文章编号:1005-8451(2005)02-0051-03

# 开放环境下铁路信息网接入技术及其安全策略

温成钢
(乌鲁木齐铁路局 电算中心,乌鲁木齐 830011)

**摘 要**:从网络的安全性、建设新型和扩充性等多个方面分析比较了当前流行的和成熟的接入网技术及网络安全防范技术,并结合铁路系统自身的特点,提出了铁路信息网应该采用的方案。

**关键词**:铁路;接入网;网络安全;开放环境
**中图分类号**:TP39 **文献标识码**:B

## Cut-over technology and security policy of railway information network in open environment

WEN Cheng-gang
(Computer Center of Urumqi Railway Administration, Urumqi 830011, China)

**Abstract:** It was analyzed and compared comprehensively current primary technology of INTERNET access network and network security from the aspects of safety, developments, expenses, enlargement etc. Finally, it was introduced a project according to railroad system's characteristics.

**Key words:** railway ; access network; network security; open environment

为了适应客户和企业自身发展的需要,铁路系统的客、货运输以及其它与旅客、货主有关的信息需要通过多种便利的渠道和社会信息相连,Internet 将是其中重要方式之一。目前铁路系统为了安全,内部网和 Internet 是隔断的。企业内部网一旦接入 Internet 就存在一个采用何种技术接入以及解决面临的网络安全问题。

## 1 接入网技术

### 1.1 接入网的概念

接入网是由业务节点接口和用户网络接口之间一系列传送设备组成,接入网是介于本地交换机和用户之间,主要完成用户接入到核心网的任务。

### 1.2 宽带接入网的分类及比较

#### 1.2.1 宽带接入网的分类

鉴于铁路系统的信息量大、时效性强等特点,需要宽带接入技术才可以满足需求。Internet 宽带接入技术可以分为 4 大类:

(1)以太网接入技术;
(2)基于传统电信网的有线接入;
(3)基于有线电视网络(HFC)的接入技术;
(4)光纤接入技术。其中,光纤接入是未来有线接入网技术的发展趋势。

#### 1.2.2 以太网

以太网接入技术具有强大的网管功能,能进行配置管理、性能管理、故障管理和安全管理,还可以向计费系统提供丰富的计费信息,使计费系统能够按信息量、连接时间长短或包月制等方式计费。

在局域网中 IP 协议都是运行在以太网上,即 IP 包直接封装在以太网帧中,以太网协议是目前与 IP 网配合最好的协议之一。以太网接入手段已成为宽带接入的新潮流,它拥有的带宽是其它方式的几倍或者几十倍。完全能满足用户对宽带接入的需要。主要优点是:技术简单、投资成本较低、扩展性好、可以共享资源、技术成熟且应用领域广泛。其缺点则是:由于以太网技术原本是为局域网络而开发的技术,把它用于公用接入运营网络,将存在相对较为严重的安全问题。

#### 1.2.3 ADSL接入技术

ADSL 的全称是非对称数字用户线系统,它是充分利用现有电话网络的双绞线资源,实现高速、高带宽数据接入的一种技术。ADSL 是 xDSL 的一种非对称版本,其它的 xDSL 版本应用远远不如 ADSL

收稿日期:2004-05-20
作者简介:温成钢,工程师。

广泛，此处不作讨论。）它采用FDM（频分复用）技术和DMT（离散音频）调制技术，在保证不影响正常电话使用的前提下，利用原有的电话双绞线进行高速数据传输。

ADSL接入技术的优势在于：ADSL接入可以利用现有的市内电话网和电话交换局的机房，可以降低施工和维护成本，对电话业务没有影响。而其缺点则是：它对线路质量要求较高，传输距离较短（3 km~6 km）。并且带宽有限，难以满足很高信息量的传输，另外扩展也比较困难。

#### 1.2.4 基于HFC网的电缆调制

Cable Modem（电缆调制）的通信和普通Modem一样，是数据信号在模拟信道上交互传输的过程，但也存在差异，普通Modem的传输介质在用户与访问服务器之间是独立的，即用户独享传输介质，而Cable Modem的传输介质是HFC网，将数据信号调制到某个传输带宽与有线电视信号共享介质；另外，Cable Modem的结构较普通Modem复杂，它由调制解调器、调谐器、加/解密模块、桥接器、网络接口卡和以太网集线器等组成。

用电缆调制解调器在HFC网上架构宽带接入网的优点是，可利用已经有的HFC网，只需要对同轴电缆网进行双向改造及可以使用有线电视台机房等。缺点是需要进行HFC网的双向改造，工程施工和系统调试较为复杂，不可预见因素多。此外还需要投资建立一个维护队伍以保障网络的正常运行。另外带宽进一步扩展能力有限，而且无法建设独立的社区内部网络平台。

#### 1.2.5 光纤接入技术

根据光网络单元的位置，光纤的接入方式可分为如下几种：FTTR（光纤到远端接点）；FTTB（光纤到大楼）；FTTC（光纤到路边）；FTTZ（光纤到小区）；FTTH（光纤到用户）。光网络单元具有光/电转换、用户信息分接和复接、以及向用户终端馈电和信令转换等功能。当用户终端为模拟终端时，光网络单元与用户终端之间还有数模和模数的转换器。

光纤接入技术与其他接入技术（如铜双绞线、同轴电缆、五类线、无线等）相比，最大优势在于可用带宽大，而且巨大潜力可以挖掘，还具有传输质量好、传输距离长、抗干扰能力强、网络可靠性高、保密性好和节约管道资源等特点。另外，SDH（同步光网络）和APON（无光源网络）设备的标准化程度都比较高，有利于降低生产和运行维护成本。

当然，与其他接入技术相比，光纤接入网最大的问题是成本比较高。

## 2 网络安全方案

### 2.1 设计原则

系统必须具有先进性、完整性、稳定性、灵活性、开放性和可扩充性。

（1）先进性要求安全方案中采用的技术具有良好的性能，能防范最新的安全攻击手段，并不容易被新的入侵攻克。

（2）完整性要求安全方案能够涵盖主机、网络、应用和管理等各方面，不能留有安全死角，同时整个方案又是一个个安全单元组成的有机整体。

（3）稳定性要求安全系统运行可靠，不能由于安全系统的加入造成系统故障率上升、资源开销大增、运行不稳定。

（4）灵活性要求安全系统既是一个完整的整体，各个部分又相对独立，能够灵活配置，能够根据具体的安全要求对系统组成进行增减。

（5）开放性要求安全系统建立在开放的系统平台上，包括操作系统平台、数据库平台等开放系统，方案能够在最大程度上兼容目前的系统，同时开放性也要求方案能够使用多种安全产品。

（6）可扩充性要求安全系统采用的安全产品能够随着安全形势的发展而不断升级，以确保用户对安全的投资得到最大限度的保护，发挥尽可能大的作用。

### 2.2 网络安全技术

#### 2.2.1 防病毒技术

从目前情况看信息系统安全的主要问题之一就是病毒问题。现在防病毒技术的发展趋势是以防为主、预警为辅，越来越重视对隐患和漏洞的预先防范。

#### 2.2.2 防火墙技术

防火墙技术是网络安全的重要技术手段，其主要作用是在网络入口点检查网络通讯，根据用户设定的安全规则，有条件地提供内外网络通讯。防火墙系统通常不能提供实时的入侵检测能力和防范内部攻击，仅仅使用防火墙系统，网络安全还远远不够。

#### 2.2.3 入侵检测技术

入侵检测技术是一种新型网络安全技术，目的

是提供实时的入侵检测及采取相应的防护手段，它可以记录证据，用于跟踪和恢复、紧急时断开网络连接等。它能够作为防火墙系统的补充，对付来自网络内部的攻击，它能够大大缩短“黑客”可利用的入侵时间。

### 2.2.4　安全扫描技术

安全扫描技术是网络安全中的另一类重要技术，它不是被动的防护网络安全。而是主动地查找网络系统的漏洞。这项技术源于“黑客”在入侵网络系统时采用的工具，它抓住系统漏洞是系统被攻击的主要原因这一点，及时查找漏洞、拒绝攻击者的外部或内部攻击。配备安全扫描系统，通过范围宽广的穿透测试检测潜在的网络漏洞，评估系统安全配置，以提前主动地控制安全危险，对潜在危险发出预警。

### 2.2.5　虚拟专用网技术

虚拟专用网（VPN）技术用于通过 Internet 或其他公用网络来组建自己的安全专用网络，通过带有 VPN 功能的路由器、专用硬件 VPN 设备或软件 VPN 系统来实现。虚拟专用网是采用加密和认证技术在公共网络上建立安全专用隧道的网络。严格地说，VPN 是一种仿真的专用网络连接，是一种在公共网络连接基础上建立的专用逻辑连接。这主要是通过对数据通信进行加密来实现的。大致可分为 3 种类型：远程用户接入、远程网络互连、Intranet 网络内部的安全。

### 2.3　系统设计

（1）硬件的安全

要考虑网络本身的硬件、设施的安全。机房环境应符合有关规定。

（2）要有完整科学的安全管理制度

安全方面既要考虑软、硬件的因素，又要考虑人的因素及管理的因素。

## 3　方案讨论

对于接入方式，根据铁路系统信息流量大，时效性高等特点，铁路信息主干网络的接入方式应以光纤为主，包括铁道部到铁路局、铁路局到铁路分局、铁路分局到主要的车站。各个子网（可能是车站或段）的接入可以根据需要，选择不同的接入方式。

对于网络安全，从目前的情况看，病毒对网络的运行影响较大，对此应安装服务器 / 客户端模式的防病毒软件，做到每一台服务器，每一工作站都有防病毒软件的保护。要及时对病毒库进行更新，以防范新的病毒。

从长远来看，铁路内网和外网连接，应严格控制接入点，在接入点应综合使用各种网络安全技术，确保铁路内网的安全。为此，铁路内网也要早做统一规划，生产网、办公网、公共信息发布网应在网络层分开，通过配置防火墙阻断未经授权的通信进出被保护的网络，对于安全级别要求不太高的场合可以采用软件防火墙，软件防火墙安装简便，费用低，易维护。而对安全级别要求高的铁路局、铁路分局和其他重要网络，要求采用硬件防火墙，以增强安全性。铁路局级全网应配置网络型入侵检测系统，设立专用的服务器用来对全网进行实时的检测，以确保网络免受来自网外的攻击和非法访问。

铁路局或铁路分局和外围单位或重要的客户之间远程连接应采用虚拟专用网技术，并对使用人进行电子身份认证。这样，能够保证重要数据传输的保密性，保证特定客户服务的安全性。

## 4　结束语

铁路新希望的接入要考虑到铁路信息网和现有网络资源的实际情况，综合各种技术将现有的各种资源整合在一起，应确保统一规划、统一管理。在做信息网络安全方案时，应考虑侵入破坏的机会和危害的潜在代价，同时还要考虑用户使用的方便程度、管理的复杂性、对现有系统的影响、对不同平台的支持等。网络安全方案最终应是折衷了危害和降低危害的代价的一种策略，做到以小的安全代价换取高的安全强度。

### 参考文献：

[1] 林得敬，林柏钢．INTERNET 接入网综合分析 [J]．通信技术 2002（8）

[2] 杨亦斌，杨　毅．区域性网络安全总体方案设计 [J]．信息安全与通信保密，2003（3）

[3] 钟小平．网络拓展与管理—从内部网到外部网[M]．北京：人民邮电出版社，2002，12．

[4] 张耀江．聚焦黑客—攻击手段与防护策略[M]．北京人民邮电出版社，2002，9．

[5] 蔡立军．计算机网络安全技术[M]．北京：中国水利水电出版社，2002，1．