AT&T Wireless Services, Inc.

Connecting Fixed-End Systems to the AT&T Wireless IP Network

Peter Rysavy, Primary Contributing Author

CDPD Product Development
AT&T Wireless Services, Inc.
PO Box 97061
Redmond, WA 98073-9761

Copyright Notice

For questions about this document, please contact:

Bonnie Beeman, Manager
CDPD Product Development
AT&T Wireless Services, Inc.
PO Box 97061-6702
Redmond, WA 98073
(425) 580-6702
bonnie.beeman@attws.com

Connecting Fixed-End Systems to the AT&T Wireless IP Network

Contents

Connecting Fixed-End Systems to the AT&T Wireless IP Network

This document is for new or potential customers and network engineers who are developing new network applications or porting existing applications to use with the AT&T Wireless Services (AWS) Wireless IP network. The AT&T Wireless IP network is based on Cellular Digital Packet Data (CDPD) technology. This document describes the elements of the AT&T Wireless IP network and presents customers with unique factors to consider when connecting fixed-end systems (hosts) to the AT&T Wireless IP network.

This document builds upon an understanding of how the AT&T Wireless IP network functions. AT&T Wireless Services has additional white papers to help you better understand wireless IP network technology, such as:

- Application Considerations for Mobile-End Systems
  This document describes the unique aspects that should be considered when writing applications for a wireless (cellular) mobile data environment.

- AT&T Wireless IP Network Security

  This document addresses security issues and approaches for network solutions that use the AT&T Wireless IP network.

Contact your AT&T account representative for more details concerning these topics or to obtain copies of these white papers, you may visit our web site at http://www.attws.com/business/gov/explore/wireless_ip/network/white_papers.shtml

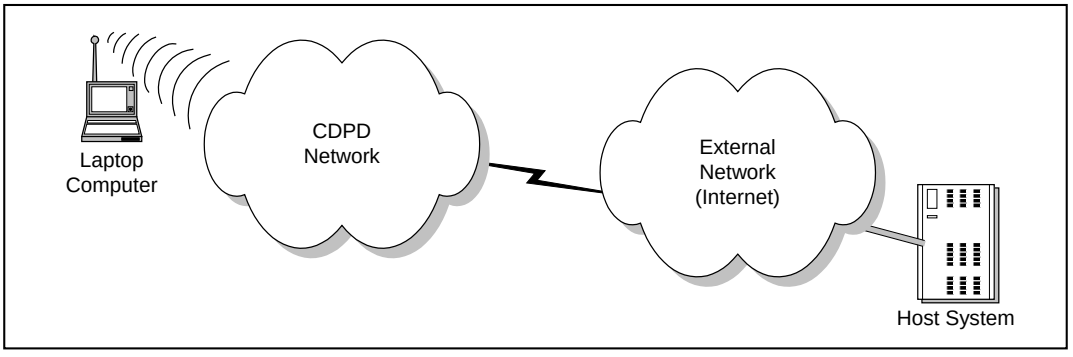
1 Introduction

When cellular telephone technology emerged in the early 1980s, the notion of wireless voice communication moved from the realm of possibility to that of reality. In the last decade, cellular telephones—which carry voice messages via radio frequency channels rather than traditional telephone lines—have enhanced and dramatically changed our lives by giving us not just wireless communications, but mobile communications. With the popularity and success of cellular phones, it was not long before wireless service providers began to ask themselves why the cellular network, although originally designed for voice transmission, could not be used for data transmission as well. What would it take to access data from a remote location using a wireless communications device? Cellular Digital Packet Data (CDPD) technology was developed in answer to this question.

The CDPD network architecture is composed of systems and a well-defined set of communications protocols. Together, these systems and protocols make the transmission of data across cellular networks possible.

The AT&T Wireless IP network operates as an extension of the existing IP-based data communication networks. Transmission Control Protocol, User Datagram Protocol and Internet Protocol (commonly referred to as TCP/IP or just IP) are the most widely used networking protocols today. They have become the industry standard because of their reliability and high degree of interoperability.

Figure 1: CDPD is an extension of other networks



The options for connecting the AT&T Wireless IP network to a customer's internal data network includes using frame relay, the Internet, or leased-line connections. This paper describes the pros and cons of these options and presents important considerations regarding other pertinent topics, such as redundant connections, protocol considerations, number of mobile devices, message volumes, and router configuration.

The next section reviews the aspects of the AT&T Wireless IP network architecture in relation to a customer's internal network infrastructure.

2 Wireless IP Network Architecture

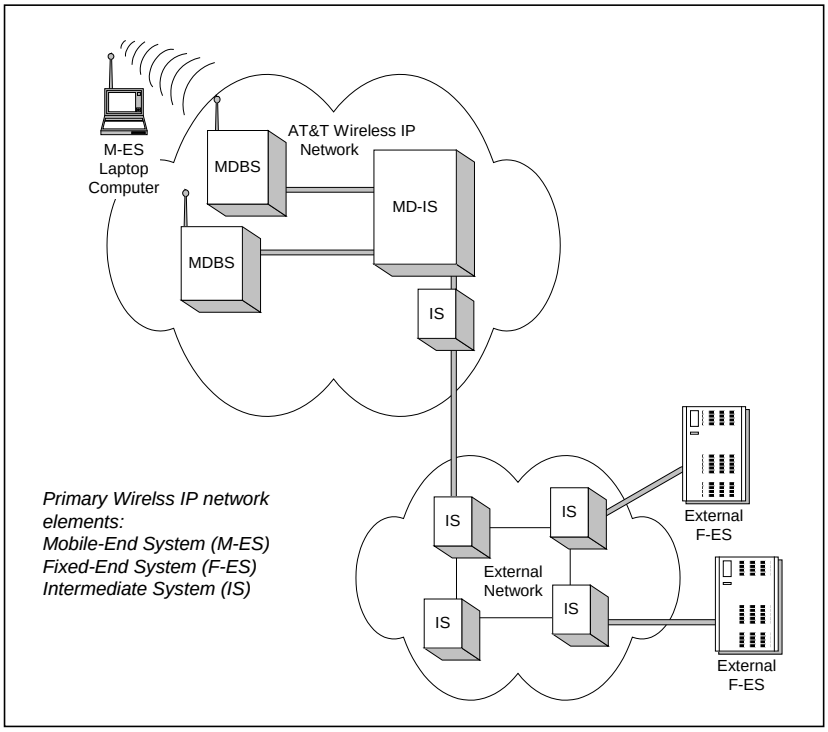
Two primary elements of the wireless IP network are the End System (ES) and Intermediate System (IS). In Open Systems Interconnect (OSI) terminology, a host system is known as an ES and a router is known as an IS.

2.1 End Systems

End Systems represent the actual physical and logical end nodes that exchange information. There are two types of ESs: a Mobile-End System (M-ES) and a Fixed-End System (F-ES). An M-ES accesses the AT&T Wireless IP network over a wireless interface called the airlink. The M-ES must contain an IP protocol stack in order to connect to the wireless IP network. The M-ES is, by definition, a system with a physical position that is subject to change. Examples of M-ESs are the AT&T PocketNet® compatible phone, or a CDPD modem-equipped laptop or handheld computer.

A Fixed-End System (F-ES) is a traditional host, server, or gateway that supports or provides access to data and applications. It can be a personal computer, workstation, minicomputer, or mainframe. By definition, its location is fixed, or permanent. Unlike an M-ES, an F-ES uses a wireline connection to the AT&T Wireless IP network. In the AT&T Wireless IP network environment, M-ESs and F-ESs are peer network entities—the origin and destination of all data transmissions. Figure 2 shows the relationship of data flow between an F-ES and M-ES via the IS.

Figure 2: Network elements



External F-ESs, which reside outside the AT&T Wireless IP network, are owned, operated, administered, and maintained by corporations or other entities outside the direct control of the AT&T Wireless IP network. In most cases, an F-ES is a traditional host system, server, or gateway that provides data or application services.

When an external F-ES is functioning as a gateway, it can provide access to non-IP compatible host systems such as those using SNA, DECnet, IPX/SPX™, and AppleTalk® network protocols.

2.2 Intermediate Systems

Intermediate systems relay packets from the ES and route them to their intended destinations. The AT&T Wireless IP network uses two types of IS:

- generic
- Mobile Data Intermediate System (MD-IS).

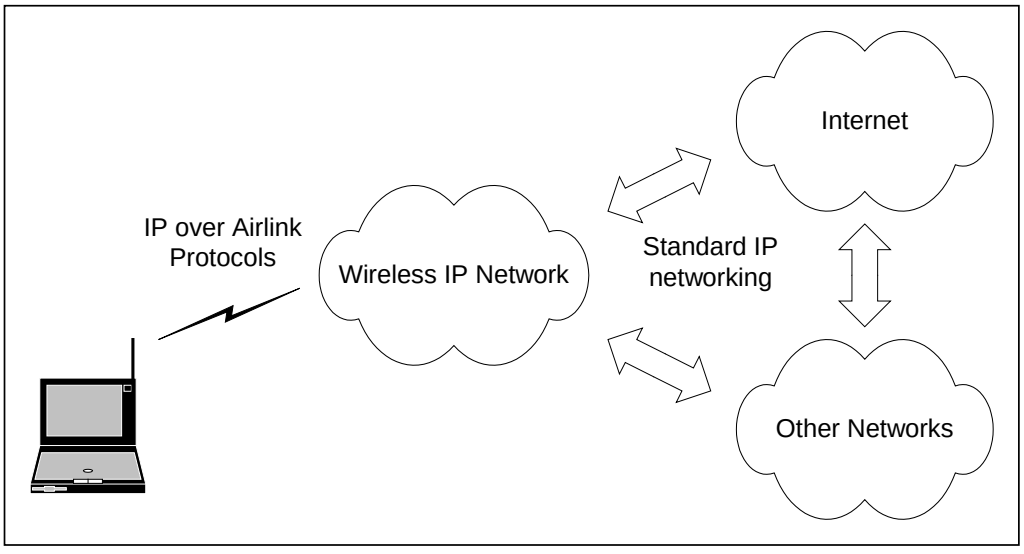
A generic IS is simply a router that has no knowledge of CDPD and M-ES mobility issues. These generic ISs, which form the backbone of the AT&T Wireless IP network, are standard, commercial, off-the-shelf routers that support IP (e.g. Border Gateway Protocol, Open Shortest Path First Protocol) and OSI network protocols.

An MD-IS is a specialized IS that routes messages based on its knowledge of the current M-ES location. The MD-IS is the core element of the AT&T Wireless IP network. An MD-IS receives data from an origin network entity (an M-ES or F-ES) and forwards the data to the destination network entity (an M-ES or F-ES).

2.3 Interconnection with Other Networks

The AT&T Wireless IP network interconnects with other networks, including the Internet and corporate intranets, based on Internet Protocols (IP). IP is used as the networking protocol from the M-ES to the F-ES. See Figure 3.

Figure 3: IP used from M-ES to F-ES



In this way, IP provides a seamless connection between the AT&T Wireless IP network and the Internet or intranet. It is seamless because an IP datagram is routed to and from an M-ES just as if the M-ES were any other Internet client. The AT&T Wireless IP network also provides a feature to block communication between the M-ES and the Internet by provisioning a "secure IP" address for an M-ES. See the white paper AT&T Wireless IP Network Security for more information, located on the ATTWS Internet web site:
http://www.attws.com/business/gov/explore/wireless_ip/network/white_papers.shtml.
End-to-end traffic between M-ESs and F-ES are maintained by transport layer protocols, either TCP or UDP.

What types of provisions are necessary when connecting an F-ES to the AT&T Wireless IP network? If the customer elects to access a server that is publicly available on the Internet, no provisions are necessary. However, if the F-ES is located within a customer's private network, or the customer needs a secure connection across the Internet, then it is important to consider the best approach for connecting to the AT&T Wireless IP network. The next section identifies the points to consider when evaluating the available options.

3 Connecting an F-ES to the AT&T Wireless IP Network

The three principal approaches used for connecting an F-ES (host, server, proxy server, or gateway system) to the AT&T Wireless IP network are via:

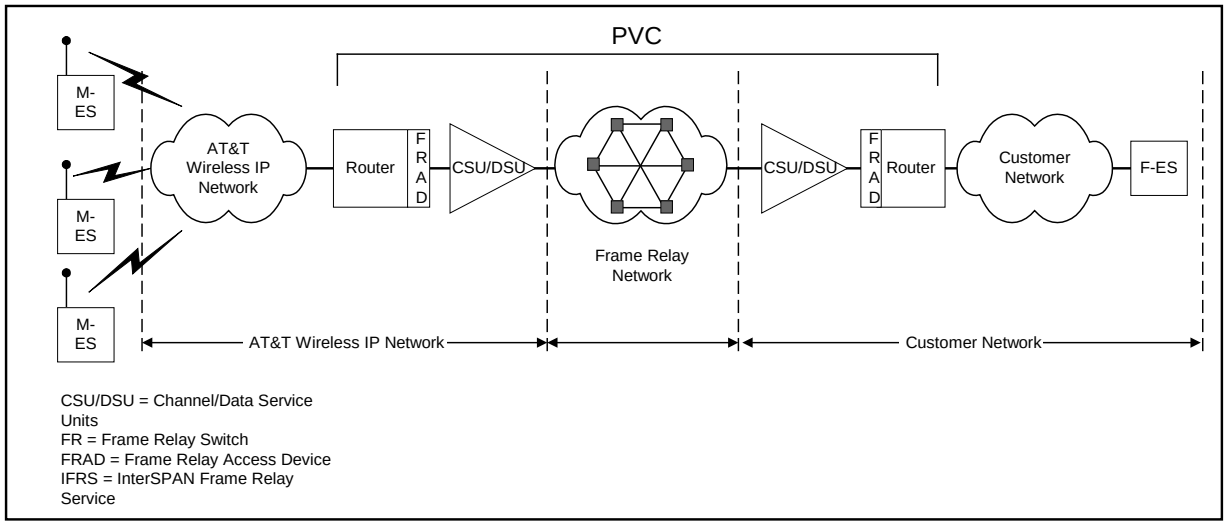
- frame relay
- the Internet
- a leased-land-line connection.

The best choice for a customer depends largely on their anticipated volume of data transmissions, the number of mobile devices requiring support over their F-ES connection, security concerns, and the current phase of their application development. For example, the type of F-ES connection a customer uses in a field trial may differ from the one they use in the final deployment of the application.

3.1 Connecting via a Frame Relay Network

Frame relay is a packet-oriented communication method for networks that operate at Layer 2 of the ISO model for networking. It is used as a wide-area network (WAN) connection over public and private networks and offers high performance (56 Kbps to 1.544 Mbps). Connections to the AT&T Wireless IP network are usually on the lower end of this range. It is often called a fast-packet switching network because tasks such as error checking, packet sequencing, and packet acknowledgment are handled by the end systems involved in the transmission rather than by the network itself. This allows the network to operate at much higher speeds than other packet switched networks, such as X.25, which perform these tasks within the network itself. Today, frame relay is one of the primary methods used to provide a link between a customer's network and the AT&T Wireless IP network. See Figure 4. In the future, Asynchronous Transfer Mode (ATM) circuits will also be available for customers who need to support a high volume of data traffic to their mobile systems. This will be especially important as new high-speed wireless data services become available. Frame relay and ATM are complementary services; transitioning from frame relay to ATM is relatively straightforward.

Figure 4: AT&T Wireless IP network connection to a frame relay network



AWS provides connection to the AT&T Wireless IP network through public carriers that offer frame relay services. Connecting a customer's F-ES to a frame relay network requires a router equipped with a frame relay access device (FRAD) interface, and a CSU/DSU located at the customer's network premises.

A FRAD is an access device through which networks of different protocol environments, such as Token Ring, Ethernet, or SNA, can connect to a frame relay wide area network. Generally, FRADs are incorporated into the router itself. The CSU/DSU connects the data terminal equipment (DTE), usually a router, to a private or public phone network. The CSU/DSU is a termination point of the wireline network.

The wide area network connection is established by building a frame relay permanent virtual circuit (PVC) from the customer's frame relay network point-of-presence (POP) to the AT&T Wireless Services network. The customer's network must support IP protocols and have a public IP address for the router connecting to the frame relay POP and the F-ES host that is to be accessed by the M-ES.

3.1.1 Obtaining Frame Relay Service

AT&T Wireless Services now offers a connection alternative which greatly simplifies the process of obtaining a frame relay connection to the AT&T Wireless IP network. This offer, the AT&T Wireless Connectivity Option, provides all the necessary network components to connect a customer's site to the wireless IP network. Highlights of this offer include: a single point of contact for ordering, provisioning and billing, a low monthly rate for all necessary network components, no installation charge and the inherent reliability inherent of the AT&T Frame Relay network. For more information please read Appendix B: AT&T Wireless Connectivity Option or call the Advanced Network Services group at 1-800-552-3373.

There are several other frame relay service providers who can implement a permanent virtual circuit (PVC) from a customer's site to the wireless IP network. Currently, connections exist between the AT&T Wireless IP network and the frame relay service providers listed below:

- AT&T Frame Relay Service, 1-800-552-3373,
  http://www.ipservices.att.com/data/framerelay/framer.html

- Paradigm 4, (425) 398-2200,
  http://www.paradigm4.com/

- Qwest (USWest), 1-800-246-5226,
  http://www.uswest.com/pcat/large_business/product/1,1749,93_4_2,00.html

- WinStar™, 1-800-961-8800,
  http://www.winstar.com/products/data/wan/content_frame.asp

AT&T Frame Relay Service, Paradigm4, and Winstar™ provide national service whereas Qwest provides regional service. To set up a frame relay PVC connection for Winstar or Qwest, an AT&T Wireless Sales representative can assist customers with the installation requirements.

Typically, there is an initial set up fee for installing a circuit, plus a monthly service fee. Charges can vary based on location, though nationwide carriers offer distance-independent circuits.

Some frame relay carriers have connections with other frame relay carriers. In some instances, these interconnections between frame relay carriers make it possible to establish a PVC from a customer's site to the AT&T Wireless IP network service using an existing frame connection that is not necessarily from one of the listed providers.

An important component of a frame relay connection is a dedicated circuit from a customer's facility to the frame relay carrier. This circuit will be either a DS0 circuit capable of supporting a committed information rate up to 56 Kbps or a DS1 circuit (T1 service) capable of rates up to 1.5 Mbps. Rates above 56 Kbps (e.g. 128 Kbps) are generally obtained by using a fractional T1 circuit. The circuit is obtained from a local exchange carrier, and pricing for this circuit is typically separate from frame relay charges. See the section entitled "Factors to Consider," for a discussion of bandwidth requirements.

The AT&T Wireless IP network has a dual T1 connection to the AT&T Frame Relay Service and a single full T1 connection to Qwest and Winstar.

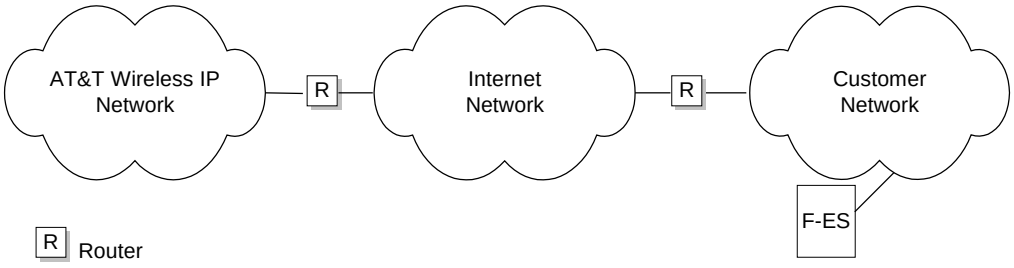
Once installation and service arrangements are made, the circuit is ordered to connect your site to the frame relay service point. Customer hardware requirements include a router and CSU/DSU. The router provides a connection between the incoming frame relay connection and the customer's local network environment. The router and CSU/DSU can be obtained through the frame relay service provider or from manufacturers, such as Cisco Systems® or Nortel Networks. AWS does not recommend any specific equipment providers, though support issues may be resolved more easily if you use Cisco Systems® equipment.

See the section entitled "Redundant Connections" for a discussion of how to set-up a redundant connection with frame relay.

3.2 Connecting via the Internet

The Internet is a mesh of interconnected computers and computer networks around the world. It interconnects local area networks (LANs) in federal agencies, research institutes, libraries, hospitals, universities, and other businesses and institutions. Data packets traverse the Internet via thousands of communication pathways—direct network connections, leased lines, satellite and microwave links, and so on. One of the largest networks in the world, the Internet is widely available, highly accessible, and offers a broad range of services. The AT&T Wireless IP network is easily connected to the Internet because both networks support and are based on IP protocols. In addition, the AT&T Wireless IP network has two direct connections to the Internet, through AT&T WorldNet and UUNET.

Figure 5: The AT&T Wireless IP network connection to the Internet



The AT&T Wireless IP network is easily connected to the Internet because both networks support and are based on IP protocols.

Many companies that have dedicated Internet connections find the Internet is an efficient method for connecting their remote workers to corporate information. For instance, it costs less on average for a remote worker to make a local call to a local ISP and use the Internet to access their corporate network than it does to make a long distance call to a dial-up remote access server. As a result, an increasing number of products are becoming available to support remote access via the Internet. These products include security features that authenticate remote users, restrict access to select services, and encrypt communications. Many of these products are used to support remote workers using IP communications.

The Internet can be an attractive option for connecting to the AT&T Wireless IP network because it is the easiest to deploy with no additional hardware or software requirements if a customer already has an Internet connection in place. As long as the connection is a dedicated connection — one that uses a router — it is appropriate for wireless IP F-ES connection. It is important to analyze the security provisions of an existing Internet connection since these may need to be adjusted to support AT&T Wireless IP mobile systems. Before making a decision to use the Internet for connecting and F-ES to the Wireless IP network, the volume of data between M-ES's and F-ES's should be taken into consideration. The Internet is not recommended for high volume traffic, nor traffic that is sensitive to latency. This is discussed further in the following two sections.

Unlike telephone networks, the Internet is not centrally managed. It is not one network but rather the interconnection of a large number of networks worldwide, including commercial, private, public, educational, and government systems. But the backbone fabric and the bulk of traffic today is carried by a small number of larger providers that monitor and manage their networks using sophisticated tools. Some national ISPs even offer quality-of-service metrics to their customers. The Internet has steadily become more reliable and an increasing number of businesses today trust it for critical corporate communications.

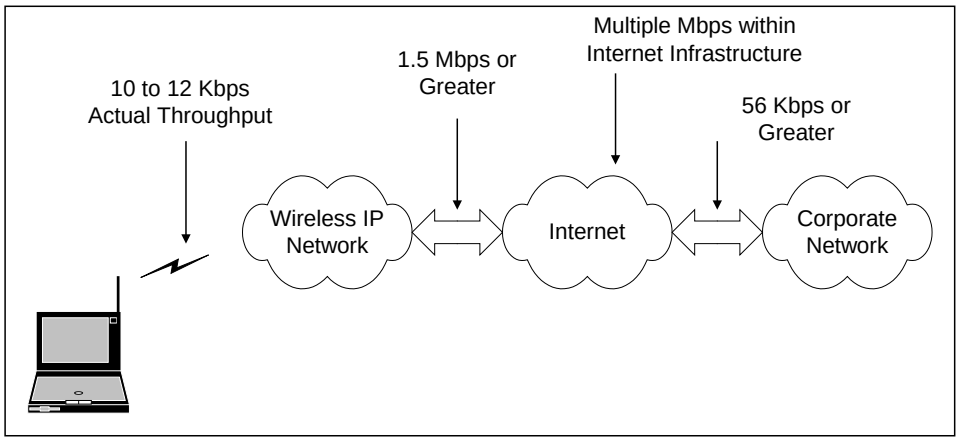
To use the Internet for fixed-end connections, we must consider whether it is up to the task. Is it reliable enough? Do throughput and latency issues exist? Is the Internet secure enough? We address these questions in this section.

3.2.1 Internet Throughput Considerations

Throughput refers to the rate at which data is communicated between two points; latency is the time is takes for data to traverse a network between two points. Throughput and latency are closely related, but they are distinctly different concepts and we discuss them separately. To understand the effects of the Internet on throughput, we must consider both the individual network connections as well as the software application.

The AT&T Wireless IP airlink operates at a rate of 19.2 Kbps, and yields an effective throughput of 10 to 12 Kbps after protocol overhead. This throughput is relatively low compared to all the other network links involved across the entire network. The AT&T Wireless IP network has high bandwidth internal components and a high bandwidth connection to the Internet, which also uses high bandwidth internal components. The minimum connection speed for a dedicated connection between a customer's ISP and a customer's network over a leased line or frame relay circuit is usually 56 Kbps. Clearly, providing a data path via the Internet for AT&T Wireless IP communications will not hinder the rate of throughput unless a large number of wireless users will be accessing the same connection simultaneously. See Figure 6.

Figure 6: Data rates involved in an AT&T Wireless IP connection through the Internet



It is important to consider the total load on the customer's dedicated Internet connection, which must carry the existing customer's Internet traffic as well as traffic to and from all the AT&T Wireless IP mobile workstations. The AT&T Wireless IP network traffic, however, should be minimal, because most wireless IP applications send and receive short transactions. For example, studies show that applications like PocketNet typically transmit 6500 bytes every 10 minutes[1].

AT&T PocketNet® Service applications in particular are very well suited for Internet fixed-end connections. Messages are small, many of the user screens are stored locally allowing users to navigate menu choices without generating any network traffic, and the AT&T PocketNet infrastructure uses sophisticated compression to minimize the amount of data transmitted.

[1] Lucent Technologies, Input parameters evaluation study, April 2000

3.2.2 Internet Latency Considerations

Latency, or delay, refers to the amount of time required for data to traverse from one point to another. Each link in a network introduces additional latency. The wireless IP network introduces a typical delay of 250 msec. to 350 msec. for a short message, though this value can increase in environments with low radio signal strength. The Internet itself adds a somewhat unpredictable amount of latency, depending on numerous factors such as the number of network hops, time to live counts, and the degree of link congestion. But for a well-designed wireless IP application, even worst-case network delays should pose no problem. The delay that the user experiences is determined by the size of messages involved, and the number of messages that must be sent back and forth to complete an operation or transaction. Minimizing message size and the amount of back and forth traffic are two key attributes of well designed wireless applications, wireless middleware, and wireless protocols such as the Handheld Device Transport Protocol (HDTP) and the Handheld Device Markup Language (HDML), as used in the AT&T PocketNet® Service.

3.2.3 Managing Internet Quality of Service

If throughput and latency are of concern, there are measures available to optimize an Internet connection. Comparison shopping of ISPs is useful in identifying what bandwidth the ISP uses to connect to the Internet backbone and at what percentage of capacity the ISP operates. Some ISPs occasionally saturate their connections, which can result in dropped packets. This causes increased latency and lowers throughput. There may also be a larger number of network hops involved when connecting with a smaller ISP. It is useful to trace the routes between a customer's network and the AT&T Wireless IP network to determine whether the number of hops involved is efficient.

The AT&T Wireless IP network connects to the Internet using high-speed connections to AT&T WorldNet® and UUNet (MCI WorldCom). The primary connection is AT&T WorldNet with UUNet always available as an immediate backup connection. By default, all traffic leaving the AT&T Wireless IP network destined for a customer F-ES traverses the AT&T WorldNet connection. Traffic from the F-ES destined for the AT&T Wireless IP network may traverse either the AT&T WorldNet or UUNet connection, depending on which of these two networks has closer routing to the customer's Internet service provider.

In general, using AT&T WorldNet® as the customer's ISP optimizes the degree of throughput and latency because of the minimal number of hops between a customer's network and the AT&T Wireless IP network.

3.2.4 Internet Security Considerations

In using the Internet for fixed-end connections, there are a number of security considerations. The primary consideration is that for an M-ES to communicate with an F-ES, a customer needs to configure their firewall to support inbound data communications from the M-ES via the Internet.

There are a variety of connection options available to a customer securing an Internet connection. Factors to consider in choosing an option are the:

- existing network configuration
- existing firewall configuration
- existing ability (or inability) for remote users to access internal company information via the Internet
- desired level of security
- services to be accessed by the M-ES
- sensitivity of the material being communicated.

Just as there are many ways of securing a physical building, there are many ways of securing a network. The good news is that for any situation and any requirement there are good security solutions available. Unfortunately, no exact guidelines are available, as the best approach will vary depending on the customer's particular circumstances.

The first thing to know is that there is nothing special about wireless IP communications. You should treat the M-ES in the same way that you treat any other Internet client that needs access to particular services on your corporate network. Since IP packets from the M-ES come via the Internet, they are indistinguishable from other traffic from the Internet except for the IP source address. Note that M-ESs use fixed IP addresses that are assigned by AT&T Wireless Services, which is an added benefit for security management. This differs from a remote worker who connects to the Internet via an ISP that assigns a temporary IP address.

To allow AT&T Wireless IP network users to gain access to the customer network via the Internet, the following items should be considered:

- **User Authentication**
  The security system should authenticate the remote user by requiring a password or other information such as from a hardware security token.

- **Server Authentication**
  Under some circumstances, a customer may want the remote user or remote application to be able to authenticate the server being accessed.

- **Service Authorization**
  Depending upon a customer's security policy, the security system should only provide the remote user access to specific servers or network hosts.

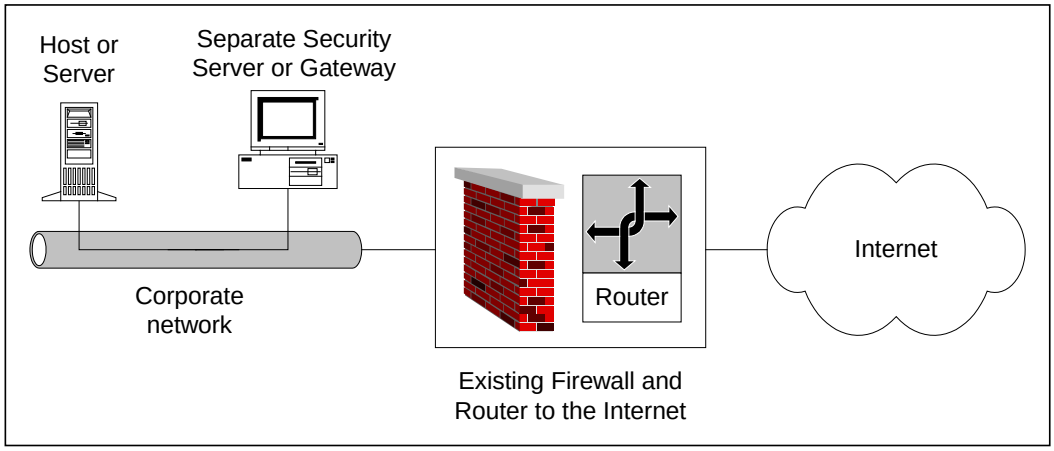
- **Message Integrity Confirmation**
  An M-ES and a customer's network should be able to confirm that messages have not been altered in transit. Hashing algorithms are available for this function.

- **Encrypting Communications**
  Although the AT&T Wireless IP network employs RC4 encryption on the airlink, a security system should encrypt communications to maintain privacy on an end-to-end basis.

This may seem like a formidable list, but there are a number of products today that implement most or all these functions. The most conservative security stance is to not make any assumptions about the security of any particular link, whether in the Internet or within the AT&T Wireless IP network itself. Extensive security information can be found in the white paper entitled, AT&T Wireless IP Network Security at http://www.attws.com/business/gov/explore/wireless_ip/network/white_papers.shtml

The first line of security is a customer's existing router and firewall. Router and firewall vendors are busily adding new security features to their products. Many are supporting new security standards as the standards become finalized. A customer's existing router or firewall may already offer adequate security features. Alternatively, a customer can implement a security solution that serves M-ESs by installing it behind the customer's Internet router and firewall on a security server or gateway. See Figure 7. As discussed in the next section, Virtual Private Networking," AT&T Wireless Services offers a secure method of using the Internet for fixed-end connections.

Figure 7: Security system can be implemented in multiple locations



There are two fundamental types of wireless IP security solutions. One solution is packet filtering and port monitoring, which is implemented at the edge of the customer's network. The other is a virtual private network solution that involves implementing a secure "tunnel" across the Internet.

Packet filters examine each incoming packet's source address and port number (which defines the applications involved) against a detailed set of rules. Customers can program their firewall to accept communications from the AT&T Wireless IP network nodes by specifying the fixed IP addresses and ports associated with the AT&T Wireless IP network accounts. Packet filtering provides a limited level of security, and most security experts recommend that it be only one component of an overall security system. AWS recommends an approach that does not depend solely on the mobile's IP address. This can be done using virtual private networking as discussed in the next section.

3.2.5 Virtual Private Networking

There are two fundamental ways of applying VPN technology to AT&T Wireless IP network connections. One way is to use the AT&T VPN Gateway. The other way is to independently implement an IP VPN solution. Additional details on both approaches are provided in the AWS white paper AT&T Wireless IP Network Security. In choosing a customer-implemented VPN or other end-to-end security solution for wireless IP communications, a customer should make sure the security product provides these elements:

- **Mobile Support.** The product must support mobile systems. A product that only operates on a server-to-server basis will not be useful.

- **Software Implementation.** Some VPNs are implemented in hardware, which is not usually suitable for mobile systems. Look for software implementations.

- **Stack and Modem Support.** The VPN client software must be compatible with the IP stack in the M-ES. Moreover, the client software must be compatible with the SLIP or PPP mode used between the mobile computer and the CDPD modem. If using Microsoft® Windows®, ensure the product is compatible with the version of Windows® being used**.** Many modem manufacturers have on-line support for using their modems with particular VPNs.

- **Firewall Support.** The product must be able to co-exist with a customer's existing Internet firewall. Either the product is implemented at the firewall, in which case this should not be an issue, or the customer must be able to configure their firewall to pass VPN traffic to the security server or gateway.

Refer to "

Appendix A: VPN Products" for a list of VPN products that may be applicable.

3.3 Connecting via a Leased Line

A leased-line connection involves installing a dedicated DS1 (1.5 Mbps T1 service) circuit between a customer's site and the AWS MD-IS complex in Bothell, WA. This approach typically is used if the customer's network requirements preclude the use of frame relay or the Internet for F-ES connections. Since this option is expensive for both the customer and for AT&T Wireless Services, and since it does not use network resources efficiently, this is not a preferred approach and is only available under special circumstances. Leased line connections are generally only feasible for customers located in the Seattle metropolitan area.

Once the customer makes installation and service arrangements, the customer must arrange through their local telephone company for a circuit to connect their company site to the MD-IS complex in Bothell, WA. For leased line connections, AWS must dedicate a router port to the connection. A customer must also have routers and CSU/DSUs available at their site. Routers provide a connection between the incoming leased-line connection and the customer's local network environment. Routers can easily be obtained from a variety of manufacturers including Cisco Systems®, Nortel Networks, and others.

4 Redundant Connections

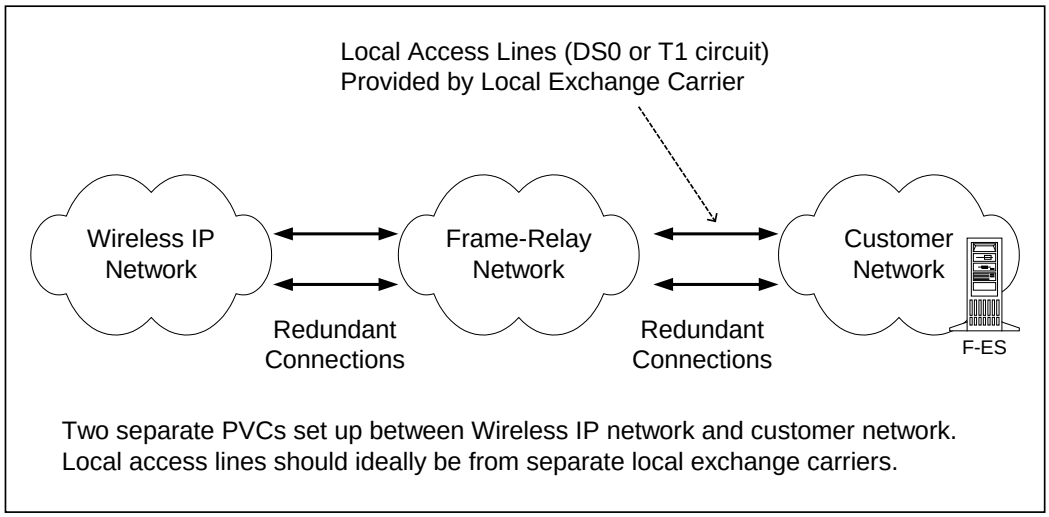
When deploying a critical application, redundant F-ES connections should be considered. The advantage offered by a redundant connection is that if one connection fails, the other connection can automatically take over so that communication between the wireless IP mobile user and the fixed-end system is not interrupted. The goal is to provide a constant and seamless service for Mobile End Systems.

The AT&T Wireless IP network itself has redundant connections. For Internet communications, the primary connection is via AT&T WorldNet®, with a backup connection via UUNet (MCI/WorldCom). These ISP connections terminate on different routers and diverse facilities on the AT&T Wireless IP network. For frame relay connections, AT&T has redundant connections to the AT&T Frame Relay Network. A redundant connection is also planned for Winstar™. These redundant connections require manual intervention to restore service, but will be self-healing in the future.

When using frame relay for fixed-end connections, a customer can establish fully redundant fixed-end connections by creating two separate PVCs via the AT&T frame relay service. Each PVC connects to a separate Data Link Connection Identifier (DLCI) within the AT&T Wireless IP network. To implement the redundant connection, routers both at the AT&T Wireless IP network and at a company's internal network must be programmed to use both PVCs. One PVC can be designated as primary with the other PVC as a backup, or both PVCs can be used simultaneously to improve throughput. In case of failure of one of the PVCs, data traffic can be automatically routed over the other PVC. For such automatic handling of failures, both PVCs must be active.

Customers can use one router with two ports (one port for each PVC connection) or customers can use two separate routers, which offers additional redundancy. In either case, using two PVCs in the manner just described will help protect the fixed-end connection from service disruptions at either end of the frame relay connection. Note that frame relay networks themselves have redundancy built into them. See Figure 8.

Figure 8: Redundant connections



Keep in mind that for true redundancy, the two circuits that connect a customer's network to the frame relay carrier need to be independent, and should not pass through the same local carrier central office or traverse the same physical route. This can be accomplished by using separate local exchange carriers, if available.

When using the Internet for fixed-end connections, a customer needs more than one connection to the Internet to establish redundancy. AT&T does not make any specific recommendations on how best to achieve this, except that two different ISPs should be used. A customer's redundant Internet connection combined with the AT&T Wireless IP network's redundant connection to the Internet, along with the proper configuration in the customer's network, will result in a fully redundant connection that spans from the AT&T Wireless IP network to the customer's internal network.

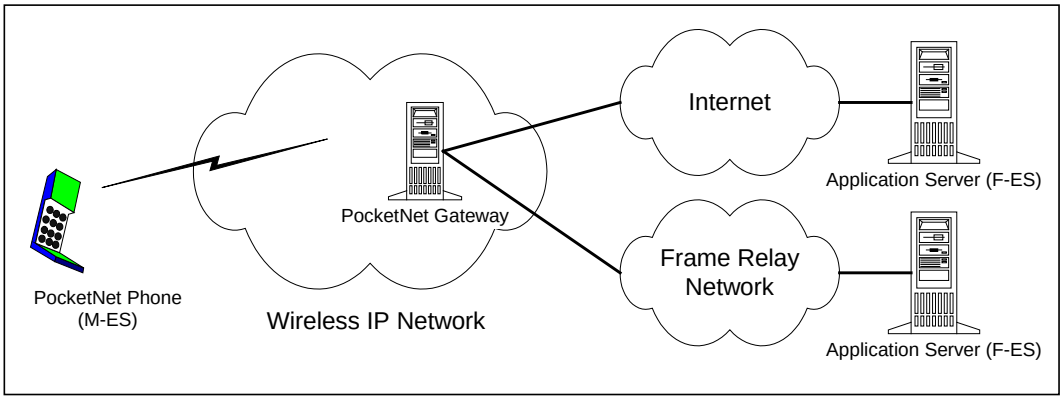
In all cases, AT&T cannot take responsibility for how to implement redundancy on a customer's end of the fixed-end connection. Please contact Advanced Network Services at 1-800-552-3373 for up-to-date information on available redundancy options, or talk with your AT&T Wireless Advanced Sales representative.

Customers using the AT&T Wireless Connectivity Option have additional redundancy options as described in Appendix B.

5 PocketNet® Compatible Phone

What feature differentiates the AT&T PocketNet® compatible phone? The PocketNet is different in that an F-ES (or application server) does not communicate directly with the M-ES (the PocketNet compatible phone) but with the PocketNet gateway that is owned and operated by AWS. The gateway translates application traffic from IP networks into a format optimized for wireless communications with the PocketNet compatible phone. See Figure 9.

Figure 9: An F-ES communicates with the PocketNet gateway



A customer who hosts their own PocketNet application requires a fixed-end connection from their own PocketNet application server to the AT&T Wireless IP network. This fixed-end connection can be any of the choices discussed in this white paper, including frame relay, via the Internet, or a leased line. The nature of this connection is no different than if a customer's F-ES was communicating directly with the M-ES, and all previous considerations apply.

Note that the Mitsubishi T-250 PocketNet® compatible phone can be used as a CDPD modem tethered to a computer using a serial cable. When used this way, communication does not involve the PocketNet gateway and takes place directly between the device connected to the PocketNet compatible phone and an F-ES.

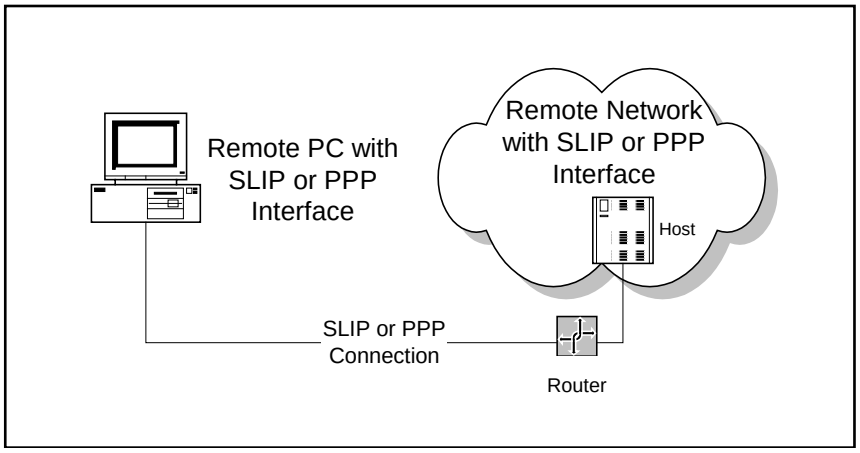
6 F-ES Protocol Considerations

The only method for connecting F-ES to the AT&T Wireless IP network today is by using IP protocols. IP is also the most straightforward connection approach because the IP protocol stack that resides on the F-ES does not need to be modified in any way, nor does a specialized router or gateway need to be employed. Further, the stack resident on the F-ES does not need to be from the same manufacturer as the IP stack resident on the M-ES. If an organization has standardized on a particular manufacturer's IP stack on a host or server, they are free to continue using it. A customer is encouraged, however, to use an IP stack on the M-ES that offers the capabilities required to provide a good interface to the wireless IP airlink (refer to the companion white paper entitled Application Considerations for Mobile-End Systems available at: http://www.attws.com/business/gov/explore/wireless_ip/network/white_papers.shtml

6.1 Use of SLIP and PPP in the AT&T Wireless IP Network

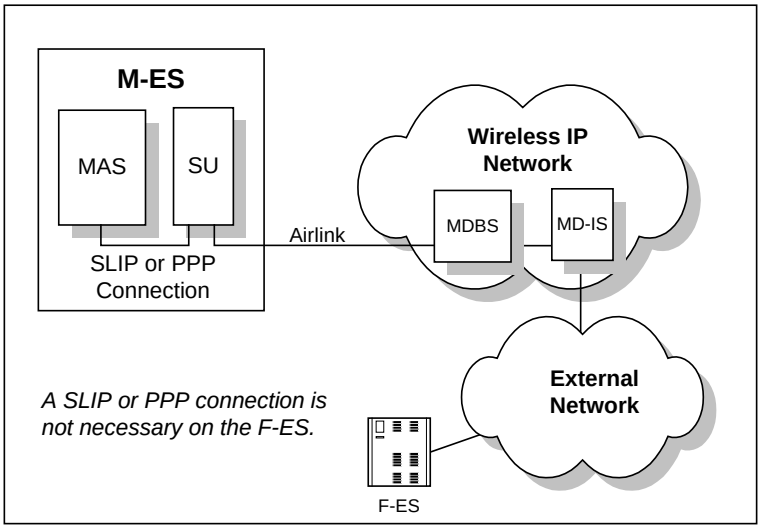
One possible point of confusion surrounding F-ES connectivity today stems from the fact that a Serial Line Internet Protocol (SLIP) connection or Point-to-Point Protocol (PPP) connection is used between the two subsystems that make-up the M-ES. These two subsystems are the mobile computer (technically referred to as the mobile application subsystem or MAS) and the CDPD modem (referred to as the subscriber unit or SU). This implementation differs from traditional SLIP and PPP implementations that can provide connections between hosts, servers, and routers over a communications line such as a modem connection. See Figure 10.

Figure 10: Traditional SLIP or PPP end-to-end connection



In a CDPD environment, the SLIP (or PPP) connection exists only between the mobile application subsystem (MAS) and the subscriber unit (SU). This is because the SU (which is a wireless modem) acts as the SLIP (or PPP) server and routes packets via the AT&T Wireless IP network to the F-ES. See Figure 11. To the F-ES, the M-ES simply appears as another network node or ES on its existing network.

Figure 11: Forwarding packets to an F-ES



For more information on the SLIP interface within the M-ES, refer to the companion white paper entitled Application Considerations for Mobile-End System available at

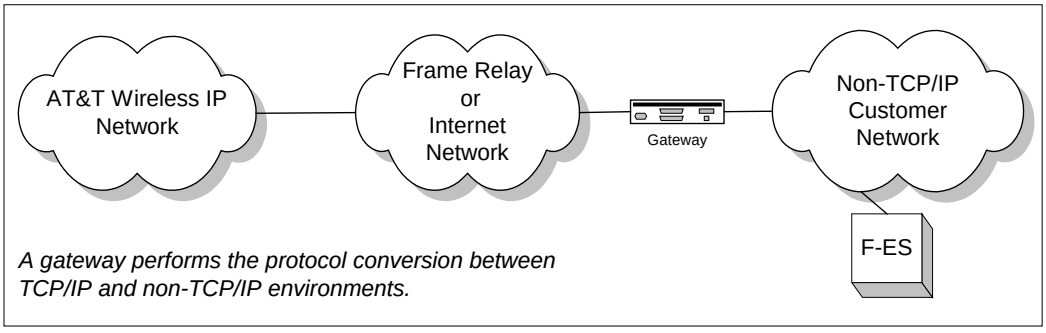
http://www.attws.com/business/gov/explore/wireless_ip/network/white_papers.shtml

Note that it is possible for SU vendors to supply a Network Device Interface Specification (NDIS) driver to establish communication between the IP protocol stack and the SU. NDIS is a standard interface for network devices in the Microsoft Windows environment between protocols stacks and network interface cards. When using network interface card drivers that conform to this specification, a customer can expect any NDIS compliant protocol stack to function. When using an NDIS driver, neither SLIP nor PPP are used. NDIS offers some advantages such as easier installations.

6.2 Using a Gateway to Link TCP/IP and Non-TCP/IP Environments

When an F-ES to which a customer connects supports non-IP protocols (such as SNA, IPX/SPX, NetBEUI, or DECnet), a gateway or similar type of protocol translation facility must be used. The gateway performs the necessary protocol conversion between the non-IP F-ES and the IP data stream received from the frame relay or Internet network. See Figure 12. This approach is typically used when the application is resident on a host system that already supports non-IP WAN-based communications. AT&T Wireless Services does not offer these gateways and, if used, they are the customer's responsibility to configure and maintain.

Figure 12: A gateway linking different environments



7 Factors to Consider

Other factors to consider before making a decision on how to implement a fixed-end connection to the AT&T Wireless IP network are identified in this section, including the AT&T provisioning process, the number of M-ES devices, message volumes, router configuration, and out sourcing.

7.1 AT&T Provisioning Process

It is important to consider the logistics involved in obtaining a fixed-end connection to the AT&T Wireless IP network. If a customer is using the Internet for their fixed-end connection, no action is required, unless an AT&T secure tunnel will be used, because the M-ES can communicate directly with the Internet. If, however, a customer is using a frame relay or leased line connection, it is necessary to make special arrangements with AWS for the provisioning of the F-ES connection. These arrangements are in addition to obtaining accounts for the M-ES.

The local AWS sales person will work with the customer and an AWS sales engineer. The sales engineer will explain details of the options described in this white paper, and will collect all the necessary customer information. The sales engineer will place a “network service order” to order the F-ES connection, which is processed by an operations team. This team will assign items such as router IP addresses and frame relay DLCI information.

The sales engineer will make recommendations for F-ES connectivity, but ultimately all costs and time frames associated with connecting to the AT&T Wireless IP network are the responsibility of the customer.

For additional information, you can also call Advanced Network Services at 1-800-552-3373.

7.2 IP Address Management

The F-ES must have a public Internet IP addresses for the AT&T Wireless IP network to route traffic, regardless of the type of fixed-end connection. Valid IP addresses are assigned by the Internet Corporation for Assigned Names and Numbers (ICANN),.[2] While AWS always assigns a fixed IP address to the M-ES, it can also provide a public IP address for the F-ES. If necessary, the customer should contact their local Advanced Sales representative or Sales Engineer about obtaining public IP addresses for fixed-end systems. AT&T policy guidelines do not support private IP addresses.

If a customer has more than one fixed-end System, a public IP address will need to be configured on each F-ES. In some cases, a customer may want to use network address translation to direct mobile access to its internal data network. The device performing network address translation can have a single IP address, but can forward IP traffic to multiple F-ESs. This approach can also be used if the customer is using non-public IP addresses within its network. AWS also does not perform any form of network address translation on behalf of the customer.

Note that there is not necessarily a one-to-one correspondence between IP addresses and F-ES, as some computing systems can support multiple IP addresses.

7.3 Number of M-ES Devices

The average number of M-ES devices that will simultaneously access a customer's F-ES is a factor to consider in making the most appropriate connectivity choice. For instance, if a customer has a large number of M-ES devices in the field, it is more likely that the customer will have a large number of users attempting to access the F-ES simultaneously. In this case, a customer will want to ensure that the bandwidth of the connection to the AT&T Wireless IP network is sufficient to handle the traffic and relative volume of data transmitted by analyzing the communications traffic to determine the bandwidth required.

[2] ICANN – Internet Corporation for Assigned Names and Numbers is a non profit organization that was formed to assume responsibility for the IP address space allocation, protocol parameter assignment, domain name system management, and root server system management functions previously performed under U.S. Government contract by IANA and other entities. See http://www.icann.org/general/abouticann.htm.

Customers should keep in mind that the geographic dispersion of the M-ES devices could influence the load on the F-ES connection. This is because CDPD uses dedicated channels in each cell site, but the channels are a shared public resource among multiple users and many organizations. If there are multiple M-ES operating within the same cell (or within the same sector if a "sectorized" cell), their combined throughput cannot exceed the bandwidth of the AT&T Wireless IP service in that cell, which is roughly 12 Kbps.

7.4 Message Volumes

In this context, message volume refers to the frequency of transmission as well as the length and nature of the data that customers transmit. Some applications transmit long, extended messages whereas others require numerous smaller transmissions to complete a single transaction. Still others contain only short, "bursty" data in single transmissions.

For applications that transmit extended messages, transmission speed is a primary concern. Speed is also a primary concern if you have a broad base of users sending messages. In both cases, a customer may prefer to use a fast link such as frame relay because of its reliable throughput and low latency.

Some traffic analysis will be made available shortly with the AT&T Frame Relay service, through Customer Network Management Services (CNMS). AT&T offers a course on CNMS and the reporting feature. If customers are interested in the reporting feature, they should contact their AT&T Wireless Advanced Network Services representative, or Customer Care at 1-800-552-3373.

7.5 Router Configuration

When connecting to the AT&T Wireless IP network via the Internet, there is little action required to provide for communication between the M-ES and F-ES other than to address security. In addition, the customer will require a fixed IP address.

If using a frame relay connection, however, there are some guidelines. The frame relay PVC will require a dedicated port on the customer's router. The router will require correct configuration to properly communicate with the AT&T Wireless IP network. Most importantly, the AT&T Wireless IP network uses statically defined routes, and dynamic routing is not supported.

Customers should only route IP datagrams that represent data traffic to the M-ES. Though the firewall at the AT&T Wireless IP network blocks any other communications, including routing protocols, any extraneous traffic consumes unnecessary bandwidth. In particular, customers should not make their default route the AT&T Wireless IP network.

In implementing a security policy, customers should be aware that the AT&T Wireless IP network will route IP datagrams from any M-ES (including M-ESs that belong to other wireless IP customers as well as M-ESs associated with other CDPD carriers) that are addressed to a customer's F-ES. Refer to the AWS white paper, AT&T Wireless IP Network Security for a detailed discussion of security considerations associated with fixed-end connections.

7.6 Out Sourcing & Managed Services

Though a customer can independently implement a fixed-end connection, they can also employ a network-consulting firm, or utilize an ISP. Not only can a third-party vendor help the customer obtain the service and configure their network correctly; a third-party vendor can also manage the equipment (e.g., routers) on an ongoing basis. AT&T provides Global Managed Internet Resources and can be located on the Internet at http://www.ipservices.att.com/ipaccess/gmis/ or can be reached at 1-800-288-3199.

8 Appendix A: VPN Products

AWS has identified a number of security products that may be applicable when using the Internet for fixed-end system connectivity. However, AWS does not endorse any of these products and recommends that AT&T Wireless IP customers do their own thorough evaluation. The companies listed are representative of the industry and the list is by no means exhaustive.

This list does not include packet-filtering products. Rather it emphasizes end-to-end security solutions. Products are listed alphabetically by vendor. Note that the approaches and range of services and features offered by VPN products varies considerably. Note also that these products should only be considered if the customer wants to implement their own VPN solution that spans from their M-ESs to their network. As discussed in this white paper as well as the AT&T Wireless IP Network Security white paper, AWS itself offers a VPN service to establish IPSec-based tunnels between the AT&T Wireless IP network and the customer's network

Company	Product	Further Information
Aventail	Mobile VPN	http://www.aventail.com
Axent	Raptor Mobile	http://www.axent.com/
Check Point Software	FireWall-1 SecuRemote	http://www.checkpoint.com
Extended Systems	ExtendNet VPN	http://www.extendsys.com/products/vpn/
Microsoft	Remote Access Services	http://www.microsoft.com
RadGuard	cIPro-client	http://www.radguard.com
RedCreek	Ravlin	http://www.redcreek.com/
Shiva	LanRover VPN Express	http://www.shiva.com/remote/
Sun Microsystems	SunScreen SKIP	http://www.sun.com/security/
TimeStep	Permit	http://www.timestep.com
VPNet	VPNremote	http://www.vpnet.com

9 Appendix B: AT&T Wireless Connectivity Option

AT&T Wireless Services has recently launched a new service called AT&T Wireless Connectivity Option (WCO). WCO combines frame relay service with a private line that extends from the customer network to the AT&T frame relay network. WCO uses the AT&T worldwide frame relay network, but WCO service and support is provided by AT&T Wireless Services. This allows customers to obtain Wireless IP service and frame relay service from one vendor. This cooperative arrangement between AT&T and AT&T Wireless Services simplifies a customer's provisioning, billing, and support.

The AT&T frame relay network is mature, stable, and widely available, with hundreds of thousands of private virtual circuits (PVCs) deployed worldwide. Since the network is extensively deployed throughout the United States, customers can readily obtain service regardless of their geographic location.

AT&T Wireless is a wholly owned subsidiary of AT&T Corporation. This close association allows both companies to benefit from the services of each other, and pass those benefits onto customers. The Wireless Connectivity Option is therefore the preferred connectivity option for customers.

9.1 Advantages

Wireless IP customers who receive WCO service enjoy these advantages:

- a single point-of-contact through AT&T Wireless Services for ordering, provisioning and service support
- a single, consistent, nationwide pricing plan
- a single bill for both Wireless IP and WCO charges
- support for two access speeds: 56 Kbps and 128 Kbps
- no start-up fees
- service support twenty-four hours a day, seven days a week
- superior mean time to repair
- a variety of redundancy options.

Table 1 contrasts the differences in features and benefits between WCO and other service providers.

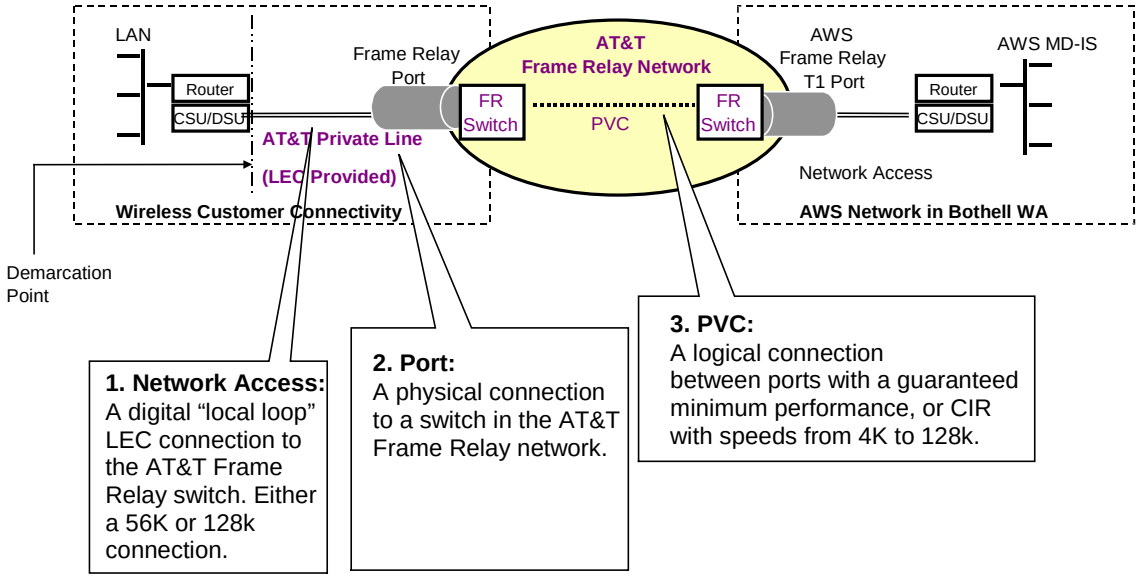
Table 1: Comparing WCO and other service providers

Feature/Benefits	WCO	Other Service Providers
Service Offering - Elements	Includes both a frame relay service and private line that AT&T obtains from the local exchange carrier (LEC). Multiple network access speeds, PVC, and committed information rates (CIR) are supported.	Winstar is the only other company that provides both frame relay service and private line.
Service Offering - Purchase	Customer can purchase WCO directly from AWS.	Customer must purchase services from a frame relay service provider and may also have to work with a local exchange carrier (LEC) to obtain a private line.
Service Offering – Coverage	WCO is available nationally through the extensive AT&T network.	No other frame relay service provider has a frame relay network with as many points of presence as AT&T.
Service Queries and Information	AWS provides support personnel to answer customer questions 24 hours a day, 7 days a week. AWS supports both the frame relay connection as well as the private line.	A customer must contact the frame relay provider directly for assistance.
Pricing	Simple competitive pricing with no start-up fees.	Start-up fees and installation charges are often involved.
Billing	AWS will use a single bill for Wireless IP and WCO charges.	In addition to their Wireless IP bill, customers will receive a bill from the frame relay service provider and possibly also from the LEC.
Mean Time for Ordering and Provisioning	AWS will complete orders within a 35-45 day timeframe	Order times vary depending on service provider
Mean Time to Repair	AWS will repair a frame relay problem in less than 4 hours. AWS will repair a LEC problem in less than 8 hours.	Mean time to repair varies considerably, and is usually more than 4 hours for a frame relay problem.
Network Availability	The AT&T frame relay network is one of the most reliable networks available. In addition, a variety of redundancy and backup options are available.	Other frame relay service providers do not offer the same level of reliability nor redundancy and backup options.

9.2 Network Overview

Figure 13 shows the components of WCO.

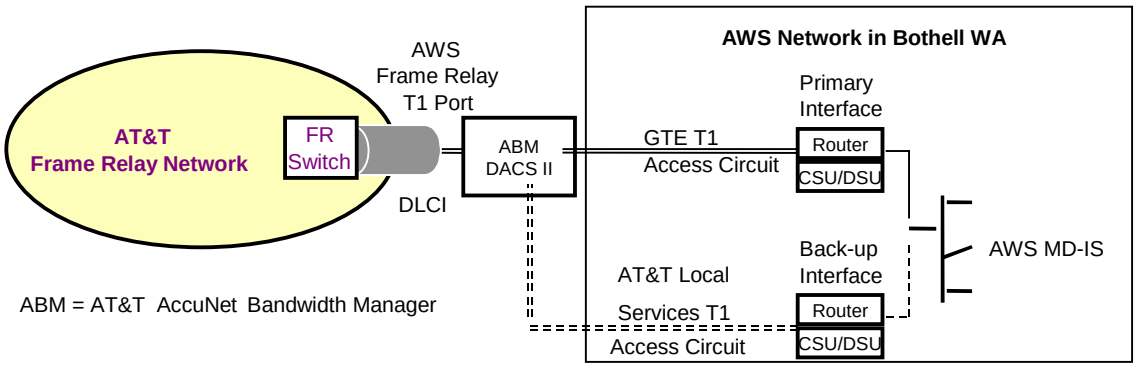
Figure 13: WCO components



9.3 Wireless IP Network Redundancy

WCO customers are protected against access failure between the AT&T Wireless IP network and the AT&T frame relay network. Figure 14 shows the redundancy built into this connection.

Figure 14: Redundancy between the AT&T Wireless IP network and the AT&T frame relay network



When the network experiences an outage on the primary T1 access circuit, within 30 minutes or less, AT&T Wireless Services will switch the traffic to the backup circuit.

9.4 Redundancy and Backup Options

The AT&T frame relay backbone network is protected against failure and has comprehensive recovery mechanisms, including automatic rerouting of PVCs by the network's internal switches. However, a customer should consider the need to implement additional measures to protect their wireless applications against access (e.g., LEC circuit) failure, major site (i.e., data center) failure or customer premises equipment (CPE) failure.

There are a variety of redundancy options available to customers. As discussed in the section on redundant connections in the main body of the white paper, it is possible for customers to connect their fixed-end systems to the AT&T Wireless IP network using two PVCs and two separate LEC circuits. Customers can work with AT&T Wireless Services to arrange for traffic to be automatically routed to the secondary PVC if the primary PVC becomes unavailable. In addition to this automatic failover capability, WCO offers two separate plans. One is called the Access Protection Plan and the other is called the Backup PVC Plan.

Since different costs and different network configurations are involved in the various types of redundancy and backup arrangements, customers will need to analyze the costs and networking requirements to decide which approach best meets their needs.

9.4.1 Access Protection Option

This option offers protection against access circuit failure and customer premises equipment (CPE) failure. The customer requires two active access circuits (private lines) and two ports in the same point of presence (POP) within the AT&T frame relay service. The customer works with AT&T Wireless Services to designate which circuit is primary and which is secondary. If a failure occurs in one of the circuits, the customer calls the network operations center (NOC) and requests reconfiguration of the ports, so that the PVC (or PVCs) is moved from the unavailable port to the available port. Note that this is a manual reconfiguration compared to the automatic scheme described in the preceding paragraph. The following figure shows an example of a network configuration before a failure, and the subsequent figure shows the reconfigured network after the failure.

Figure 15: Access Protection Option - Before Access Failure

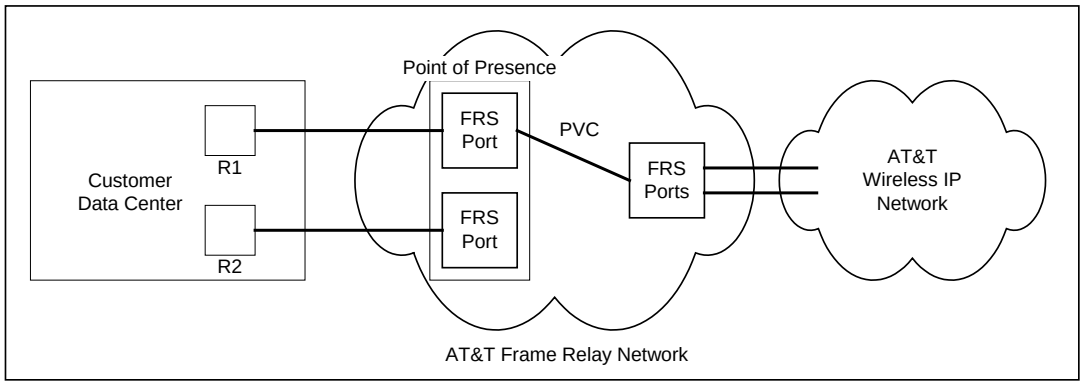
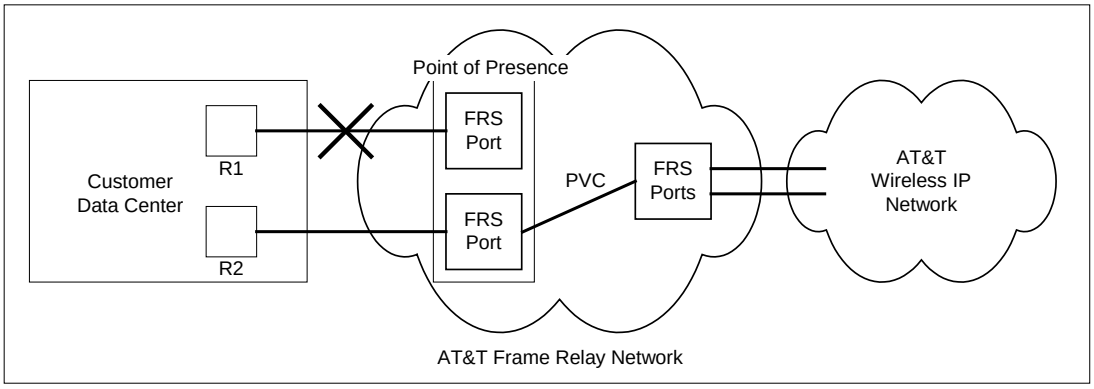


Figure 16: Access Protection Option - After Access Failure



9.4.2 Back-Up PVC Option

This option offers protection against a major failure of a customer's site, such as their data center. If a customer has a backup site, this option allows the customer's PVCs to be reconfigured to the backup site. Pre-assigned (but inactive) backup ports and access circuits are required and the customer will have predetermined primary and secondary PVC pairs that use the same Data Link Connection Identifier (DLCI). When a customer calls the NOC to report a site failure and request reconfiguration, the PVCs that were routed to the failed site are moved to their secondary site, as shown in the following figures:

Figure 17: Backup PVC - Before Site Failure

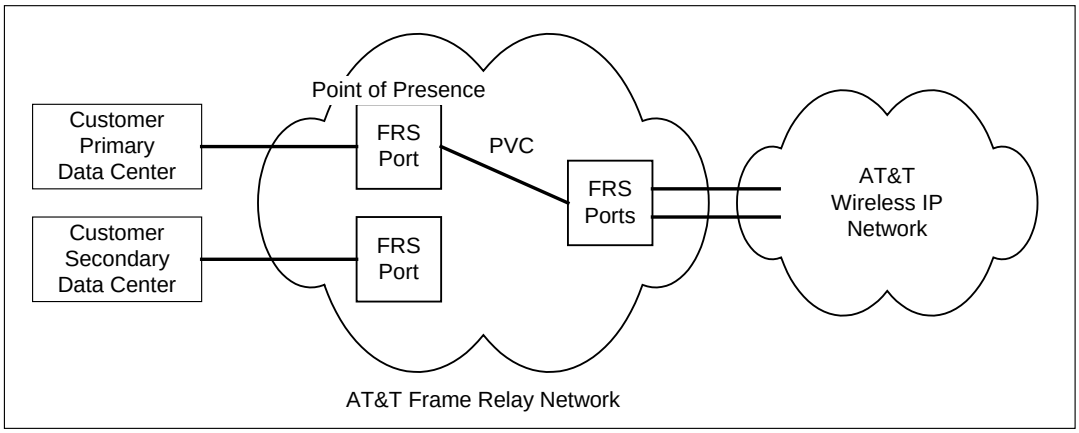
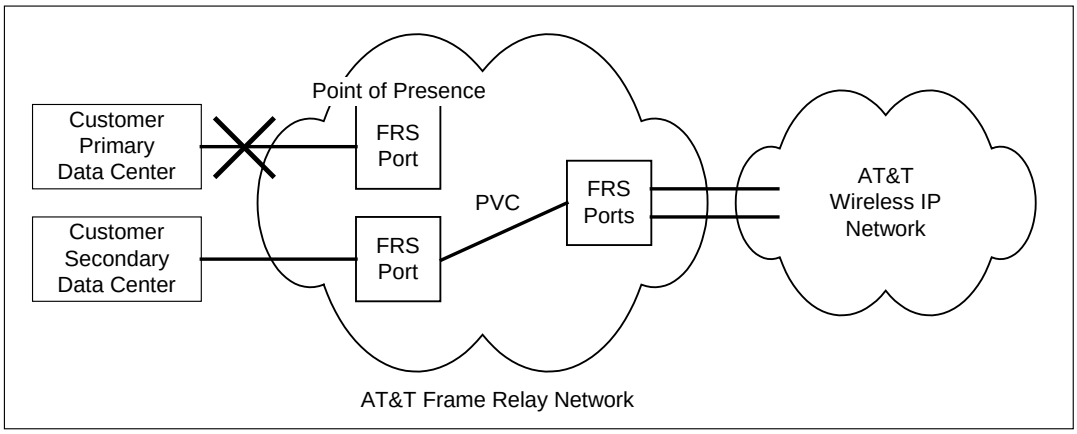


Figure 18: Backup PVC - After Site Failure



9.5 Pricing

The following table shows preliminary WCO pricing. Note that the Access Protection option and Backup PVC option will not be available until some time after WCO is launched. Please contact AT&T Wireless Services for the most recent information on service options and pricing.

Table 2 : WCO Pricing

Wireless Connectivity Option Charges	56 Kbps	128 Kbps
Monthly Recurring Charge	$449	$549
Early Termination Charge (Note 1)	$825	$1025
Access Protection Option Charges	**56 Kbps**	**128 Kbps**
Monthly Recurring Charge	$449	$549
Non Recurring Charge (Activation Fee)	$1000	$1000
Early Termination Charge (Note 1)	$1100	$1300
Back-up PVC Option Charges	**56 Kbps**	**56 Kbps**
Monthly Recurring Charge	$469	$659
Early Termination Charge (Note 1)	$975	$1175

Note: If the customer terminates their service within six months of activation, they must pay an early termination charge. The pricing for the WCO is a national flat monthly rate. The pricing provided by other frame relay service providers often depends on distance. If the customer's premises are remotely located from the nearest LEC, there could be an impact on pricing

9.6 Service Level Agreements

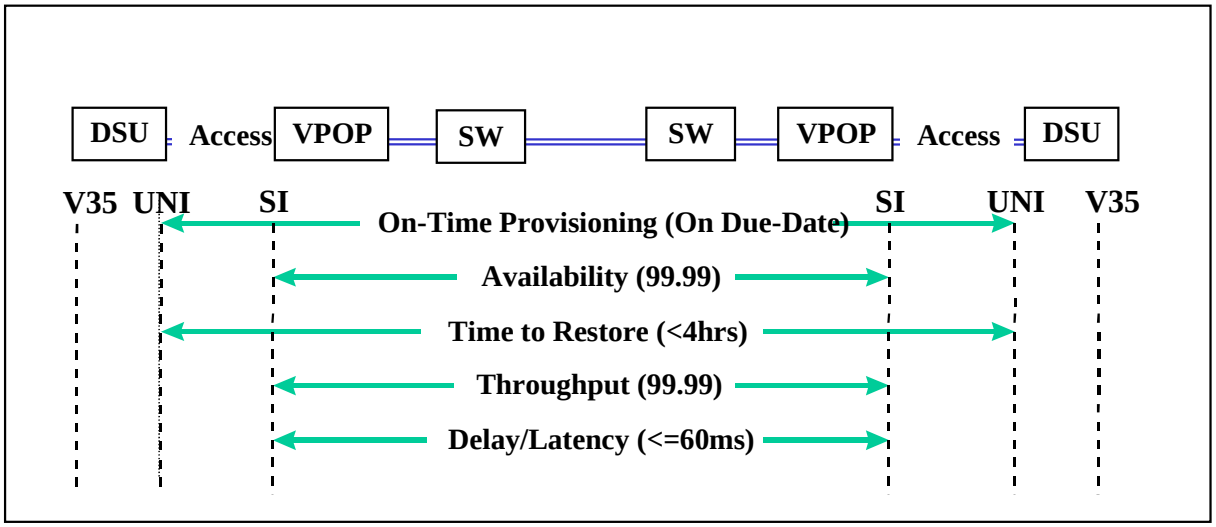
Network Service Level Agreements (NSLA) are written contractual agreements between customers and AT&T that bind AT&T to a specified level of service. AT&T will consistently meet or exceed the stated service levels, or apply a credit to the customer's service charges. The following table summarizes the service level parameters:

Table 3: AT&T Frame Relay Network Service Level Agreement

Service Level	Definition
On-Time Provisioning	All new ports and PVCs will be installed on or before the agreed due date.
Network Availability	The core frame relay network will be available 99.99% of the time.
Time To Restore	All PVC problems reported by the customer will be cleared within 4 hours.
Network Delay	95% of the time PVCs will experience less than 120 ms of round-trip delay from frame relay virtual point of presence (VPOP) to VPOP, including back-haul time.
Frame Delivery Rate	99.99% of the discard eligible (DE) = 0 packets, within the CIR, offered to the frame relay switch will be delivered. (Note: Customer cannot over-subscribe an egress port, and average frame size must be greater than or equal to 100 bytes.)

The following figure shows the part of the connection encompassed by the various SLA parameters.

Figure 19: SLA boundaries



10 Appendix C: Acronyms

ABM	**AT7T AccuNetBandwidth Manager**
AFRN	**AT&T Frame Relay Network**
AFRS	**AT&T Frame Relay Service**
ATM	**Asynchronous Transfer Mode**
AWS	**AT&T Wireless Services**
CDPD	**Cellular Digit Packet Data**
CIR	**Committed Information Rate**
CPE	**Customer Premise Equipment**
CSU/DSU	**Channel Service Unit/Data Service Unit**
DLCI	**Data Link Connection Identifiers**
DM	**DataTAC Messaging**
ES	**End System**
F-ES	**Fixed-End System**
FR	**Frame Relay**
FRS	**Frame Relay Service**
HDML	**Handheld Device Markup Language**
HDTP	**Handheld Device Transport Protocol**
IP	**Internet Protocol**
IS	**Intermediate Server**
ISP	**Internet Service Provider**
LAN	**Local Area Network**
LEC	**Local Exchange Carrier**
MDB S	**Mobile Data Base Station**
MD-IS	**Mobile Data Intermediate System**
M-ES	**Mobile End Systems**
NOC	**Network Operation Center**
NSLA	**Network Service Level Agreement**
OSI	**Open Systems Interconnect**
POP	**Point Of Presence**
PPP	**Point-to-Point Protocol**
PVC	**Permanent Virtual Circuit**
SLIP	**Serial Line Internet Protocol**
TC/IP	**Transmission Control Protocol/Internet Protocol**
VPN	**Virtual Private Network**
VPOP	**Virtual Point Of Presence**
WAN	**Wide Area Network**
WCO	**Wireless Connectivity Option**