



NETWORK TO NETWORK INTERFACE PLAN

AT&T will provide interconnect points at both the Network Security Operations Center (NSOC) and the Sam Houston Building (SHB), the prescribed DIR locations via AT&T's VPN (AVPN) service. The standards-based solution uses capabilities specific to RFC-4364 (option A) as the method of connecting AT&T's commercially available MPLS network with DIR. In AT&T's proposed solution, MPLS PE routers from different networks will interconnect individual VPNs using logical channels via a single physical interface. AT&T uses this method today with great success to interconnect AVPN VPNs with other customer VPNs.

Proposed Interconnection Capacity

AT&T can provide a wide range of bandwidth/speeds and interfaces services dependent upon the State's traffic requirement(s). Services can range from a 10Mbps service to a 10Gbps LAN PHY (physical) service.

AT&T Virtual Private Network (AVPN) allows the State of Texas to mix and match port type protocols to access the VPN. AT&T VPN provides Internet Protocol/ Point-to-Point Protocol (IP/PPP), Internet Protocol/ Multi-link Point-to-Point Protocol (IP/MLPPP), Ethernet, and DSL access to the VPN.

Private Line connections to the AVPN are available at speeds ranging from 64Kbps to 622 Mbps using PPP/MLPPP protocols.

IP MPLS ports in the MLPPP format are available in speeds of NxT1 at the following port speeds:

- 3.088Mbps
- 4.632Mbps
- 6.176Mbps
- 7.720Mbps
- 9.264Mbps
- 10.808Mbps
- 12.352Mbps

MPLS U.S. Ethernet connections to AVPN are available at speeds as follows (where available):

- **Access Speeds.** 5M, 10M, 20M, 50M, 100M, 150M, 200M, 250M, 300M, 400, 500, 600M, 700M, 800M, 900M, 1G, 10 G (1 and 10 Gbps subject to vendor availability)
- **AVPN defined Ethernet port speeds (Mbps).** 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 20, 30, 40, 50, 60, 70, 80, 90, 100, 150, 200, 250, 300, 400, 450, 500, 600, 700, 800, 900, 1000 and 10,000 Mbps,



- **VLAN Logical Channel Speeds (Mbps).** 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 20, 30, 40, 50, 60, 70, 80, 90, 100, 150, 200, 250, 300, 400, 450, 500, 600, 700, 800, 900, 1000, 10,000 Mbps

Collocation Equipment Requirements

Service delivery will be provided on one of the services mentioned above. The implementation documentation for the collocation equipment needed for the service will be provided to DIR when the specific service has been identified.

Capacity Management

Decisions to add capacity to the AT&T IP/MPLS network are based on real-time measurements of current network loads along with trending data based on both business and traffic forecasts. AT&T manages capacity for different traffic classes (and services) by measuring traffic in different classes (i.e., CoS4 or CoS6) in use today to ensure that performance targets (e.g., latency, jitter, packet loss) are maintained across the AT&T network. AT&T has upgraded many of our tools to include measurements across all of the various CoS options and service types.

AT&T's IP/MPLS network is designed to provide excellent performance and meet its Service Level Agreement commitments even in the event of a single link or single node failure across all service types. AT&T calls this engineering practice "survivability" and engineers its network for single-link and single-node "survivability." An example of AT&T's engineering for survivability for uplinks is the following: if a single router has two uplinks, at such point that the peak hour utilization reaches a consistent 42% over time, additional capacity is ordered, with the goal to have the third uplink in place before 47% utilization is reached; this practice then ensures network "survivability."

Network Interface Security Plan

AT&T's proposed methodology for securing customer data is comprised of a two-piece design approach/response:

1. **Point of Interconnect.** Per RFO requirement, AT&T will provide detail regarding the multitude of features built into AT&T's IP network to secure data at the point of interconnect
2. **External Security Capabilities.** DIR has the option to extend the security of customer data beyond the MPLS interconnect via AT&T's external security capabilities

Point of Interconnect - AT&T IP Network Security

AT&T's methodologies for securing data throughout its IP Network begin with the following design principles and philosophies. Any reliable network security model must include the comprehensive, holistic type of approach outlined in the following sections.



- **Defense-in-Depth.** One of AT&T's fundamental security design principles is the strategy of "Defense-in-Depth" to provide a multi-layered secure environment. "Defense-in-Depth" ensures that many integrated mechanisms provide multiple levels of protection against attacks. Should one security mechanism be breached, other mechanisms continue to provide protection and prevent or limit the potential damage.
- **Prevention.** AT&T focuses on preventing network attacks by designing security into every AT&T network and service from the start, from architecture to deployment, using the best available methods and technology. This includes designing its networks with security as a primary concern. AT&T has adopted measures to ensure that its network, systems, and services are secure against all known attacks.
- **Security Management.** AT&T is focused on deploying a variety of methods and systems for dealing with the evolving security environment. Areas of interest include software management and system integrity; configuration management, traffic measurement and detection; response and mitigation; and post-event analysis and remediation. As part of this effort, AT&T is moving intelligence into the IP network to eliminate the costly inefficiencies of deploying security solutions at the edge of the network.
- **Innovation Transfer.** AT&T has always treated its enterprise network and infrastructure as a "living laboratory" where innovations are put into place and rigorously tested for feasibility, scalability, and reliability. AT&T has long had a practice of developing and implementing security innovations on its enterprise network first and then extending those technologies to its networks and services provided to customers.

AT&T's philosophy exemplifies the due diligence and discipline that a service provider can take to successfully protect its network and computing infrastructures, as well as those of its customers. AT&T's expertise was demonstrated by its ability to ward off the MS-SQL worm attack that slowed global Internet traffic to a crawl for millions of users on hundreds of ISP networks in January of 2003 as well as its advance warning to its Internet Protect customers of attempts that became the Sasser worm in May 2004.

AT&T Internal IP Network Security Features

Specific elements built into AT&T's IP network that help secure customer data at the point of interconnect include:

- **Physical Security.** All nodes within the U.S. portion of the AT&T IP network are located in AT&T owned and maintained secure facilities. They are guarded and manned 24x7 and are only accessible to authorized personnel. All nodes are protected by uninterruptible power sources, including both battery backup and emergency diesel generators. In addition a robust disaster recovery scheme is tested regularly to ensure that all components work in the event of a power failure.
- **Functionality Policing.** All of the general, non-routing functions in the core routers are disabled. This enhances the performance of the network and reduces the potential of a hacker using general router capabilities to illicitly access the system.



- **IP Source Address Filtering (RFC2267).** AT&T's IP network security is enhanced through the use of IP Source Address Filtering. AT&T has installed source address filters on AT&T network routers at two places:
 - At all dedicated customer connections to the AVPN network
 - At all entrances from the public Internet to the AVPN network

At all dedicated retail customer connections, the source address of all inbound packets is examined to make sure it matches the IP address which AT&T expects to find on those packets; if the source address doesn't match, the packets are discarded. This is a key method that enhances the security of Service Providers networks since hackers typically try to hijack someone else's IP address in order to hide their identity while they are doing their mischief.

- **Private IP Addressing.** AT&T uses private AT&T blocks for backbone IP infrastructure addressing which are not publicly routable. AT&T blocks any packets destined directly to any infrastructure routers, regardless of protocol type. AT&T does not allow any diagnostic or other packets to be directed to backbone routers.
- **BGP Authentication.** Border Gateway Protocol (BGP) MD5 authentication is implemented on all AT&T's U.S. peering links, most of its Most of World (MoW) peering links, and can be implemented on customer dedicated Internet access links (MIS/GMIS), upon customer request. MD5 authentication on BGP routing ensures that route announcements for a given network (autonomous system) are indeed being received from that network (AS) and not an imposter. It also prevents BGP resets from being received by an unauthorized source, thus helping to maintain network stability.
- **Least Privilege.** Infrastructure routers and Provider Edge (PE) interfaces are hardened by turning off, or severely restricting, unnecessary protocols and ports.
- **Route Transaction Limits.** Route dampening is used to limit the rate, or total number, of route update transactions performed by a router.
- **TACACS+ Authentication.** TACACS+ centralizes administration of users that have access to network elements. Thus, AT&T does not have to separately administer the users on each element. The TACACS+ security mechanism allows a separate access server (the TACACS+ server) to provide the services of authentication, authorization, and accounting independently. Each service can be tied into its own database or can use the other services available on that server or on the network.
- **Center and Service Complex Protection.** Network Management centers, Data Centers, and service complexes are protected by firewalls and intrusion detection systems, another example of domain separation.
- **Automated Security Tools.** Automation of perimeter security tools provides additional protection of AT&T's MPLS network. AT&T has focused on automated methods to ensure that customer-edge (CE) to provider-edge (PE) routes are properly managed and



represented in VPN Forwarding and Routing (VFR) instances, and has developed several innovative tools in support of managing the MPLS VPN environment.

- **Event Threat Analysis.** Monitoring of IP traffic to provide early warning of Internet viruses and worms by capturing, monitoring and analyzing traffic flow data to identify clear patterns of network anomalies by AT&T's security systems.
- **Industry Standard Security M&Ps.** Control of operational security in AT&T's network is strictly enforced to maintain high levels of reliability and availability. To accomplish this, AT&T operations follow mature and proven Methods & Procedures and are certified, wherever appropriate, to the highest industry standards. Additionally, all incidents are subject to comprehensive Root Cause Analysis to ensure that processes are improved.
- **Proactive Security Resolution.** AT&T provides response to security incidents by proactive teams trained in the details of MPLS as well as IP security. AT&T uses a multi-tiered approach to identify, respond to, and mitigate any detected security problems.
- **AT&T Labs.** AT&T Labs is developing innovative new techniques with MPLS for protecting customer traffic and systems. This ongoing research effort complements AT&T's development, engineering, and operations teams in a way that remains unique within the industry to ensure flawless execution of security practices and principles.
- **Proactive Network Security Probes.** AT&T Network Security continually probes its networks, both internally and externally, for security vulnerabilities using the same techniques as a potential intruder. AT&T compiles and analyzes test results, reports their findings to the organization that requested testing, and recommends measures to close the vulnerabilities that testing uncovered. In addition, AT&T employs deception technology (in the form of "honey pots" that use AT&T-patented technologies) to look for potential subversive activity. This service is deployed on both intranet and on the Internet networks.

In addition, an experienced, trained AT&T Tiger Team will respond to any critical security incident.

- **Ongoing Security Evaluation.** The AT&T Network Security Evaluation Program (SEP) evaluates the security of both existing environments and for new features that are to be delivered within AT&T. This ensures that security is embedded into the lifecycle process for all AT&T services. SEP and client organizations jointly develop a Custom Security Plan specific to the client's environment.

AT&T's External Security Capabilities

AT&T can also provide a number of security services that extend beyond the MPLS interconnect interface in the event a customer requires additional security capabilities. These AT&T services supplement the inherent security of the AT&T IP network described above and include:

- Intrusion Prevention/Detection Service
- Managed Firewall Services (Network-based, Premises-based, or Router-based)



- Managed Encryption Services
- Secured Device Management Service

These products/services are described in detail as part of AT&T's Premier Services response.