

## 3G 有线无线备份解决方案



北京泰亚东方通信设备有限公司

## 公司介绍

北京泰亚东方通信设备有限公司成立于 1998 年，是一家以无线数据/视频传输产品研发/生产/销售、移动通信产品分销、通信网络产品销售及工程技术服务、系统集成为主营业务，可持续稳健发展的综合性高科技企业。

公司提供专业的基于无线广域网、城域网、局域网等网络的行业信息化解决方案，关注“无线自由”的用户体验，专注于 2.5G、2.75G、3G、Wifi 等网络无线数据、视频传输产品的研发和生产，为行业用户提供基于 GPRS、EDGE、CDMA、TD-SCDMA、WCDMA、CDMA2000、MESH-WIFI、WIMAX 等无线技术接入的解决方案。

2003 年泰亚东方被广发银行认定为重点扶持 100 家企业之一。此外，政府主管部门也给予了泰亚东方高度的评价，2000 年至 2008 年连续九年获得“海淀区先进企业”称号。

长期以来，泰亚东方秉承“科技为本、应用为先、服务为众”的企业理念和“团结、勤奋、谦虚、创新”的企业精神，致力于为用户提供最优质的产品和服务。

## 目录

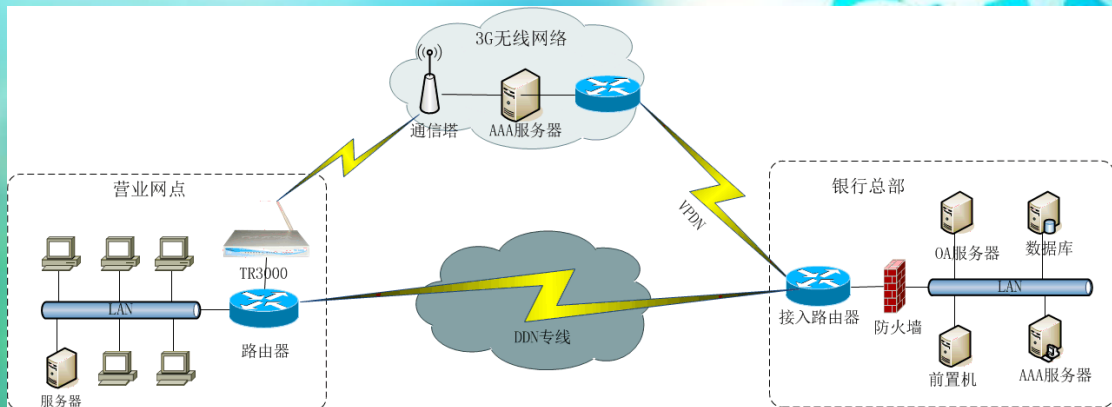
一、概述.....	4
二、某银行无线接入营业网点应用案例.....	5
三、3G传输方式的优势.....	5
四、3G无线接入的安全性.....	7
1、3G无线接入的工作流程: .....	7
2、安全性保障.....	7
五、3G无线路由器TR3000 相关技术参数.....	11
六、相关设备及价格.....	14

## 一、概述

在大的行业单位或者大型连锁企业的日常业务中，各分支机构业务系统需要与总部的数据中心进行实时的数据交换。目前，大部分的联网方式是采用DDN专线或者ADSL VPN的方式，这会造成通信成本高，同时，也因为采用单一专线方式，如果专线出现故障，将造成业务中断，业务无法正常开展，需要一定的时间恢复，在线路维修过程中，正常的业务无法开展，造成不良影响。虽然有些单位也有采用备份的线路，但是都是采用同一个运营商的同一条通信路由，只不过是通过同一条接入线路接入到不同的通信业务网络，如果是接入的部分发生中断，如光纤被挖断了，这样恢复起来时间长，而且会造成所有的通信业务中断，则备份的线路起不到备份的作用。对于选择备份线路一般是优先选择不同的运营商，在无法选择不同运营商的时候是考虑选择不同的接入路由。

随着3G业务的推出，3G以其高速、无需布线的优点，逐渐成为了有线网络的一个不可缺少的补充，特别是在应急和线路备份方面，将起到一个非常重要的作用。为此，我司推出基于3G无线路由器的有线无线备份解决方案。

## 二、某银行无线接入营业网点应用案例



在营业网点和银行总部间租用一条运营商的 DDN 专线，我司的 TR3000 无线路由器通过运营商的 3G 网络搭建起基于 vpdn 的 ipsec 隧道连接到银行总部。

DDN 专线作为这个网络的主线路，3G 网络作为备份线路。

在路由器上添加两条默认路由，一条是走主线路的默认路由，一条是走备份线路的默认路由，走备份线路的默认路由的管理距离比主线路的管理距离大。

当路由器检测到主线路不可达时，数据会自动切换到 3G 无线备份线路上来，从而确保了营业网点与银行总部的能正常通信。

## 三、3G 传输方式的优势

3G 是英文 3rd Generation 的缩写，指第三代移动通信技术。相对第一代模拟制式手机（1G）和第二代 GSM、TDMA 等数字手机（2G），第三代手机一般地讲，是指将无线通

信与国际互联网等多媒体通信结合的新一代移动通信系统。它能够处理图像、音乐、视频流等多种媒体形式，提供包括网页浏览、电话会议、电子商务等多种信息服务。为了提供这种服务，无线网络必须能够支持不同的数据传输速度，也就是说在室内、室外和行车的环境中能够分别支持至少 2Mbps（兆比特 / 每秒）、384kbps（千比特 / 每秒）以及 144kbps 的传输速度。

在银行联网业务方面，以前经常采用单一专线 DDN 方式连接到地区银行结算中心，现在则可以使用 3G 无线数据网络构建的 VPDN 安全隧道作为备份链路进行数据结算。相对于 DDN 等接入方式，具有以下优势：

- 1) 3G 用户可随意分布和移动自己的网点，无需担心线路的维护或有线在移机时导致的通讯中断。建设新的营业厅无需进行拉线、埋线等工作。较光纤或专线系统投资较少，设备安装方便。
- 2) 终端价格比较低。
- 3) 3G 资费便宜，计费合理。
- 4) 3G 能最好地支持频繁的、少量突发型数据业务。通信质量稳定可靠，永不掉线。
- 5) 3G 网络相对比普通专线带宽更高，接入速度快，提供了与现有数据网的无缝连接，过去专线完成的任务，3G 也完全可以实现。
- 6) 数据集中，易于管理。
- 7) 覆盖好，运营商投入大，三大运营商 3 种 3G 网络，可视现场情况任意选择。

相对于 2G 等接入方式,具有以下优势,3G 与 2G 相比主要的优势在于频谱利用更高,可以提供更高的数据速率,目前速率可以达到 7.2Mb/s (联通 WCDMA),未来的技术速率会更高。3G 能提供的服务,现在互联网都能提供,而且性价比更高。3G 的优势在于在移动中仍可以获得数据业务,消费者可以随时、随地的接入互联网。

## 四、3G 无线接入的安全性

### 1、3G 无线接入的工作流程:

在运营商完成网络侧配置后,银行网点通过无线设备接入 3G 网络后,3G 分组接入设备 PDSN 上通过 L2TP 隧道路由连到银行系统中心内的 LNS 路由器上,中间经过运营商骨干网和专线。整个隧道的开启和通过均在运营商网络内部,作为大型的网络运营商,有严格的安全管理和保护措施,确保网内的数据安全可靠,具有很高的安全性保障,而且不存在互连互通瓶颈,可以有效保证用户使用性能。

### 2、安全性保障

3G 在设计就考虑到安全性私密性,比 2G 更安全。用户端到无线网络接入设备间的无线空中通道目前不可能被破解;无线分组设备到用户终端设备间,采用隧道穿过专线接入,可以有效保证整个系统的安全。要保护整体系统的安全,首先要保证网络本身的安全。必须尽可能地屏蔽外部非法访问及非法数据,对从外部网络连入的终端进行严格的用户认证及控制。针对 3G 网络的各环节,我们分别分析其安全性,并提供 5 级业务安全保障,从而充分保证网络中数据的安全。

#### 1) 第一级安全保障:3G 网络本身的安全性

3G 网络系统 in 安全保密方面具有很大优势。快速功率切换让 3G 信号很难锁定。需要破解用户信息编码。窃听器很难破译出 3G 无线的编码。所以 3G 无线技术本身就很安全。

## 2) 第二级安全保障：3G 网络侧的 AAA 认证

AAA 是指认证 (Authentication)、授权 (Authorization)、计费 (Accounting) 三个过程，其中：

认证是，用户在使用网络系统中的资源时对用户身份的确认。这一过程，通过与用户的交互获得身份信息（像用户名—口令、生物特征信息等），然后提交给认证服务器；认证服务器对身份信息与存储在数据库里的用户信息进行核对处理，然后根据处理结果确认用户身份是否正确。

授权是，网络系统授权用户以特定的权限使用其资源，这一过程指定了被认证的用户在接入网络后能够使用的业务和拥有的权限，如授予 IP 地址，准许访问时间等。

计费是，网络系统收集、记录用户对网络资源的使用信息，以便向用户收取资源使用费。以互联网业务提供商 ISP 为例，用户的网络接入使用情况可以按流量或者时间准确地记录下来。

认证、授权和计费一起实现了网络系统对特定用户的网络资源使用情况的准确记录。这样既在一定程度上有效地保障了合法用户的权益，又能有效地保障网络系统安全可靠地运行。

移动通信从电路交换，发展到 CDMA 1X 分组网络，再到第三代移动通信网络，用于认证、授权和计费的协议也在随之演进，从基于 7 号信令的协议，到部分采用 RADIUS，再发展到 Diameter，这主要是由越来越丰富的业务决定的。Diameter 协议由 IETF 的 AAA 工作组在 2002 年 3 月提出的认证计费协议草案。Diameter 协议支持移动 IP、NAS 请求和移动代理的认证、授权和计费工作。协议的实现和 RADIUS 类似，也是采用 Attribute-Length-Value 三元组来实现，但是其中详细规定了错误处理等内容。它在设计过程中，不仅保持了与广为使用的 RADIUS 协议的兼容，更克服了 RADIUS 协议的许多不足，而且它不仅仅被互联网采用，更被下一代移动通信网（3G）采用。在第三代移动通信网络和业务开展初期，为了和已有的设备和传统业务互通，需要采用 Diameter 与 RADIUS 之间的协议转换器，但是最终还是统一使用 AAA Diameter 协议。

### 3) 第三级安全保障：3G 网络 and 用户网络之间的 VPN 链接

3G 网络 and 用户网络之间可以采用专线链接，也可以使用 Internet 链接。使用 Internet 链接必须考虑安全性，因此，可以使用 VPN 将二者利用 Internet 链接起来。

VPN 技术非常复杂，涉及到通信技术、密码技术和现代认证技术。主要包含两种技术：隧道技术与安全技术。

隧道技术的基本过程是在源局域网与公网接口处将数据封装在一种可以在公网上传输的数据格式中，在目的局域网与公网的接口处将数据解封装，被封装的数据包在互联网上传播时的所经过的路径被称为“隧道”。常用的隧道协议有：1. 点到点隧道协议—PPTP（现已基本淘汰）； 2. 第二层隧道协议—L2TP，该协议是国际标准隧道协议，具有 PPTP 协议以及第二层转发协议（L2F）的优点，可以使 PPP 包以隧道方式通过各种网络，包括 ATM、SONET、帧中继。但没有任何加密措施；3. IPSec 协议，该协议是一个范围广泛、开放的 VPN 安全协议，工作在网络层。它提供所有在网络层上的数据保护和透明的安全通信。可以在两种模式下运行：一种是隧道模式，一种是传输模式。在隧道模式下 IPSec 把 IPv4 数据包封装在安全的 IP 帧中；传输模式是为了保护端到端的安全性，不会隐藏路由信息。目前一种趋势是将 L2TP 和 IPSec 结合起来：用 L2TP 作为隧道协议，用 IPSec 协议保护数据。市场上大部分 VPN 采用这类技术。4. SOCKS v5 协议，SOCKS v5 工作在 OSI 模型中的第五层——会话层，可作为建立高度安全的 VPN 的基础。SOCKS v5 协议的优势在访问控制，因此适用于安全性较高的 VPN，SOCKS v5 现在被 IETF 建议作为 VPN 的标准。

VPN 是在不安全的 Internet 上传输的，传输内容可能涉及到企业的机密数据，因此安全性非常重要。VPN 中的安全技术通常由加密、认证及密钥交换与管理组成。主要有认证技术，加密技术，密钥管理与交换技术。

### 4) 第四级安全保障：用户网络侧的安全防火墙（FW）

防火墙技术是目前用来实现网络安全措施的一种主要手段，主要是用来拒绝非法用户的访问，阻止非法用户存取敏感数据，同时允许合法用户顺利访问网络资源。防火墙

实际上是一种访问控制技术，在某个机构的内部网络和不安全网络之间设置障碍，阻止对信息资源的非法访问，也可以使用防火墙阻止保密信息从受保护网络上的非法输出。

实现防火墙的主要技术有：数据包过滤，应用网关和代理服务等。包过滤（Packet Filter）技术是在网络层中对数据包实施有选择的通过。依据系统内事先设定的过滤逻辑，检查数据流中每个数据包后，根据数据包的源地址、目的地址、TCP/UDP 源端口号、TCP/UDP 目的端口号及数据包头中的各种标志位等因素来确定是否允许数据包通过，其核心是安全策略即过滤算法的设计。应用网关（Application Gateway）技术是建立在网络应用层上的协议过滤，它针对特别的网络应用服务协议即数据过滤协议，并且能够对数据包分析并形成相关的报告。应用网关可以严格控制某些易于登录和控制的所有的输出输入通信环境，以防有价值的程序和数据被窃取。它的另一个功能是对通过的信息进行记录，如什么样的用户在什么时间连接了什么站点。在实际工作中，应用网关一般使用专用工作站系统。代理服务器（Proxy Server）作用在应用层，用来提供应用层服务的控制，起到内部网络向外部网络申请服务时中间转接作用。内部网络只接受代理提出的服务请求，拒绝外部网络其它节点的直接请求。

用户网络可以选用适合于本单位的防火墙产品来保证自己网络数据的安全。

#### 5) 第五级安全保障：金融企业网络侧的 AAA 鉴权认证

用户网络侧的 AAA 鉴权认证可以实现对 VPDN 成员的身份认证。与第二级的安全保障不同，本级的 AAA 服务器将鉴别 VPDN 成员的用户名和密码的正确性。

VPDN 中成员的用户名和密码等资料将保存在用户专网侧的 AAA 服务器，具有很好的安全性和管理的灵活性。

## 五、3G无线路由器TR3000 相关技术参数

设备外观（如下图）



TR3000 前面板示意图

基本参数	外观	重量	~400g		
		尺寸(mm)	190×117×26, 110×86×26(mini 版)		
		颜色	白色		
	工作条件	工作环境温度	-20℃~60℃		
		工作环境湿度	≤95%		
		电源输入	DC12V/1A		
硬件参数	基本参数	功耗	≤3.6W		
		处理器	MIPS32 24KEc	主频 320MHz	
		FLASH	8MB NOR		
		SDRAM	32MB		
		以太网接口 (RJ45)	10/100M 直连交叉自适应	1 个 WAN 口	1 或 4 个 LAN 口
		支持 WiFi 组网	支持 150M/300M 传输		
		USB 接口 (A 型)	HOST/SLAVE	1 个	
		CONSOLE 口	RJ11 专用串口配置口	1 个	
		电源接口	Φ 2.1 插座	1 个	
		天线接口	SMA 阴头	2 个	
其他	其他	SIM 卡接口	抽屉式	1 个	
		恢复出厂按钮			
		状态指示灯	电源指示灯	1 个	
			网络指示灯	6 个	
软件参数	配置方式	状态指示灯	5 个		
		WEB 浏览器配置			
		TELNET 配置			
		本地串口配置			
		远端网管软件配置			

基本功能	WEB 远程升级	通过 WEB 页面进行软件升级	
	日志功能	系统自动记录运行状态,应用程序日志与系统分开,并可实时上传至远端日志服务器	
	运行状态指示	LED 显示运行状态(信号强度,在线灯)	
	路由管理功能	支持静态路由,可添加多条路由表项	
	网络时钟同步		
	复位功能	通过外部复位键或软件复位恢复出厂设置	
	配置导入导出功能		
	断线检测,自动修复技术	链路及网络故障时,按照预定策略重新拨号	
	多级链路检测技术	LCP 链路检测	
		PPP 心跳检测	
		ICMP 心跳检测机制	
	支持网管软件	支持 SNMP 协议或定制协议网管软件	
	支持 DTU 功能	串口转以太网协议	
	网络状态监测	采用 WEB 界面方式,使用者对设备连接网络状态、VPN 状态及网络服务信号质量等进行监测管理	
防火墙	可设置多条防火墙过滤规则,可过滤指定的 IP 或端口		
网络功能	接入方式	TD-SCDMA/HSDPA、CDMA2000-1X/EVDO、WCDMA/HSDPA 三种制式 3G 接入; PPPoE 支持 xDSL/Cable MODEM, 小区宽带固定 IP, 小区宽带动态 IP 接入。	
	组网模式	Bridge、Gateway、Ethernet Converter、AP Client 四种组网模式	
	网络协议	IEEE 802.11b/g/n, IEEE 802.3, IEEE 802.3u, IEEE 802.3x, CSMA/CA, CSMA/CD, TCP/IP, DHCP, ICMP, NAT, PPPoE	
	认证方式	PAP/CHAP/MS-CHAP	
	动态域名绑定	用户的动态 IP 地址映射到一个固定的域名解析服务上,将动态 IP 绑定固定域名服务,支持 qdns、ezip、pgpow、dhs、dyndns、dyndns-static、tzo、easyns、justlinux、dysn、hn、zoneedit	
	NAT 功能	DNAT/SNAT/静态 NAT	
	流量管理技术	监测制定网卡的流量状况	
	DHCP 服务		
	MAC 地址绑定		
	DMZ		
	端口映射		
	多 IP 设置	可设置多个本机 IP 设置,且这些 IP 均可以作为网关(交换机功能)	

	链路备份	
	PPPOE 客户端	
WiFi 功能*	支持 802.11b/g/n	
	150M/300M 传输速度	
	WMM Wi-Fi 多媒体	
	WPA、WPA2、WPA/WPA2 混合等多种加密与安全机制	
	WPS 一键加密功能	
	WDS 无线分布式系统	
	Roaming 无线漫游技术	
	隐藏无线 SSID 功能和基于 MAC 地址的访问控制(多达 30 组)	
VPN 功能	PPTP	PPTP 服务器
		PPTP 客户端
	L2TP	LNS
		LAC
	IPSec	IPSec 服务器
		IPSec 客户端
		IKE 自动密钥管理
		支持 AH 和 ESP
		PFS Group 1,Group 2,Group 5
		NATT
		DPD
		支持 AES/128、3DES/168 和第三方算法
		支持 MD5-HMAC、SHA1-HMAC
		和 Cisco、Netscreen、华为、首信、华堂、linksys、NESCO 等其它 VPN 产品互通
定制功能	短信报警	
	呼叫激活	
	MPPC/MPPE	
	GPS 定位	

## 六、相关设备及价格

设备名称	规格型号	数量	价格
cisco 路由器	Cisco2811 路由器 (支持 L2TP、IPSEC)		
AAA 服务器	泰亚 AAA 硬件服务器		
无线数据上网卡	WCDMA/CDMA-2000/TD-SCDMA		
网管软件	泰亚无线设备管理软件		
无线传输设备	TR3000		