure 1.3.3.d-2** [redacted]

Figure 1.3.3.d-2: Approach for Operations System Enhancements. [redacted]

Table 1.3.3.d-2 summarizes AT&T's approach for incorporating enhancements to the OSS that are required to introduce emerging technology to the network.

APPROACH FOR OPERATIONS SYSTEMS ENHANCEMENTS	
Approach	***Description***
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

Table 1.3.3.d-2: OSS Enhancements for Emerging Technology. [redacted]

1.3.3.d.3 Approach for Enhancing the Security System

Emerging technology insertion creates a security threat to the network.

Introducing emerging technology into the network creates the potential for security threats. These potential security threats must be identified, quantified, and mitigated prior to technology introduction. Otherwise, the service provider puts at risk the service quality and performance of the new technology and, potentially, the rest of the network.

To prevent an emerging technology or service from impacting the security of the existing network infrastructure, AT&T follows a rigorous process prior to network introductions. **Table 1.3.3.d-3** summarizes AT&T approach for securing emerging technology.

APPROACH FOR NETWORK SECURITY ENHANCEMENTS	
Approach	*Description*
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

Table 1.3.3.d-3: Approach for Network Security Enhancements. [redacted]

1.3.3.d.3.2 Two-Stage Security Introduction Process

Emerging technology requires the development of new security capabilities that are introduced in conjunction with the emerging technology. The new security technology is not integrated into the existing security platform. As the emerging technology is integrated into the core network, the associated

security package is integrated into the network security infrastructure as described in **Figure 1.3.3.d-3**.

Figure 1.3.3.d-3: Approach for Security System Enhancements. [redacted]

1.3.3.d.4 Infrastructure Enhancements and Emerging Technologies

Many new technologies and services have emerged during the FTS 2001 contract timeframe such as VoIP and WiFi. AT&T anticipates many technologies will also emerge during the Networx contract timeframe. AT&T recognizes the importance of embracing emerging technologies to remain competitive from a service and cost perspective. **Table 1.3.3.d-4** summarizes the infrastructure enhancements and emerging technologies anticipated to impact AT&T's network during the Networx contract timeframe.

Emerging technologies anticipated during the Networx Contract time frame.

INFRASTRUCTURE ENHANCEMENTS AND EMERGING TECHNOLOGIES	
Emerging Technologies	***Description***
[redacted]	[redacted]

INFRASTRUCTURE ENHANCEMENTS AND EMERGING TECHNOLOGIES	
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

Table 1.3.3.d-4: Key Network Enhancements and Emerging Services. [redacted]

1.3.3.d.5 Problems and Solutions with Emerging Technologies

Emerging technology and services must be introduced into the network carefully to mitigate potential problems.

Emerging technologies must be introduced carefully to mitigate risk.

Stability, reliability, and security of the emerging technology and of the existing network must be evaluated prior to introduction, and potential issues must be identified and resolved. The benefits of emerging technology can only be realized when it operates safely and securely as planned. To facilitate this result, AT&T has identified the following general problems and solutions, as summarized **Table 1.3.3.d-5**.

EMERGING TECHNOLOGIES PROBLEMS AND SOLUTIONS	
Issue	***Description and Solution***
Emerging technology is not always reliable and stable	[redacted]

EMERGING TECHNOLOGIES PROBLEMS AND SOLUTIONS	
Emerging technology is a security risk to the Network	[redacted]
Emerging technology must be operational	[redacted]

Table 1.3.3.d-5: Problems and Solutions with Introducing Emerging Technologies. [redacted]

1.3.3.d.5.1 AT&T One Process Phase Gate Approach

To minimize the risks and maximize the value of emerging technology, AT&T follows a rigorous technology/service introduction process [redacted] (**Figure 1.3.3.d-4** and **Table 1.3.3.d-6**).

Figure 1.3.3.d-4: AT&T One Process [redacted]

The culmination of the Approach is the introduction of emerging technology to the network. The introduction is closely monitored to minimize risk to the other services.

[redacted]

Phase	Description
Concept Phase	[redacted]
Feasibility Phase	[redacted]
Design Phase	[redacted]
Development Phase	[redacted]
Service Testing Phase	[redacted]
Introduction Phase	[redacted]

Table 1.3.3.d-6: [redacted] Approach. *This comprehensive and phased approach for securing emerging technology reduces associated risks.*

In summary, the risks associated with emerging technology are reduced by AT&T's strategic approach. [redacted]

1.3.3.e Approach to Support Interoperability of IP and Public Switched Networks [L.34.1.3.3.e]

(e) Describe the approach to support and ensure interoperability between Internet Protocol (IP) networks and the Public Switched Telephone Network (PSTN), including the approach to map between IP and PSTN addresses. [L.34.1.3.3.e]

Using the AT&T VoIP products, Agencies can make and receive calls as they always have. The VoIP to PSTN interconnect facilities seamlessly map traditional Agency telephone numbers to the IP addresses of VoIP telephones and IP-enabled PBX systems. **Table 1.3.3.e-1** presents the basic elements used to completely interoperate with the PSTN and map IP addresses to E.164 numbers.

DEVICES	FUNCTION	BENEFIT
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Table 1.3.3.e-1: Basic Network Elements for Mapping IP addresses to E.164 numbers. *Multiple network elements work together to complete the translation between IP address and E1.64 number.*

The E.164 to VoIP address mapping and call-routing strategy is described in **Figure 1.3.3.e-1**. [redacted]

Figure 1.3.3.e-1: AT&T's VoIP to PSTN interconnect. [redacted]

1.3.3.e.1 Registration and Device Location

[redacted]

The assignment of e.164 numbering

is still governed by the North American numbering plan administration (NANPA) or local number portability (LNP) translation.

1.3.3.e.2 PSTN Call Routing and Handoff

A call coming from the PSTN to a VoIP phone starts out in the PSTN End Office (SSP). The call's signaling is routed through the PSTN using SS7 and the Signal Transfer Points (STP). [redacted]

1.3.3.e.3 Call Routing in VoIP

[redacted]

1.3.3.e.4 Setting up the Call's Talk Path

[redacted]

1.3.3.e.6 Number Assignments and Allocation

AT&T is a local switching entity, or CLEC, [redacted] Using that carrier interconnect status as well as its long standing status as an Interexchange Carrier (IXC) numbers that are terminated within the AT&T VoIP network come from multiple sources.

- Numbers Assigned to AT&T as a CLEC by the North American Numbering Plan Administration (NANPA)
- Numbers Ported to AT&T using Local Number Portability (LNP)
- Numbers Assigned to other LECs and CLECs that follow the Terminating Switched Access Arrangement (TSAA) reroute rules for PBX connections

Using a combination of these typical number sources, AT&T is able to route Agency numbers through the VoIP network as part of the PSTN. This means that in using AT&T VoIP no concessions need be made, such as the loss of 911 services.

1.3.3.e.7 ENUM and its Evolution

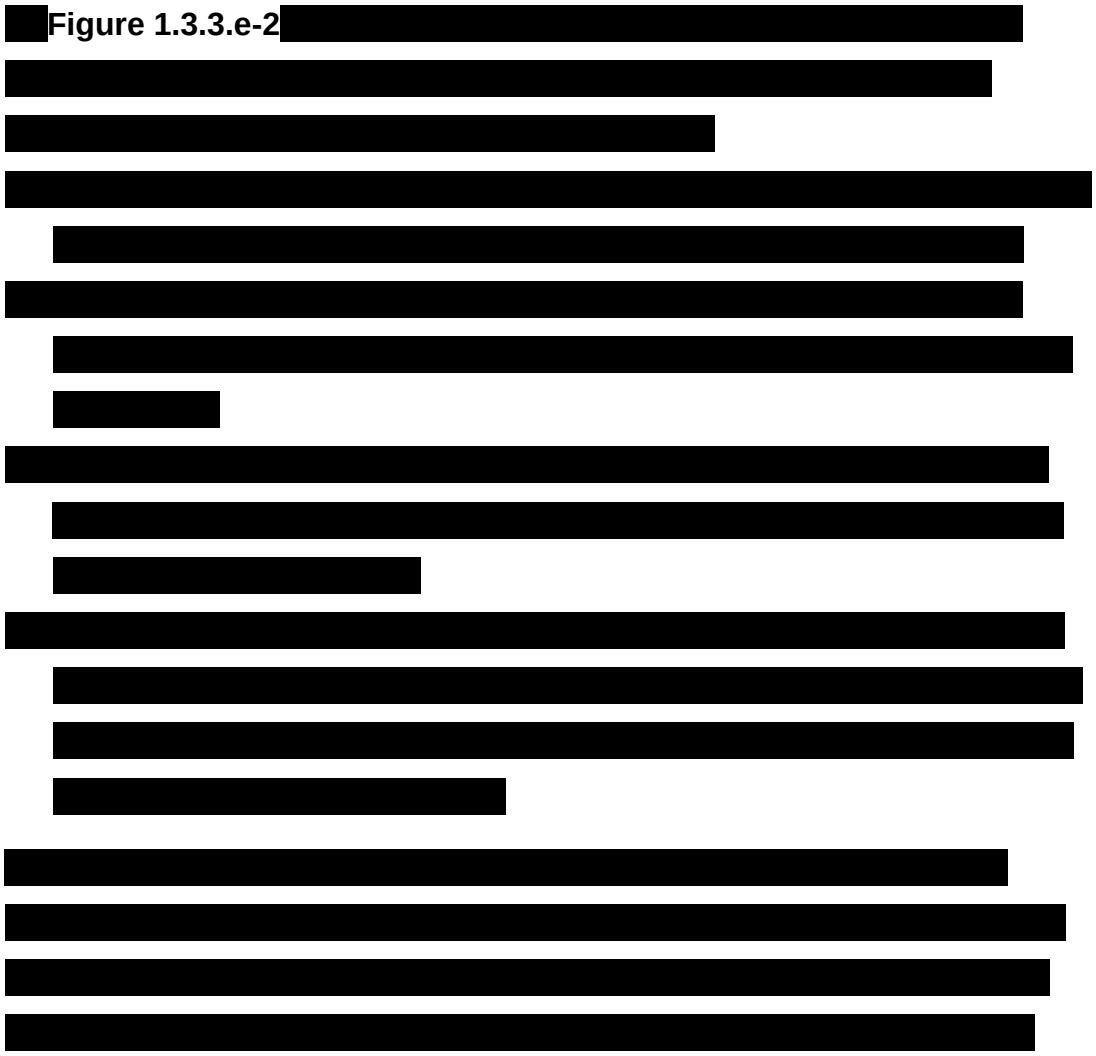
[redacted] **Figure 1.3.3.e-2**, [redacted]

[redacted]

Figure 1.3.3.e-2: [redacted] interconnect carriers at the IP to IP level

[redacted]

[redacted]**Figure 1.3.3.e-2**[redacted]



1.3.3.f IPv4-to-IPv6 Migration Support [L.34.1.3.3.f]

(f) Describe the approach for IPv4-to-IPv6 migration. [L.34.1.3.3.f]

In July 2005, Karen Evans, the Office of Management and Budget's administrator for e-Government and information technology set a June 2008 deadline for civilian Agencies to add IPv6 technology to their network backbones. The civilian Agencies are right behind the Department of Defense, which has started the migration to IPv6 due to the June 2003 announcement to transition all inter- and intra-networking by FY 2008.

Clearly, the Federal Government will lead the migration to IPv6 in the United States.

The AT&T strategy to support and assist Agencies in their move to IPv6 networks and applications includes the use of test networks, the newest IPv6 routing platforms, and the AT&T MPLS IP-version agnostic routing core.

It has long been recognized that a larger number of unique IP addresses is needed to support the vast number of devices and services that use the Internet and its private network variations. Since emerging countries such as China have started using large blocks of IPv4 addresses, the supply of free unique IPv4 addresses is diminishing rapidly. The diminishing number of IPv4 addresses has prompted a worldwide use of NAT tools, which require special firewall-like devices to be employed and break the functionality of several peer-to-peer applications. In addition, IPv4 global routing has become disjointed and inefficient.

Deployment of IPv6 will increase the number of available addresses from IPv4's $4x10^9$ to IPv6's $3.4x10^{38}$. This very large number of addresses will supply every potential network device with a unique dedicated address. In addition, the IPv6 address space is broken into segments that provide for better inter-network routing and larger blocks of locally administered addresses. IPv6 header space and functionality is expanded over IPv4 as well.

To support customers who want to transition to IPv6, AT&T has undertaken a set of tasks to ready the network for IPv6 support. **Figure 1.3.3.f-1** shows the AT&T migration to IPv6 in a logical set of steps from planning and testing through building and use. [redacted]

Figure 1.3.3.f-1: AT&T Lead in Transition to IPv6. [redacted]

1.3.3.f.1 AT&T's IPv6 Strategy

[redacted]

Figure 1.3.3.f-2 [redacted]

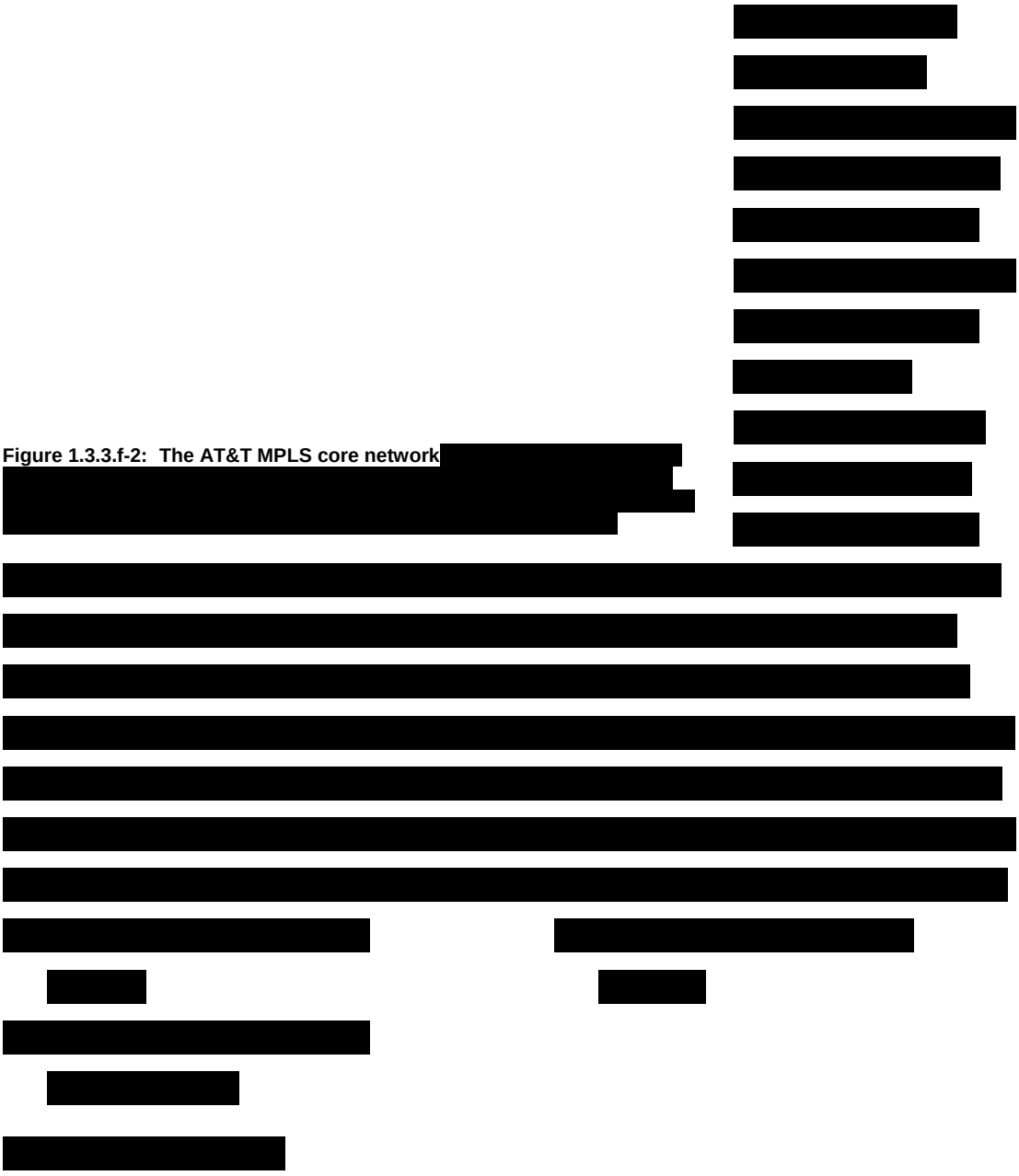


Figure 1.3.3.f-2: The AT&T MPLS core network

1.3.3.f.1.1 Dedicated IPv6 Network Support

Direct, dedicated IPv6 access is provided to Agencies by supplying a connection to the IPv6 core via an IPv6 customer edge router. In this topology, IPv6 packets are routed in their native format through the Agency access

network to the Agency local network. This access methodology will serve those users ready to become wholly dedicated to IPv6 on an Agency-wide basis.

1.3.3.f.1.2 Remote IPv6 Network Access

This topology is one that provides IPv6 packet routing that is tunneled through traditional IPv4 routing. This mechanism wraps each IPv6 packet in a complete IPv4 header and forwards it through the IPv4 network as normal. This IPv6 support methodology is similar to the Internet dial access that started in the early 1990s and continues today. Remote IPv6 tunneled access allows Agencies to operate an IPv6 local network that is connected to the IPv6 core through an IPv4 access strategy. The comparison of the dial access to the remote IPv6 tunneled access is shown in **Figure 1.3.3.f-3**.

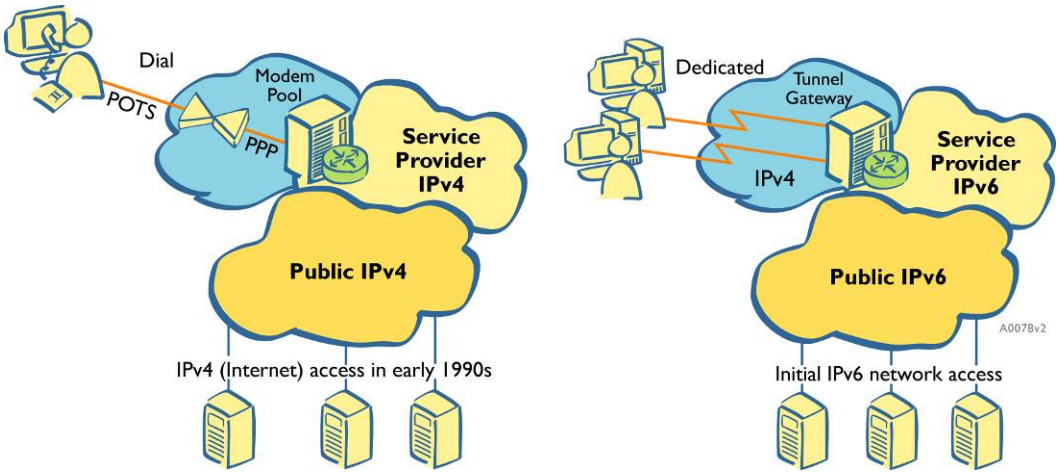


Figure 1.3.3.f-3: Initial IPv6 tunnel access is analogous to the dialup IPv4 access of the early 1990s. *The Point to Point Protocol (PPP) access to IPv4 networks in the beginning of the public access to Internet has a direct analogy to the use of IPv4 tunnels to access an IPv6 network. Both strategies employ a large existing network base.*

1.3.3.f.1.3 IPv6 VPN Options

[redacted]

[redacted]

1.3.3.f.1.4 IPv6 Translation Mechanisms

[redacted]

[redacted]

1.3.3.f.2 Beyond the Deployment

The IETF, Internet, and network providers envision IPv6 being an enabling technology. Along with the additional address space, the following offers are expected to become available once IPv6 is more widely deployed:

- Native security
- Mobility
- Anycast
- Peer-to-peer
- Applications Aware Networks

AT&T is dedicated to evolving its network to support its customers in the migration from IPv4 to IPv6. Through planning, testing, building, and support, Agencies will receive service from a network that is IPv6-ready when the time to migrate arrives.