

YD

中华人民共和国通信行业标准

YD/T 1148—2001

网络接入服务器(NAS)技术要求 ——宽带网络接入服务器

Technical Requirements of Network Access Server(NAS)
——Broadband Network Access Server

2001-09-03 发布

2001-11-01 实施

中华人民共和国信息产业部 发布

目 次

前 言 II

1 范围 1

2 引用标准 1

3 定义 2

4 缩略语 2

5 设备功能 3

6 通信接口 6

7 通信流程 7

8 IP 地址管理和分配流程 8

9 协议要求 9

10 性能和技术指标 30

11 环境要求 31

12 电源与接地 33

13 例行试验 33

前 言

本标准 of 宽带网络接入服务器设备标准。本标准参考国外同类产品标准，根据国际相关标准，结合国内网络的实际情况制定。本标准是宽带网络接入服务器设备研制、开发和生产的依据。

本标准由中华人民共和国信息产业部电信研究院提出并归口。

本标准起草单位：上海贝尔有限公司
信息产业部电信传输研究所
深圳市中兴通讯股份有限公司
华为技术有限公司
西安大唐电信股份有限公司

本标准主要起草人：于洪斌 许 飞 顾方方 江 华 胡海涛 徐 晖

中华人民共和国通信行业标准

网络接入服务器(NAS)技术要求 ——宽带网络接入服务器

Technical Requirements of Network Access Server (NAS)
—— Broadband Network Access Server

YD/T 1148—2001

1 范围

本标准规定了宽带网络接入服务器的接口功能、协议要求、通信流程、业务流程、性能及技术指标等基本要求。

本标准适用于宽带网络接入服务器的研制、生产和引进。

2 引用标准

下列标准所包含的条文，通过在本标准中引用而成为本标准的条文。本标准出版时，所示版本均为有效。所有标准都会被修订，使用本标准的各方应探讨使用下列标准最新版本的可能性。

GB 191-2000	包装储运图示标志
GB/T 2423.1-1989	电工电子产品基本环境试验规程 试验 A: 低温试验方法
GB/T 2423.2-1989	电工电子产品基本环境试验规程 试验 B: 高温试验方法
GB/T 2423.9-1989	电工电子产品基本环境试验规程 试验 Cb: 设备用恒定湿热试验方法
GB/T 3873-1983	通信设备产品包装通用技术条件
GB/T 4798.3-1990	电工电子产品应用环境条件 有气候防护场所固定使用
YD/T 1045-2000	网络接入服务器(NAS)技术规范
YD/T 1097-2001	路由器设备技术规范——高端路由器
YDN 099-1998	SDH 技术体制
RFC0768 (1990)	UDP 协议
RFC0791 (1990)	IP 协议
RFC0792 (1990)	ICMP 协议
RFC0793 (1990)	TCP 协议
RFC0854 (1990)	Telnet 协议
RFC0855 (1990)	Telnet 协议选项规范
RFC0858 (1990)	Telnet 抑制前进选项
RFC0894 (1990)	在以太网上传输 IP 数据包的标准
RFC1144 (1992)	低速串行链路上的 TCP/IP 头的压缩算法 (SLHC 协议)
RFC1155 (1990)	基于 TCP/IP 的互连网管理信息的结构和标识
RFC1157 (1990)	简单网络管理协议 (SNMP)
RFC1213 (1991)	基于 TCP/IP 的互连网的网络管理信息库: MIB-II
RFC1321 (1992)	MD5 算法
RFC1332 (1992)	IPCP 协议

RFC1334 (1992)	PAP 协议
RFC1631 (1994)	IP 网络地址转换器 (NAT)
RFC1661 (1994)	PPP 协议
RFC1990 (1996)	PPP 多链协议
RFC1994 (1996)	CHAP 协议
RFC1662 (1994)	在类 HDLC 帧中的 PPP 协议
RFC2364 (1998)	PPP over AAL5
RFC2516 (1999)	传输 PPPoE 之方法
RFC1973 (1996)	PPP in Frame Relay
RFC 2615 (1999)	PPP over SONET/SDH 协议
RFC 1483 (1993)	AAL5 上的多协议封装
RFC 1490 (1993)	FRAME RELAY 上的多协议封装
RFC 2138 (1997)	RADIUS 协议
RFC 2139 (1997)	RADIUS 计费协议
RFC1994 (1996)	网络互连设备的性能测试方法
RFC 2661 (1999)	L2TP 协议
RFC 2453 (1998)	RIP v2 协议
RFC 2328 (1998)	OSPF v2 协议

3 定义

本标准应用了下列定义:

1) 网络接入服务器 (NAS)

网络接入服务器 (Network Access Server, NAS) 是远程访问接入设备, 它位于公共电话网 (PSTN/ISDN) 与 IP 网之间, 将拨号用户接入 IP 网, 它可以完成远程接入、实现拨号虚拟专网 (VPDN)、构建企业内部 Intranet 等网络应用。

2) 宽带网络接入服务器 (BNAS)

宽带网络接入服务器 (Broadband Network Access Server, BNAS) 是面向宽带网络应用的新型接入网关, 它位于骨干网的边缘层。其可以完成用户宽带的 (或高速的) IP/ATM 网的数据接入 (目前接入手段主要基于 xDSL/Cable Modem/高速以太网技术/无线宽带数据接入等)、实现 VPN 服务、构建企业内部 Intranet、支持 ISP 向用户批发业务等应用。

4 缩略语

ADSL	Asymmetric Digital Subscriber Line	非对称数字用户线
ATM	Asynchronous Transfer Mode	异步传递模式
BGP	Boulder Gateway Protocol	边界网关协议
CMTS	Cable Modem Termination Systems	
DDN	Digital Data Network	数字数据网
FR	Frame Relay	帧中继
IPSEC	IP Security Protocol	网络安全协议
ISDN	Integrated Service Digital Network	综合业务数字网
LAN	Local Area Network	局域网
L2TP	Layer 2 Tunnelling Protocol	第二层隧道协议
MP	Multilink PPP	PPP 多链路协议

OSPF	Open Shortest Path First Protocol	开放式最短路径优先协议
PPP	Point To Point Protocol	点到点协议
PPPoA	PPP over AAL5	
PPPoE	PPP over Ethernet	
PPPiFR	PPP in Frame Relay	
PSTN	Public Switched Telephone Network	公共交换电话网
RADIUS	Remote Authorization Dial In User Service	远程认证拨号用户服务
RIP	Routing Information Protocol	路由信息协议
SDH	Synchronous Digital Hierarchy	同步数字序列
SNMP	Simples Network Management Protocol	简单网络管理协议
VPDN	Virtual Private Dial _up Network	虚拟拨号专网
VPN	Virtual Private Network	虚拟专用网

5 设备功能

5.1 宽带网络接入服务器的参考结构

宽带网络接入服务器位于骨干网的边缘层，作为用户接入网和骨干网之间的网关，终结来自用户接入网的连接（主要是高速的用户接入网），提供接入到宽带核心业务网（主要为 IP 网和 ATM 网）的服务。

图 1 为宽带网络接入服务器的参考结构。

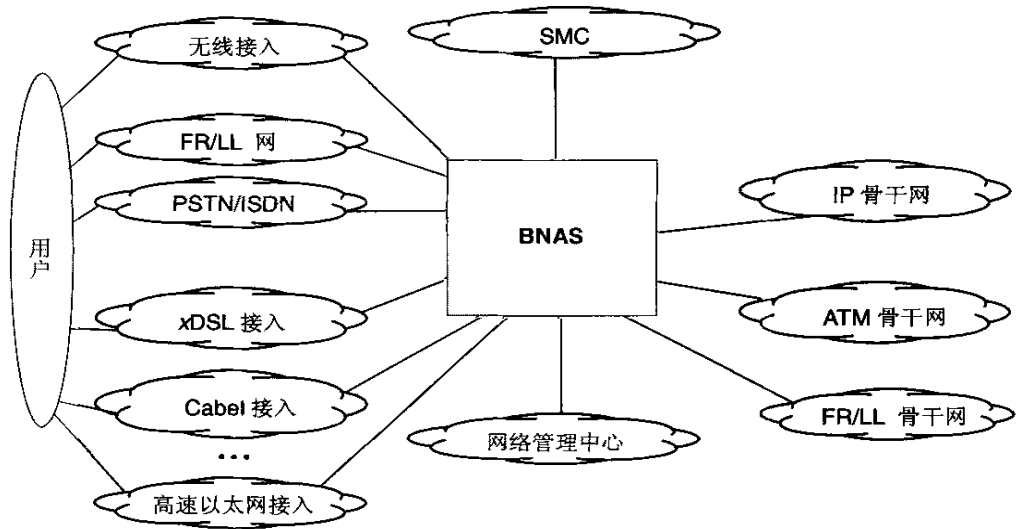


图 1 宽带网络接入服务器的参考结构

5.2 设备的功能组成

宽带网络接入服务器的功能组成可归类为五大功能模块。

5.2.1 接入功能模块

接入功能模块包括用户侧的接入模块（例如：FR/LL 接入、xDSL/接口接入、Cabel Modem 接入及 10/100/1000Mbit/s 接入等）和网络侧的接口模块（例如：ATM 接口模块、POS 接口模块、千兆以太网接口及 IP over WDM 接口模块）。

5.2.2 通信协议处理模块

通信协议处理模块包括用户侧通信协议（例如：FR UNI, PPPoA/PPPoE, IEEE802.3/IEEE802.3u/IEEE802.3z）和网络侧通信协议（例如：TCP/IP, IEEE802.3z, IP over SDH/IP over WDM, L2TP, IPSec）等。

5.2.3 网络安全模块

宽带网络接入服务器的网络安全模块包括 IP VPN 模块和防火墙模块（可选）。

5.2.4 业务管理模块

宽带网络接入服务器的业务管理模块包括网络接入认证与授权模块、计费模块和统计模块。

5.2.5 网络管理模块

宽带网络接入服务器的网管模块包括 SNMP 代理功能模块、Telnet 服务器功能模块和设备监控功能模块。通过这三种途径方式，可对宽带网络接入服务器进行配置、控制和管理。

5.3 设备功能要求

5.3.1 接口功能

宽带网络接入服务器在接入侧有以下功能接口。

1) ATM 接口（必选）

至少应能支持 STM-1 接口。宽带网络接入服务器在用户侧的 ATM 接口主要指与 xDSL 接入设备的接口，功能是终结或中继 xDSL 用户的 PPP 连接。

2) 10/100Mbit/s 以太网接口（必选）

宽带网络接入服务器的以太网接口主要指与 Cable Modem 接入的 CMTS 的接口，应至少支持 10/100Mbit/s 的以太网接口，功能是终结 Cable Modem 用户的 PPP 连接。以太网口也可以和 PSTN/ISDN 拨号用户的远程接入服务器（RAS）相连，转发拨号用户的 IP 数据流。

3) E1 接口（可选）

宽带网络接入服务器的 E1 接口主要是与 FR/LL 复接设备、远程接入服务器（RAS）及无线接入的局端设备相连，功能是将 FR/LL 用户的 PVC/专线连接在宽带网络接入服务器处终结，或将 PSTN/ISDN 拨号用户的远程接入服务器（RAS）的 IP 数据流中继到宽带网络接入服务器，然后通过宽带网络接入服务器将 IP 数据流转发到的 IP 业务网中去，或将移动数据用户的 PPP 连接在宽带网络接入服务器处终结或中继。

4) 同步串行接口（可选）

宽带网络接入服务器的同步串行接口（如 V.35 接口），主要是指与 FR/LL 复接设备、NAS 及无线接入局端设备相连的接口，功能是将 FR/LL 用户的 PVC/专线连接在宽带网络接入服务器处终结，或将 PSTN/ISDN 拨号用户的远程接入服务器（RAS）的 IP 数据流中继到宽带网络接入服务器，然后通过宽带网络接入服务器将 IP 数据流转发到的 IP 业务网中去，或将移动数据用户的 PPP 连接在宽带网络接入服务器处终结或中继。

宽带网络接入服务器在网络侧有以下功能接口。

1) ATM 接口（可选）

如果支持，至少支持 STM-1 接口和 STM-4 接口。宽带网络接入服务器在网络侧的 ATM 接口主要是将用户接入到 ATM 骨干网中去。

2) PoS 接口（可选）

如果支持，至少支持 STM-1 接口和 STM-4 接口。宽带网络接入服务器的 PoS（Packet over SDH）接口主要是将用户接入到 IP 骨干网中去。

3) 千兆以太网接口（必选）

至少应支持 1000Base-SX/1000Base-LX/1000BaseT 接口的一种。宽带网络接入服务器的千兆以太网接口主要是将用户接入到 IP 骨干网中去，

4) FR/LL 接口（可选）

一般为 E1 接口和 V.35 等同步串行接口。宽带网络接入服务器的 FR/LL 接口主要是将用户接入到 FR/LL 网中去。

5) WDM 接口 (可选)

是用户接入到 IP 骨干网的一种可选方式, 如果支持, 应符合相应标准。

5.3.2 通信协议实现和转换功能

宽带网络接入服务器面向不同类型接入设备 (如 DSLAM、CMTS、RAS 等), 是一种能提供端到端宽带连接的新型网络路由设备, 终结或中继来自用户的各种连接, 包括基于 PPP 的会话和采用不同封装形式的 PVC 连接。

宽带网络接入服务器应实现的网络协议如下:

1) 接入侧的通信协议

- a) FRAME RELAY LMI (ANSI T1.617 Annex D/ITU-T Q.933 Annex A) 协议 (可选);
- b) PPPoE 协议;
- c) PPPoA 协议;
- d) PPPiFR 协议 (可选);
- e) PPP 协议;
- f) LAN 协议 (IEEE 802.3/IEEE 802.3u);
- g) FRAME RELAY 上的多协议封装 (RFC 1490) (可选);
- h) AAL5 上的多协议封装 (RFC 1483)。

2) 网络侧的通信协议

- a) LAN 协议 (IEEE 802.3z);
- b) L2TP 协议;
- c) IP over SDH 协议 (RFC2615);
- d) IP over WDM 协议 (可选);
- e) TCP/IP 协议;
- f) IP 网络安全协议 IPSec (可选);
- g) 路由协议 (RIP v2 / OSPF v2 / BGP4) (可选);
- h) 接入认证协议 RADIUS;
- i) 网管协议 SNMP;
- j) Telnet 协议。

5.3.3 集中的流量控制和管理功能

宽带网络接入服务器接入的用户种类不同, 用户的业务需求也不同, 可对来自用户的各种连接中的流量加以整形, 应支持用户对业务带宽的集中控制和管理, 保证与用户协定的服务质量。

5.3.4 集中的接入认证与授权、计费 and 统计功能

宽带网络接入服务器应对不同的用户连接采取不同的集中接入认证与授权、计费信息统计策略, 如对 xDSL 用户可采取虚拟拨号方式进行类似接入服务器中的拨号用户的 AAA 服务, 对 FR/DDN 用户可采取端口出租, 收月租费的方式进行计费服务。

5.3.5 防火墙和 NAT 功能 (可选)

宽带网络接入服务器可选地支持防火墙功能, 如果支持, 主要有两种方式, 分别称为 IP Filter 和 IP Pool。IP Filter 是指宽带网络接入服务器提供 IP 包的过滤功能, 向不同权限的用户提供不同层次的 IP 包过滤功能, 以实现不同的用户有不同的接入能力。IP Pool 是指根据用户的授权从不同的 IP Pool 中读取 IP 地址给相应的用户作为用户的主叫 IP 地址, 在相应路由器中设定对不同主叫 IP 地址的不同的 IP 包的过滤能力, 从而实现不同的用户有不同的接入能力。

NAT 功能可选。

5.3.6 IP 安全网关功能（可选）

宽带网络接入服务器可为用户提供 IP 安全服务即 IP VPN 服务，可以支持基于 IPSec（IP 网络安全的标准协议）方式在 IP 网络上生成安全隧道，为用户提供在 IP 网络或 Internet 上建立安全的点对点连接。宽带网络接入服务器应具备开启和终结 IP 隧道的功能，支持公共密钥系统认证。

5.3.7 网管接口功能

宽带网络接入服务器接受 IP/ATM 业务网网管的管理，完成网络管理功能：配置管理、性能管理、故障管理、安全管理及记账管理等。

宽带网络接入服务器内置网管代理模块，通过网管代理模块实现与网管的通信、采集系统的信息并维护 MIB 库。

宽带网络接入服务器采用的管理协议为 SNMP，MIB 应符合 SNMP(RFC1157)、MIB II(RFC1213)、MIB II Traps(RFC1215)、ATM MIB(RFC1695)、Ethernet MIB(RFC1643)，可选地支持 RIP MIB(RFC1389)、OSPF MIB(RFC1253)、BGP4 MIB(RFC1657)及 FRAME RELAY MIB(RFC1315)等规定。

宽带网络接入服务器配置管理也应可通过 Telnet 来实现，其应具有 Telnet 通信协议接口和口令等安全管理功能。

网管对以下信息进行统计：用户 PPP 呼叫次数、PPP 呼叫不能连接次数、用户访问的平均时长、用户访问的平均费用、闲时概率、忙时概率、日均用户曲线、月均用户曲线、设备元素故障概率、无法拆链次数、ATM/FR PVC 的吞吐量、ATM/FR PVC 的差错率、异常终止原因及出现的频率等。

5.3.8 设备的监控和管理功能

宽带网络接入服务器应提供远端拨号接入监控功能和本地控制台（console）管理功能。远端拨号终端或本地控制台应能实现宽带网络接入服务器故障恢复后重新启动（reboot）功能，能实现对其维护和监控功能；远端拨号终端或本地控制台应能实现修改用户帐单的功能，可以添加或撤销用户帐单；远端拨号终端或本地控制台应能实现设备安全控制管理，可以修改用户身份码（PIN），强制拆除连接；远端拨号终端或本地控制台还应能实现设备故障定位功能。

6 通信接口

6.1 接入侧

1) xDSL 通信接口（可选）

宽带网络接入服务器的 ADSL 通信接口的物理层接口应支持 STM-1 接口，STM-1 有光接口和电接口两种。STM-1 接口技术要求参见标准 YD/T 1097-2001《路由器设备技术规范——高端路由器》。

2) Cabel Modem 通信接口（必选）

宽带网络接入服务器的 Cabel Modem 通信接口的物理层接口应支持 10/100BaseT 以太网接口（符合 IEEE802.3/ IEEE802.3u）。

3) 以太网通信接口（必选）

以太网通信接口应支持 10/100BaseT 以太网接口（符合 IEEE802.3/ IEEE802.3u）。

4) FR/DDN 接口（可选）

宽带网络接入服务器的 FR/DDN 通信接口应支持 E1 接口和 V.35 等同步串口，可选地支持 E3 接口。E1 和 V.35 同步接口技术要求参见标准 YD/T 1045-2000《网络接入服务器（NAS）技术规范》。E3 接口技术要求参见标准 YD/T 1097-2001《路由器设备技术规范——高端路由器》。

5) 无线接入通信接口（可选）

宽带网络接入服务器的无线接入通信接口通信接口应支持 E1 接口和 V.35 等同步串口。E1 和 V.35

同步接口技术要求参见标准 YD/T 1045-2000《网络接入服务器（NAS）技术规范》。

6) 远程接入服务器通信接口（可选）

宽带网络接入服务器的远程接入服务器（RAS）通信接口应支持 E1 接口、V.35 等同步串口及 10/100BaseT 以太网接口。E1 和 V.35 同步接口技术要求参见标准 YD/T 1045-2000《网络接入服务器（NAS）技术规范》，10/100BaseT 以太网接口符合 IEEE802.3/IEEE802.3u 标准。

6.2 网络侧

1) ATM 通信接口（可选）

宽带网络接入服务器的 ATM 通信接口应支持 STM-1、STM-4 接口，可选地支持 STM-16、STM-64 接口。STM-1、STM-4 接口技术要求参见标准 YD/T 1097-2001《路由器设备技术规范 —— 高端路由器》。STM-16、STM-64 接口应符合 YDN099-1998《SDH 技术体制》中对它们的相应要求。

2) LAN 接口（必选）

宽带网络接入服务器的 LAN 接口应支持千兆以太网接口（符合 IEEE802.3z）。1000Mbit/s 以太网物理接口支持 1000Base-SX、1000Base-LX 及 1000BaseT。它们的接口技术要求参见标准 YD/T 1097-2001《路由器设备技术规范 —— 高端路由器》。

3) FR/LL 接口（可选）

宽带网络接入服务器的 FR/LL 通信接口应支持 E1 接口和 V.35 等同步串口，可选地支持 E3 接口。

4) PoS 接口（可选）

宽带网络接入服务器的 PoS 接口应支持 STM-1、STM-4 接口，可选地支持 STM-16、STM-64 接口。STM-1、STM-4 接口技术要求参见标准 YD/T 1097-2001《路由器设备技术规范 —— 高端路由器》。STM-16、STM-64 接口应符合 YDN099-1998《SDH 技术体制》中对它们的相应要求。

5) WDM 接口（可选）

宽带网络接入服务器的 WDM 接口为可选。

7 通信流程

7.1 宽带接入服务器业务流程

对 PPP 会话的处理是宽带接入服务器的主要的和基本的功能之一。

宽带接入服务器可以提供基于 PPP 协商的服务选择方式，其功能是根据用户标识选择不同的 ISP 服务通道。

宽带接入服务器对 PPP 会话的处理分为：PPP 会话续传（PPP tunneling aggregation）和 PPP 会话终结（PPP terminated aggregation）两种。

下面按这两种情况描述宽带接入服务器的业务流程的处理。

7.1.1 PPP 会话续传（必选）

BNAS 完成 PPP 隧道交换，支持接入多个 ISP。

这种组网方式的特点是：

i) 用户以 PPPoE 或 PPPoA 方式上网。

ii) BNAS 根据用户 PPP 过程中输入的用户名中的结构化域名（如：“Username@ISP1.Net”）来选择对应的 ISP，并将用户的 PPP 承载在连接该 ISP 的 L2TP 隧道中，利用网络 QoS 属性实现 PVC 用户级别和限制接入速率，并进行针对用户的计费和安全进行管理。将用户来的大量 PPP 和 PVC 根据用户的选

择汇聚到连接相应 ISP 的少量 PVC 上的 L2TP 隧道，起到服务选择和 PVC 汇聚的作用。

iii) 上行 L2TP 隧道可以在 UDP/IP 上，对 ATM 核心网络而言，基于 IPoA 封装，或者直接 L2TPoA 封装（可选）；对 IP 核心网络而言，可直接封装。

7.1.2 PPP 会话端结（必选）

BNAS 完成 PPP 端结并支持多个 ISP。这种组网方式的特点是：

i) 用户以 PPPoE 或 PPPoA 方式上网。

ii) BNAS 完成用户 PPP 的验证，可以据此来划分用户级别和限制接入速率，并进行针对用户的计费和安全进行管理。注意：BNAS 需要根据用户的输入，选择不同 ISP 的 AAA 服务器完成认证。

iii) BNAS 需要与各个 ISP 之间建立一个逻辑连接（虚拟接口）（可以用 IPoA 或 PPPoA 的 PVC），BNAS 根据用户的输入选择不同的 PVC 接口发送业务包。

7.1.3 与 ISCP（Internet Service Control Point）相配合，提供基于 WEB 的服务选择方式（可选）

BNAS 为了区分用户连接，可以使用 PVC 来标识用户（IPoA，PPPoA），也可以用 PPPoE 来标识用户。下面是 BNAS 提供基于 Web 的服务选择方式下的用户上网流程的一个范例。

a) 用户机器上电启动，系统程序根据配置，通过 DHCP，由 BNAS 做 DHCP-Relay，向 DHCP Server 要 IP 地址（私网），或通过 PPPoEoA 通过 AAA 服务器分配 IP 地址（私网）；

b) BNAS 为该用户构造对应表项信息（基于 PVC 或 PPP），添加用户 ISCP 服务策略（让用户只能访问 ISCP 和一些服务器 DNS），同时将地址告诉用户终端；

c) 用户然后启动浏览器，访问 ISCP，ISCP 可以根据用户的源 IP 地址得到用户标识，提供定制的服务选择页面，或者直接提供用户登录页面，根据用户登录信息生成定制服务选择页面；

d) 通过服务选择页面在用户浏览器的 Java 虚拟机上运行，可以进行用户和 BNAS 以及 ISCP 之间的控制交互，完成用户服务选择，修改 BNAS 上的用户表项信息中的策略。

e) 如果用户选择本地 ICP 服务，可以通过页面完成与 ICP 之间的用户验证，修改 BNAS 上的用户表项信息中的策略，这样用户就可以接收到该 ICP 的服务了。

f) 如果用户选择 ISP 服务，可以通过页面完成与 ISP 之间的用户验证以及可能的地址分配，修改 BNAS 上的用户表项信息中的策略，BNAS 将该用户上 Internet 的业务转发到相应 ISP 的 PVC 上，这样用户就可以通过该 ISP 上网了。

7.2 RADIUS 的通信流程

宽带网络接入服务器的 RADIUS 的通信流程可参见标准 YD/T 1045-2000《网络接入服务器（NAS）技术规范》。

7.3 Telnet 的通信流程

宽带网络接入服务器的 Telnet 的通信流程可参见标准 YD/T 1045-2000《网络接入服务器（NAS）技术规范》。

7.4 SNMP 的通信流程

宽带网络接入服务器的 SNMP 的通信流程可参见标准 YD/T 1045-2000《网络接入服务器（NAS）技术规范》。

8 IP 地址管理和分配流程

IP 地址的管理和分配是 IP 网上接入设备的核心技术。宽带接入服务器一般采用分布式、模块化的处理技术，用户 IP 地址既可以由外部的 AAA SERVER 或专门的地址分配中心（IMC）在授权时统一提供。在用户通过认证后，接入处理单元会将获得的用户 IP 地址发送到 PPP 模块，由 PPP 模块与用户协商完成最终用户地址的分配。

一般来说，需要宽带接入服务器支持以下几种地址分配方式：

1) 本地地址分配（必选）

有两种情况：AAA SERVER 返回用户地址池，这时接入处理单元应该按照 AAA 指定的地址池为用

户分配 IP 地址；AAA SERVER 没有用户 IP 地址池的返回，这时用户处理单元应该支持缺省地址池方式，从缺省地址池中为用户分配 IP 地址。

2) AAA SERVER 指定用户地址（必选）

如果在 AAA SERVER 认证中相应包含有对用户地址的授权信息，这时宽带接入服务器处理单元应该按照 AAA SERVER 返回的地址为用户分配。

3) IAC 方式的地址分配（可选）

在某些应用中，所有 IP 地址可能会由 IP 地址管理中心 IMC 来统一管理，这时除了认证授权包外，接入处理单元应该能通过与 IMC 的包交互来完成用户地址的分配。

9 协议要求

9.1 PPP

参见标准 YD/T 1045-2000《网络接入服务器（NAS）技术规范》中 8.4 节。

9.2 PPPoA

9.2.1 定义

PPPoA 规定的是标准 PPP 帧在 AAL5 上的帧封装方法和格式，PPPoA 会话流程与标准的 PPP 会话流程相同。PPP 层把底下的 ATM AAL5 层看作一个比特同步的点到点链路，即 PPP 链路对应于一个 ATM AAL5 虚连接。ATM AAL5 虚连接必须是全双工、点到点 VCC。

9.2.2 协议基本框架

PPPoA 协议参照 RFC1483，RFC2364。

PPPoA 完成 PPP 帧在 AAL5 上的适配，其实现必须支持 VC 复用 PPP 和 LLC 封装 PPP，对于 SVC，必须用 Q.2931 附录 C 过程进行协商。目前 BNAS 只支持 PVC 方式。图 2 是 PPPoA 的协议栈结构。

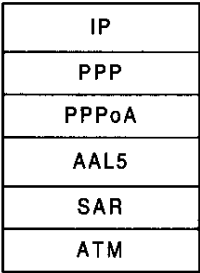


图 2 PPPoA 的协议栈

9.2.3 AAL5 层业务接口要求

PPP 层把底下的 ATM AAL5 层看作一个比特同步的点到点链路，即 PPP 链路对应于一个 ATM AAL5 虚连接。ATM AAL5 虚连接必须是全双工、点到点 PVC 或者 SVC，目前实现只支持 PVC 方式。另外，PPP/AAL5 业务接口必须符合以下要求：

接口格式：PPP/AAL5 层边界向 AAL5 层提供一个字节业务接口。

传输速率：PPP 层不对传输速率和下面的 ATM 层流量描述参数强加任何限制。

控制信号：AAL5 层必须向 PPP 层提供控制信号，指示何时虚连接链路已经连接或拆除，即提供“UP”和“DOWN”事件给 PPP 层的 LCP 状态机。

9.2.4 PPPoA 通信流程

PPPoA 的通信流程与标准的 PPP 通信流程相同。

9.2.5 PPPoA 的帧格式

a) AAL5 PDU 格式

AAL5 PDU 的格式如图 3 所示。

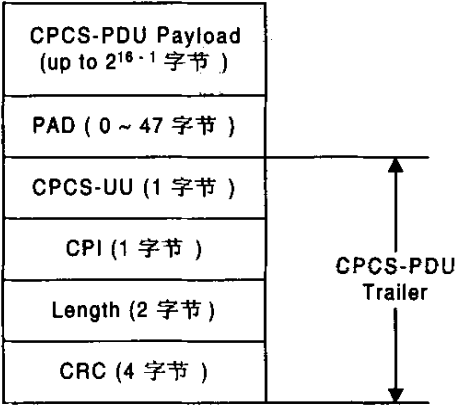


图 3 AAL5 PDU 帧格式

AAL5 PDU 格式的各字段含义如下：

- 1) CPCS—PDU 净荷：包含有最大长度为 $2^{16}-1$ 个八位组的用户信息。
 - 2) PAD：填充域填充 CPCS—PDU，使得它是 48 字节的整数倍。
 - 3) CPCS—UU：CPCS 用户到用户指示域用来透明传送 CPCS 用户到用户的信息。这个域在多协议 ATM 封装中没有作用（PPP over AAL5），并且可以被设置为任何值。
 - 4) CPI：公共部分指示域用来调整 CPCS—PDU 尾部的长度为 64bit。当只用于 64bit 调整功能时，这个域被编码为 0x00。
 - 5) Length：长度域以八位组为单位，说明净荷域的长度。长度域的最大值是 65535 个八位组。值为 0x00 的长度域用于中断功能。
 - 6) CRC：CRC 域用来保护除 CRC 域本身以外的整个 CPCS—PDU。
- b) VC 复用 PPP 帧格式

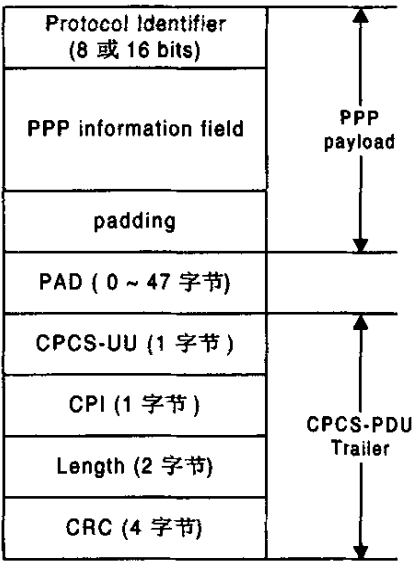


图 4 VC 复用 PPP 帧格式

图 4 是 VC 复用 PPP 帧格式。
VC 复用 PPP 帧构成 CPCS—PDU 的净荷。
c) LLC 封装 PPP 帧格式
图 5 是 LLC 封装 PPP 帧格式。

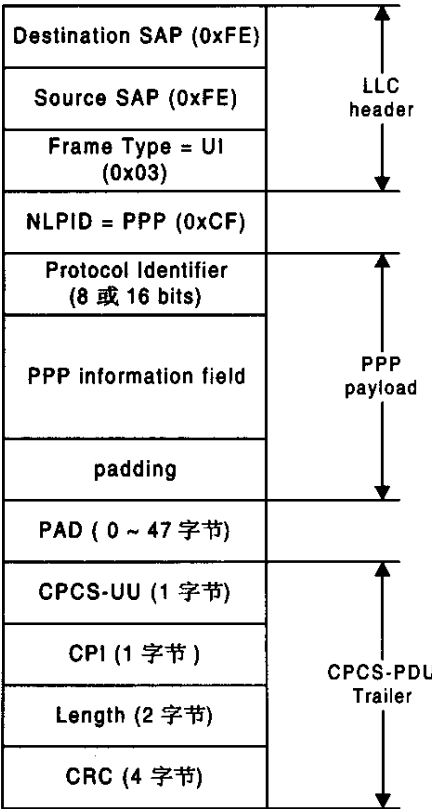


图 5 LLC 封装 PPP 帧格式

- LLC 封装 PPP 帧中的各字段含义如下：
- 1) LLC 头：说明源 SAP (0xFE)、目的 SAP (0xFE) 和无编号信息帧类型 (0x03)。
 - 2) NLPID：网络层协议 ID 表示 PPP (0xCF)。
 - 3) PPP 协议 ID：可以是 1 或 2 个八位组长。
 - 4) PPP 信息域：同上。

9.2.6 检测和恢复未主动请求的 PPP 封装转换

当虚连接丢失状态，PPP 封装技术可能会单方面地、不希望地改变。PPPoA 定义了用于下面状态转移的检测和恢复过程：

- a) VC 复用 PPP 改变到 LLC 封装 PPP；
- b) LLC 封装 PPP 改变到 VC 复用 PPP。

当使用 LLC 封装 PPP，LCP 分组的初始 6 个字节包含下面序列：FE-FE-03-Cf-C0-21，这个序列组成 AAL5 帧的最初的 6 个字节。在 VC 复用 PPP 的情况下，最初的 LCP 分组包含下面序列：C0-21，这个序列组成 AAL5 帧的最初 2 个字节。当接收到并识别出 LCP 配置请求分组，PPP 链路进入链路建立阶段。

一旦 PPP 进入网络层协议阶段，并且成功地协商一个特定的 NCP 用于 PPP 协议，如果接收到一个

帧，这个帧使用一个可选的、但是等效的数据封装（在 RFC1483 中定义），那么对于 PVC，PPP 链路必须拆除激活的 NCP，应该产生一个错误消息，进入终止状态，并且静默丢弃所有接收的分组。

这些策略防止对端丢失状态时会发生的“黑洞”。

9.2.7 PPPoA 的 LCP 配置选项

PPP over AAL5 (RFC2364) 建议进行魔数选项协商，不建议进行协议域压缩 (PFC) 选项协商。实现中必须不请求进行任何下面的选项协商，并且必须拒绝这样选项协商的请求：

- Field Check Sequence (FCS) Alternatives,
- Address-and-Control-Field-Compression (ACFC)
- Asynchronous-Control-Character-Map (ACCM)

MRU 必须不能大于虚连接相关方向的流量协定的最大 CPCS-SDU 长度。

9.3 PPPoE

9.3.1 定义

通过 PPPoE，在一个共享的以太网上的多个主机，可以通过一个或多个简单的桥接入设备，与远程接入集中器进行多个 PPP 会话。使用这种模型，每个主机使用它自己的 PPP 协议栈，并且提供给用户一个熟悉的用户接口。接入控制、计费和服务类型能够基于每用户，而不是每站点来处理。PPPoE 包含发现和 PPP 会话两个阶段，发现阶段是无状态的 Client/Server 模式，目的是获得 PPPoE 终结端的以太网 MAC 地址，并建立一个唯一的 PPPoE SESSION_ID。发现阶段结束后，就进入标准的 PPP 会话阶段。

9.3.2 协议基本框架

PPPoE 协议参照 RFC2516。

PPPoE 实现 PPP 帧在 Ethernet 上的适配，并提供 Ethernet 上的 PPP 连接。图 6 和图 7 分别是以太网上的 PPPoE 协议栈和 AAL5 上的 PPPoE 协议栈。

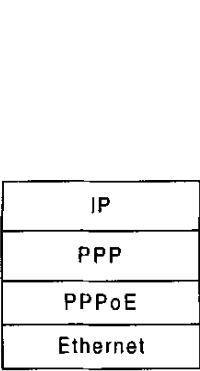


图 6 以太网上的 PPPoE 协议栈

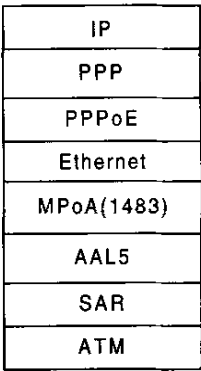


图 7 AAL5 上的 PPPoE 协议栈

9.3.3 PPPoE 连接示意图

图 8 显示了典型的 PPPoE 的连接方式。

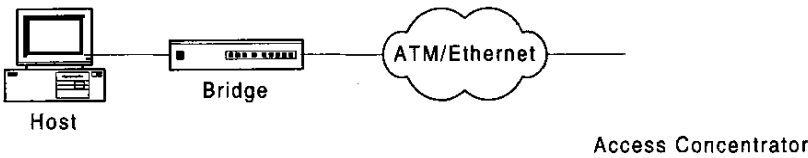


图 8 典型的 PPPoE 的连示意

9.3.4 PPPoE 通信流程

PPPoE 有两个不同的阶段：发现阶段和 PPP 会话阶段。当一个主机想开始一个 PPPoE 会话时，它必须首先进行发现阶段以识别对端的以太网 MAC 地址，并建立一个 PPPoE SESSION_ID。在发现阶段，基于网络的拓扑，主机可以发现多个接入集中器。发现阶段允许主机发现所有的接入集中器，然后选择一个。当发现阶段成功完成，主机和选择的接入集中器都有了他们在以太网上建立 PPP 连接的信息。直到 PPP 会话建立，发现阶段一直保持无状态的状态。一旦 PPP 会话建立，主机和接入集中器都必须为 PPP 虚接口分配资源。图 9 显示了 PPPoE 通信流程。

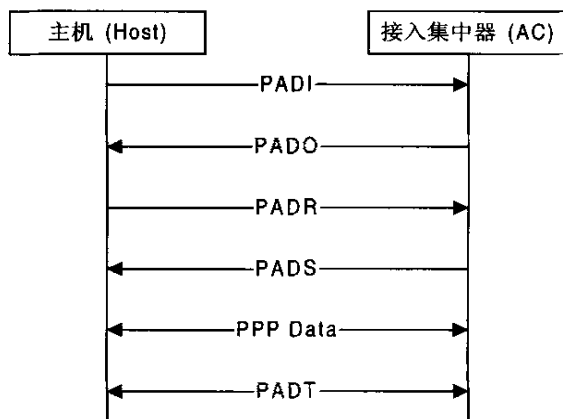


图 9 PPPoE 通信流程

a) 发现阶段

发现阶段有 4 个步骤，当此阶段完成，通信的两端都知道 PPPoE SESSION_ID 和对端的以太网地址，他们一起唯一定义 PPPoE 会话。这些步骤包括：主机广播一个发起分组 (PADI)，一个或多个接入集中器发送给予分组 (PADO)，主机发送单播会话请求分组 (PADR)，选择的接入集中器发送一个确认分组 (PADS)。当主机接收到确认分组，它可以开始进行 PPP 会话阶段。当接入集中器发送出确认分组，它可以开始进行 PPP 会话阶段。

当主机在指定的时间内没有接收到 PADO，它应该重新发送它的 PADI 分组，并且加倍等待时间，这个过程会被重复期望的次数。如果主机正在等待接收 PADS，应该使用具有主机重新发送 PADR 的相似超时机制。在重试指定的次数后，主机应该重新发送 PADI 分组。

PPPoE 还有一个 PADT 分组，它可以在会话建立后的任何时候发送，来终止 PPPoE 会话。它可以由主机或者接入集中器发送。当接收到一个 PADT，不再允许使用这个会话来发送 PPP 业务。在发送或接收 PADT 后，即使正常的 PPP 终止分组也不必发送。PPP 对端应该使用 PPP 协议自身来终止 PPPoE 会话，但是当 PPP 不能使用时，可以使用 PADT。

b) PPP 会话阶段

一旦 PPPoE 会话开始，PPP 数据就可以以任何其他的 PPP 封装形式发送。所有的以太网帧都是单播的。PPPoE 会话的 SESSION_ID 一定不能改变，并且必须是发现阶段分配的值。

9.3.5 PPPoE 帧格式

a) 以太网帧格式

图 10 是以太网帧格式，以太网帧的各字段含义如下：

1) DESTINATION_ADDR：目的地址域包含一个单播以太网地址，或者一个以太网广播地址 (0xFFFFFFFF)。对于发现阶段的分组，这个值是发现阶段定义的单播或者广播地址。对于 PPP 会话阶

段，这个域必须包含发现阶段所决定的对端的单播地址。

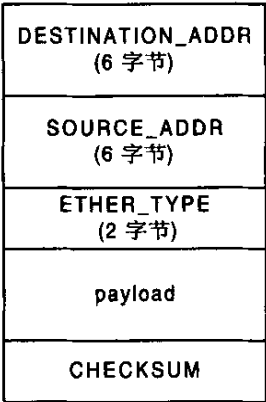


图 10 以太网帧格式

- 2) SOURCE_ADDR: 源地址域必须包含源设备的以太网 MAC 地址。
- 3) ETHER_TYPE: 类型域或者被设置为 0x8863 (发现阶段)，或者被设置为 0x8864 (PPP 会话阶段)。

b) PPPoE 帧格式

图 11 是 PPPoE 帧格式。

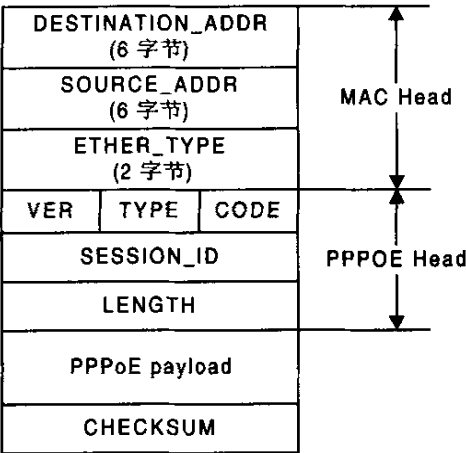


图 11 PPPoE 帧格式

用于 PPPoE 的以太网净荷的各字段的含义如下：

- 1) VER: 版本域是 4bit，并且对于 PPPoE 规范的这个版本必须被设置为 0x1。
- 2) TYPE: 类型域是 4bit，并且对于 PPPoE 规范的这个版本必须被设置为 0x1。
- 3) CODE: 代码域是 8bit，由发现阶段和 PPP 会话阶段分别定义。
- 4) SESSION_ID: 会话标识域是 16bit，它是一个网络字节顺序的无符号值。它的值由发现阶段的分组定义。对于一个给定的 PPP 会话，这个值是固定的。事实上，会话标识和以太网源地址、目的地址一起定义了 PPP 会话。值 0xFFFF 被保留，用于将来使用，并且一定不能被使用。

5) LENGTH: 长度域是 16bit。这个值是网络字节顺序, 说明 PPPoE 净荷的长度。它不包括以太网或者 PPPoE 头的长度。

PPPoE 特定的分组如下:

- 1) PPPoE 主动发现发起 (PADI);
- 2) PPPoE 主动发现给予 (PADO);
- 3) PPPoE 主动发现请求 (PADR);
- 4) PPPoE 主动发现会话确认 (PADS);
- 5) PPPoE 主动发现会话终结 (PADT)。

c) PPPoE 发现阶段净荷的 TLV 格式

PPPoE 净荷包含零个或者多个 TAGs, TAG 是一个 TLV (类型—长度—数值) 结构, 如图 12 所示。

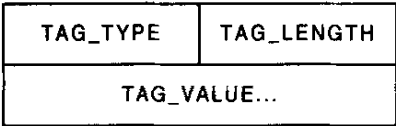


图 12 PPPoE 发现阶段净荷的 TLV 格式

TLV 各字段的含义如下:

1) TAG_TYPE: 标记类型是网络字节顺序的 16bit 字段。如果收到带有不认识的标记类型的发现分组, 必须忽略这个标记, 除非 RFC2516 中有其它说明。PPPoE 目前包含的标记类型及其相应的标记值如表 1 所示:

表 1 TAG—TYPE 字段的值

TAG_TYPES	TAG_VALUES
End-Of-List	0x0000
Service-Name	0x0101
AC-Name	0x0102
Host-Uniq	0x0103
AC-Cookie	0x0104
Vendor-Specific	0x0105
Relay-Session-Id	0x0110
Service-Name-Error	0x0201
AC-System-Error	0x0202
Generic-Error	0x0203

2) TAG_LENGTH: 标记长度是 16bit, 它是一个网络字节顺序的无符号数, 说明标记值的以字节为单位的长度。

9.3.6 PPPoE 的 LCP 配置选项

PPP over Ethernet (RFC2516) 建议进行魔数选项协商, 不建议进行协议域压缩选项 (PFC) 协商。实现中必须不请求进行任何下面的选项协商, 并且必须拒绝这样选项协商的请求。

- Field Check Sequence (FCS) Alternatives
- Address-and-Control-Field-Compression (ACFC)
- Asynchronous-Control-Character-Map (ACCM)
- MRU 必须不能大于 1492。

建议接入集中器偶尔向主机发送 **Echo_Request** 报文，来决定会话的状态。否则，如果主机没有发送 **Terminate_Request** 报文就终止了会话，接入集中器将会不能决定会话已经终止了。

当 **LCP** 终止，主机和接入集中器必须停止使用这个 **PPPoE** 会话。如果主机希望开始另一个 **PPP** 会话，它必须返回到 **PPPoE** 的发现阶段。

9.4 PPPiFR（可选）

9.4.1 定义

PPPiFR (**RFC1973**) 规定的是标准 **PPP** 帧在帧中继链路中的封装方法和格式，**PPPiFR** 会话流程与标准的 **PPP** 会话流程相同。**PPP** 把帧中继链路看作一个比特同步的链路，这个链路必须是全双工的，但可以是 **PVC** 或者 **SVC**，目前 **BNAS** 实现只支持 **PVC**。

9.4.2 协议基本框架

PPPiFR 协议参照 **RFC1973**。

PPPiFR 完成 **PPP** 帧在帧中继链路中的适配，图 13 是 **PPPiFR** 的协议栈结构。

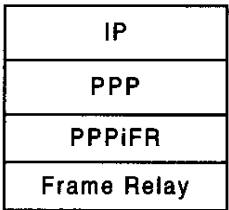


图 13 PPPiFR 的协议栈

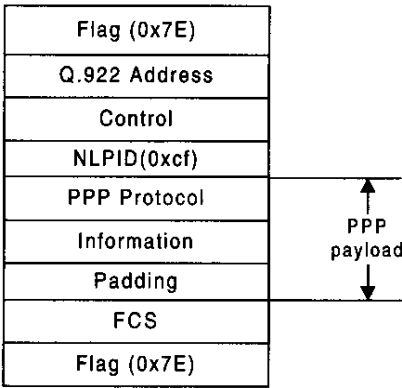


图 14 PPPiFR 的帧格式

9.4.3 PPPiFR 通信流程

PPPiFR 的通信流程与标准的 **PPP** 通信流程相同。

9.4.4 PPPiFR 的帧格式

图 14 是 **PPPiFR** 的帧格式，它的各字段的含义如下：

- 1) **Flag**: 用于帧定界；
- 2) **Q.922 地址**: 目前定义的 **Q.922** 地址是包含 10 个比特 **DLCI** 的两个八位组，在一些网络中，**Q.922** 地址可以有选择性地增加到 3 或 4 个八位组；
- 3) **Control**: 控制域是 **Q.922** 控制域；
- 4) **NLPID**: 标识后面的封装类型；
- 5) **PPP 协议域和后面的信息、填充域**是 **PPP** 帧的净荷。

9.4.5 基本帧的修改

LCP 可以协商修改基本帧结构，然而，改变的帧与标准帧应总是可明确区别的。

a) 地址和控制域压缩 (**ACFC**)

因为地址和控制域数值不是常量，并且当帧被网络交换结构传输时，地址和控制域数值被修改，所以一定不要协商地址和控制域压缩。

b) 协议域压缩 (**ACCM**)

注：不象 **PPP-HDLC** 组帧，帧中继组帧不以 32 比特边界对齐信息域。当 **NLPID** 被除去，并且协议域被压缩为一个单字节时，对齐 32 比特边界才会发生。当为了提高吞吐量时，应该协商协议域压缩。

9.4.6 带内协议解复用

为了避免协议域压缩（PFC）使能时发生多义性，协议域值：0x00CF 是不允许的。

初始的 LCP 分组头后包含下面序列：Cf—C0—21，当接收到并识别出 LCP 配置请求，PPP 链路进入链路建立阶段。

一旦 PPP 进入链路建立阶段，必须不发送具有其他 NLPID 值的分组，并且接收到这样的分组必须静默丢弃，直到 PPP 链路进入网络层协议阶段。

一旦 PPP 进入网络层协议阶段，并且成功地协商了一个用于 PPP 协议的特定的 NCP，如果接收到一个帧，它使用在 RFC1490 中定义的另一个等效的数据封装，PPP 链路必须重新进入链路建立阶段，并且发送一个新的 LCP 配置请求。这个过程可以防止对端丢失状态时发生的“黑洞”。

9.4.7 PPPiFR 的配置

PPPiFR 建议进行魔数、协议域压缩（PFC）选项的协商。初始的 MRU 是 1600。为了避免分段，网络层的 MTU 不应该超过 1500，除非数值为 2048 或者更大值的对端 MTU 被特别协商。不需要反向 ARP 来支持 PPP 链路，这个功能由 PPP NCP 协商来提供。

9.5 协议

L2TP 协议要求主要参见标准 YD/T 1045-2000《网络接入服务器（NAS）技术规范》中 8.3 节。

以下主要介绍 L2TP over ATM。

9.5.1 L2TP over ATM（可选）

通道技术（Tunneling）是 VPDN（虚拟拨号专网）技术的核心。L2TP 协议则是其中一种通道技术，它是 Internet 工程任务组 IETF 的国际标准。通道协议所采用的方法是将用户的整个数据包（包括附加的协议成份）作为网络传输协议的载荷（Payload）部分封装后再进行传输。

L2TP 协议是一个用于在 LAC 和 LNS 之间建立透明 PPP 传输通道，以实现远端拨号用户对企业内联网的访问的协议。而 L2TP over ATM 则指定 ATM 网络作为传输媒介。它分为两种情况：指定使用 ATM 网络作为 LNS 与 LAC 之间的通信链路；指定使用 ATM 网络作为接入网络。

9.5.2 L2TP 协议

L2TP 信息包括两种：控制信息（control message）和数据信息（data message）。

1) 控制信息类型

控制信息用于建立隧道、拆除隧道和维护隧道，它包括 14 种信息：

SCCRQ	Start-Control-Connection-Request
SCCRP	Start-Control-Connection-Reply
SCCCN	Start-Control-Connection-Connected
HELLO	hello
OCRQ	Outgoing-Call-Request
OCRP	Outgoing-Call-Reply
OCCN	Outgoing-Call-Connected
ICRQ	Incoming-Call-Request
ICRP	Incoming-Call-Reply
ICCN	Incoming-Call-Connected
CDN	Call-Disconnect-Notify
WEN	WAN-Error-Notify
SLI	Set-Link-Info

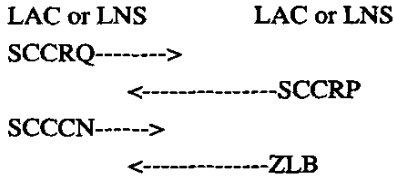
注：

1. 在 LAC 和 LNS 建立隧道，然后在隧道中建立会话，在一个隧道中可以传输多路的会话信息；
2. HELLO 信息传输是为了维护隧道的连通性；
3. WEN 用于 LAC 向 LNS 报告差错信息；

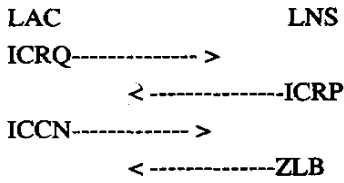
4. SLI 用于设定 PPP 协商选项。

2) 控制连接状态机

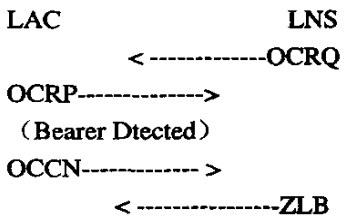
a) 隧道建立



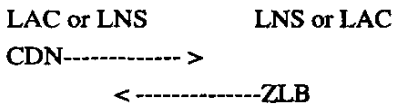
b) 入呼叫建立



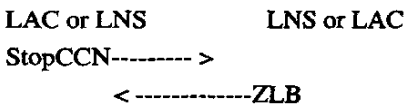
c) 出呼叫建立



d) 关闭呼叫



e) 拆除隧道



3) 数据信息封装

将 PPP 数据信息封装到 L2TP 信息包中, 从而实现 PPP 通路的逻辑扩展, L2TP 协议结构如图 15 所示。

PPP Frames	
L2TP Data Messages	L2TP Control Messages
L2TP Data Channel (unreliable)	L2TP Control Channel (reliable)
Packet Transport(UDP, FR, ATM 等)	

图 15 L2TP 协议结构

4) L2TP 数据格式

如图 16 所示。

T	L	x	x	S	x	O	P	x	x	x	x	版本号	长度（可选项）
通道标识													会话标识
发送序列号（可选）													希望接收序列号（可选）
填充长度（可选）													填充（可选）

图 16 L2TP 数据格式

各个字段的含义：

T 标志位：指定信息包的信息类型，对于数据信息它被设为 0，控制信息则置为 1；

L 标志位：当置为 1 时，长度域存在；

S 标志位：当置为 1 时，序列号域存在；

O 标志位：当置为 1 时，填充域存在；

P 标志位：当置为 1 时，这个数据信息优先处理；

版本号：对于 L2TP，必须为 2；

通道标识：指定控制连接的通道标识；

会话标识：用于指定通道中会话的标识；

发送序列号：指定这个数据或控制信息的序列号；

接收序列号：指定希望接收的下一个控制信息的序列号；

填充域：指定 L2TP 头长度，从而确定载荷的开始位置。

5) AVP 格式

每个控制信息是由一系列 AVP（属性值对）组成的，每个 AVP 有相同的格式，如图 17 所示。

M	H	保留	长度	厂商标识
属性类型				属性值
(直到指定长度)				

图 17 AVP 的格式

M 标志位：当接收到未知的 AVP 中 M 标志置位，则与之相关的通道或会话关闭；

H 标志位：当置位 1 时，指定这个 AVP 的属性值域数据已经隐藏起来；

厂商标识：厂商使用它扩展 L2TP 功能，以和其他厂商区别；

属性类型：指定 AVP 类型；

属性值：根据 AVP 类型不同，实际的值相应变化。

9.5.3 ATM 网络信息封装

当把 ATM 作为 LAC、LNS 之间的传输媒介，这时就需要将 L2TP 信息包封装到 ATM 的 ALL5 中。

L2TP 把底层 ATM AAL5 层服务作为一个位同步的点到点链路。一个 L2TP 链路对应于一个 ATM AAL5 虚电路（VC）。并且这个虚电路是全双工、点对点，可以根据需要建立或是永久建立的。

1) 采用 ATM 作为传输媒介需要考虑的问题如下：

a) 最大传输单元（MTU）

L2TP PDU 是封装在 ALL5 PDU 中的，因此 ALL5 连接的最大传输单元就限制了用这个连接的通道的 MTU 和用这个通道的所有 PPP 连接的 MTU。这就要求需要 ATM 指定合适的 MTU 以适应 L2TP 协议

的要求。

b) 服务质量

对于每个不同的客户连接可能需要不同的服务质量，可以在 LAC、LNS 之间建立多个 ALL5 连接来满足需要。

c) ATM 连接参数

为了建立 PVC（永久虚电路），双方需要协商特定的流量参数。

2) 多协议封装

有两种方法标识封装在 ALL5 PDU 的载荷域的协议：基于多路复用的虚电路[Virtual circuit (VC)based multiplexing]和逻辑链路控制封装[Logical Link Control (LLC) Encapsulation]。

对于第一种方法，载荷的协议类型是使用监督或控制平台过程（provisioning or control plane procedures）由虚电路的端点协商。这种机制被称为 VC 多路复用 L2TP；对于第二种方法，载荷的协议类型由 AAL5 PDU 中的 IEEE 802.2 LLC 头部标识的。这种机制被称为 LLC 封装 L2TP。

要求一种 L2TP 的实现方案：

- a) 必须支持在 PVC 上 LLC 封装 L2TP；
- b) 可以支持 SVC 上的 LLC 封装 L2TP；
- c) 可以支持在 PVC 或 SVC 上的 VC 多路复用 L2TP。

当一个 PVC 被用时，端点必须被配置使用两种封装方法中的一种。

如果一种实现方案支持交换式 VC 连接，它必须使用 Q.2931 去协商连接开始过程(connection setup)，将宽带底层接口（B-LLI）信息单元编码以发出 VC 多路复用 L2TP 或 LLC 封装 L2TP。

3) LLC 封装 L2TP over AAL5

当使用 LLC 封装时，AAL5 CPCS PDU 的载荷域采用图 18 所示的编码格式。

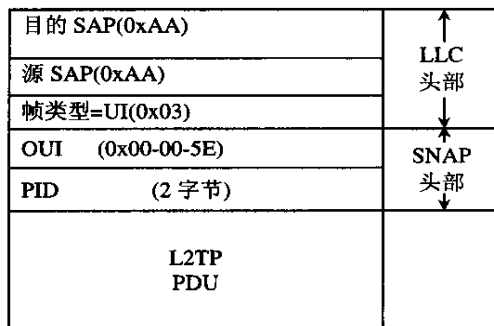


图 18 LLC 封装

a) IEEE 802.2 LLC 头部：包括源和目的 SAP，值都为 0xAA，接着是未编号信息的帧类型（值 0x03），这个 LLC 头部指定了接下来的 IEEE 802.1a SNAP 头部。

b) IEEE 802.1a SNAP 头部：3 个字节的团体唯一标识符[Organizationally Unique Identifier (OUI)]，其值为 0x00-00-5E 标识 IANA(Internet Assigned Numbers Authority)，以及两个字节的协议标识（PID），指定了 L2TP 作为封装协议。这个 PID 值是由 IANA 确定的。

c) L2TP PDU。

4) 虚电路多路复用 L2TP over AAL5

VC 多路复用 L2TP over AAL5 是一种可选的封装方案，在这种情况下 L2TP PDU 是 AAL5 负载，

因此它也被称为“空封装”(“Null encapsulation”)。

AAL5 CPCS PDU 格式如图 19 所示。

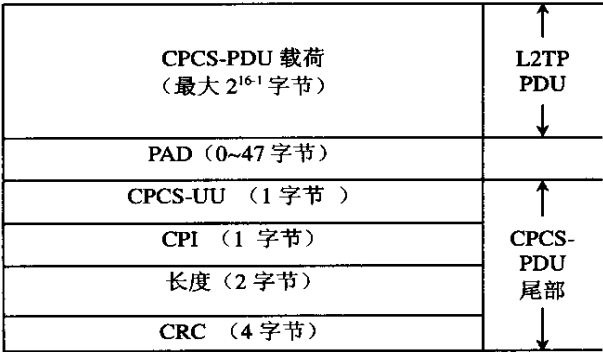


图 19 AAL5 CPCS-PDU 格式

通用部分会聚子层(CPCS)PDU 载荷域包括最大可至 $2^{16}-1$ 字节的用户信息。PAD 域填充 CPCS-PDU 以适应 ATM 信元使得由 SAR (分割与重组) 子层产生最后一个 48 个字节的信元 (包括 CPCS-PDU 尾部) 正好在一个信元中。

CPCS-UU (用户到用户指示) 域被用来透明传输 CPCS 用户到用户信息。这个域在多协议 ATM 封装中没有意义, 可以设为任何值。

公共部分指示符 CPI (Common Part Indicator) 域使得 CPCS-PDU 尾部是 64 比特的整数倍。将来可能会加入其他功能, 目前设置为 0x00。

长度域以字节为单位指定载荷的长度。这个域的最大值是 65535。

CRC 域提供了除 CRC 段本身以外的整个 CPCS-PDU 的差错检查能力。

5) 带外控制平面信令 (Out-Of-Band Control Plane Signaling)

a) 连接建立 (Connection Setup)

一个交换式虚电路连接可以由 LAC 或 LNS 发起。支持 SVC 的实现方案必须能够发起和响应 SVC 建立 (setup) 请求。

当呼叫方发起一个交换虚电路 AAL5 连接时, 它必须在 SETUP 信息中指出是要求 VC 多路复用 L2TP 还是 LLC 封装 L2TP, 或者是两者皆可。B-LLI 信息单元将会用来指定要求的封装信息格式。

实现方案必须能够接收一个由 LLC 封装 L2TP 请求的入呼叫。当接收到一个不支持的封装方式时, 被呼的过程必须抛弃呼叫建立请求。

如果一个 SVC 通道重起时, 双方必须清除连接, 并且在这个通道中的任何呼叫将被终止, 当从一个客户接收到一个新的请求时任何一方都可以试图重建。

b) 连接建立失败

当连接建立失败时, 试图进行连接建立的 L2TP 实体认为被呼实体不可达。实体怎样认为对方不可达以及怎样确定对方可用是由实现方法决定的。

c) 连接终止 (Connection Teardown)

当在 SVC 通道中没有活动的呼叫, 任何一方都可以有选择地清除连接。

d) 连接失败

当收到一个 AAL5 SVC 连接被清除的消息, 实现方案要求关闭通道并且返回控制连接状态到空闲状态。

如果一个 AAL5 PVC 进入到停止状态 (“Stopped” state), 实现方案也将关闭通道返回控制连接状

态到空闲状态。

9.5.4 ATM 网络信息扩展

当指定 ATM 网络作为 VPDN 实现方案的接入网时, L2TP 协议要进行以下方面的扩展。

- a) ATM 连接的流量管理方面 (例如: 不对称的带宽分配和服务种类选择能力);
- b) 用于交换 ATM 网络的地址格式;
- c) 当在 PPP 连接的接入网部分传输 PPP over AAL5 (PPPoA) 时强加到 LCP 协商上面的一些限制。

1) ATM 接入增强过程

当一个虚拟拨号客户通过一个 (交换) ATM 接入网发起呼叫时, 这时整个过程和 PSTN 作为接入网有所不同。

a) ATM 连接

在初始化 PPP 协议层以前, 需要在用户和网络接入服务器 (LAC) 之间建立一个虚连接 (虚电路), 这个虚连接可以是事先由用户和 LAC 配置好参数的永久虚电路 (PVC), 也可以是通过双方的 ATM 信令协商按需建立的交换式虚电路 (SVC)。在这两种方式中, 用户指的是虚拟拨号用户。

在接收来自虚拟拨号用户的交换连接之前, LAC 应当决定是否接受这个呼叫。如果连接是 SVC, LAC 可以根据呼叫建立信息的参数决定。并且为了使用户接入适当的 LNS, LAC 要承担部分的认证工作。

b) 通道建立

如果在 LAC 和指定的 LNS 之间没有通道连接存在, 就需要建立一个通道。在通道建立过程中, LNS 和 LAC 需要彼此指定载体能力和帧能力 (bearer and framing capabilities), 载体能力需要扩展以便于在 LAC 端识别 ATM 设备。它也允许 LNS 使用这个扩展用于支持出呼叫的 ATM。如果双方 (LAC、LNS) 没有就扩展达成一致, 将不能建立通道。

c) 呼叫建立

对于宽频出呼叫和入呼叫, 需要定义一些必要的属性扩展。

对于 OCRQ, LNS 需要指定 LAC 接收和发送流量的最大、最小速率。它允许 ATM 流量双向的不对称性。为了支持 LAC 和用户之间的 UBR 连接, 最小的 BPS 必须设为 0。并且在 OCRQ, LNS 要向 LAC 方指定要求的服务种类, 也就是实时 (rt) 或非实时 (nrt) 传输服务。这些指定的参数 (最大、最小的接收发送速率、要求的服务种类) 使得 LAC 可以根据自己的能力、ATM 接入网能力建立一个合适的 ATM 连接。实时连接是由 CBR 或者 rt-VBR ATM 服务种类提供的; 非实时连接则是由 UBR、nrt-VBR、ABR 或 GFR ATM 服务类型提供的。

另外在 OCRQ 信息中 LNS 必须向 LAC 指出被叫号码 (NSAP 格式)。当被叫号码全为 0 时, LAC 应当察看服务名 AVP 以便于将呼叫捆绑到正确的 PVC。

d) 帧格式转换

用户发给 LNS 的 PPP PDU 通过一个 AAL5 连接发送给 LAC, LAC 根据封装格式去掉 AAL5 特定域, 然后用地址和控制域封装 PPP PDU 以便在 L2TP 通道中传输。

LNS 发给用户的 PPP PDU 也是通过 LAC 和用户之间的 AAL5 连接传送的。LAC 必须去掉标识 L2TP 通道的地址和控制信息然后根据特定封装格式插入 AAL5 指定域。

2) 服务模式

a) 认证

对于 ATM 交换式 VC, 呼叫方号码信息可以作为第一级认证。对于永久虚电路, 因为存在 LAC、LNS 供应商双方的协商一致性, 就无需认证阶段。

b) 授权

因为建立 ATM 连接的复杂性, 从而造成在接收 ATM 连接建立以前就需要一些授权。非授权的访问请求会造成连接释放。

3) 新的和扩展 AVP

a) 新的 AVP 定义

—— 接收的最小 BPS AVP 如图 20 所示。

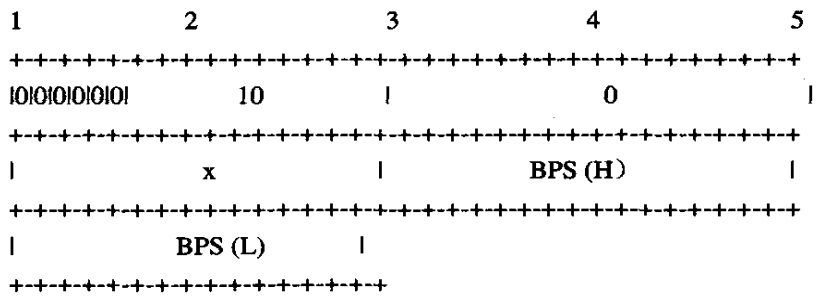


图 20 接收的最小 BPS AVP 示意

接收的最小 BPS AVP 指定在非对称传输中接收方向的最小可接受的线速率。这个 AVP 可以包括在 OCRQ 消息中并且当 LAC 指定 ATM 支持时只能包括在 OCRQ 中。

—— 接收的最大 BPS AVP 如图 21 所示。

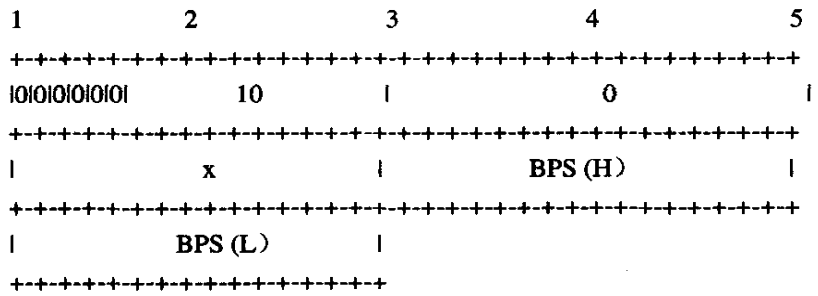


图 21 接收的最大 BPS AVP 示意

接收的最大 BPS AVP 指定在非对称传输中接收方向的最大可接受的线速率。这个 AVP 可以包括在 OCRQ 消息中并且当 LAC 指定 ATM 支持时只能包括在 OCRQ 中。

—— 服务种类 AVP 如图 22 所示。

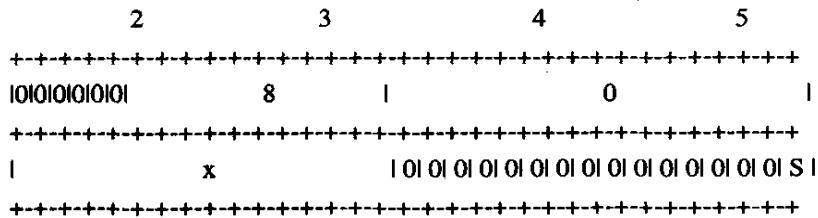


图 22 服务种类 AVP 示意

服务种类 AVP 对于呼叫建立希望的服务质量提供了可选附加信息。S 位指定了是实时的 (S 位是 1)

还是非实时的（S 位是 0）。其他位保留为将来使用。这个 AVP 可以包括在 OCRQ 和 ICRQ 信息中。

—— 服务名 AVP 如图 23 所示。

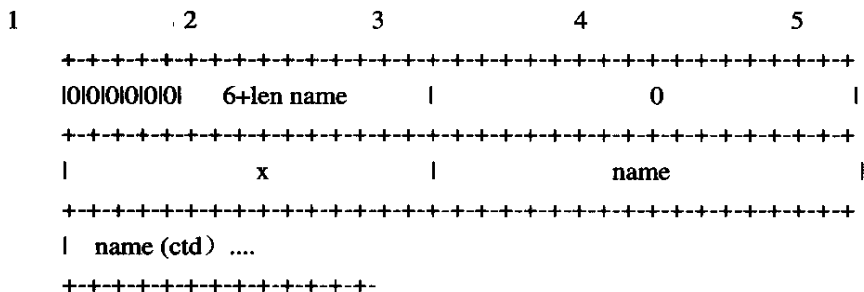


图 23 服务名 AVP 示意

服务名 AVP 仅仅当被叫号码域全为 0 时才被提供,它通过一个文本名得到一个 PVC。这个 AVP 可以包括在 OCRQ 和 ICRQ 信息中。

—— ATM Cause Code AVP 如图 24 所示。

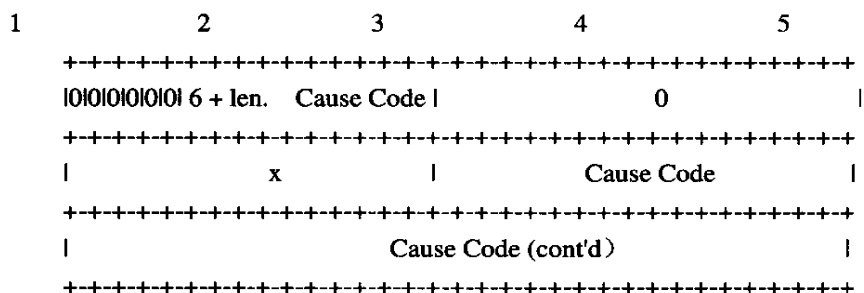


图 24 ATM Cause Code AVP 示意

当 ATM 连接失败时, ATM Cause Code AVP (ATM 原因码 AVP) 指定失败原因。这个 AVP 必须包括在 CDN 信息中。

(2) 改变的 AVP 定义

下面的 AVP 包括在 L2TP 协议中但为了支持 ATM 需要相应的变化。

—— Bearer Capabilities AVP 如图 25 所示。

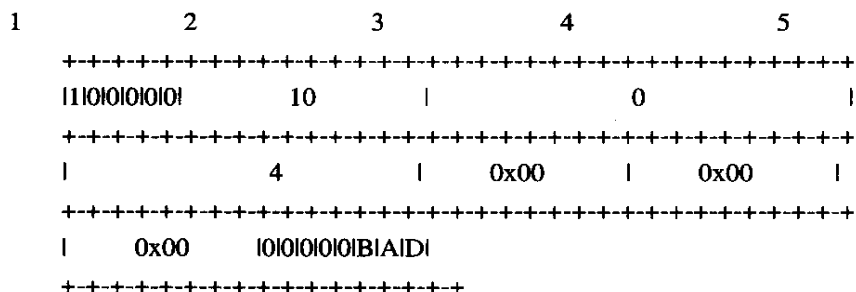


图 25 Bearer Capabilities AVP 示意

载体能力 AVP 包括在一个 SCCRQ 或 SCCRP 消息中, 它指定了发送方所能提供的载体能力: 如果 B 位置位, 支持宽带接入 (ATM); 如果 A 位置位, 支持模拟接入; 如果 D 位置位, 支持数字接入。

—— (Tx)Minimum BPS AVP

发送最小 BPS AVP 指定在发送方向的最小可接受线速率。这个 AVP 可以用在 OCRQ 消息中。如果接收最小 BPS 在这个消息中不存在，这就暗示是对称传输。

发送最小 BPS 的单位是比特/秒 (bit/s)，并且对于 ATM 网络可以被映射成 PCR (peak Cell Rate 峰值信元速率) 单位是信元/秒 (cell/s)。

—— (Tx)Maximum BPS AVP

发送最大 BPS AVP 指定在发送方向的最小可接受线速率。这个 AVP 可以用在 OCRQ 消息中。如果接收最大 BPS 在这个消息中不存在，这就暗示是对称传输。

发送最大 BPS 的单位是比特/秒 (bit/s)，并且对于 ATM 网络可以被映射成 PCR (peak Cell Rate 峰值信元速率) 单位是信元/秒 (cell/s)。

—— 载体类型 AVP 如图 26 所示。

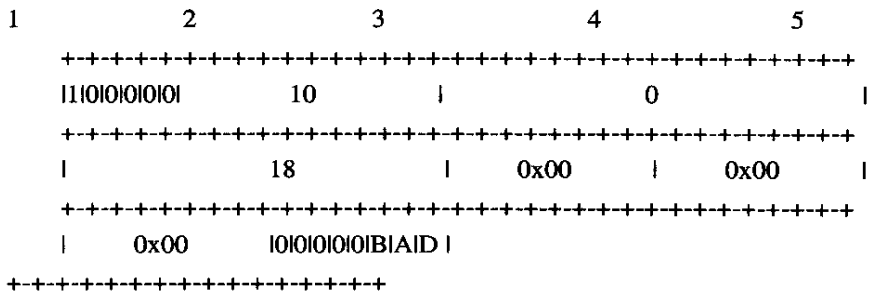


图 26 载体类型 AVP 示意

载体类型 AVP 指定请求呼叫的载体类型，这个 AVP 必须包括在 OCRQ 信息中，可以包括在 ICRQ 消息中。如果 B 位置位，支持宽带接入 (ATM)；如果 A 位置位，支持模拟接入；如果 D 位置位，支持数字接入。

—— Dialed Number AVP 如图 27 所示。

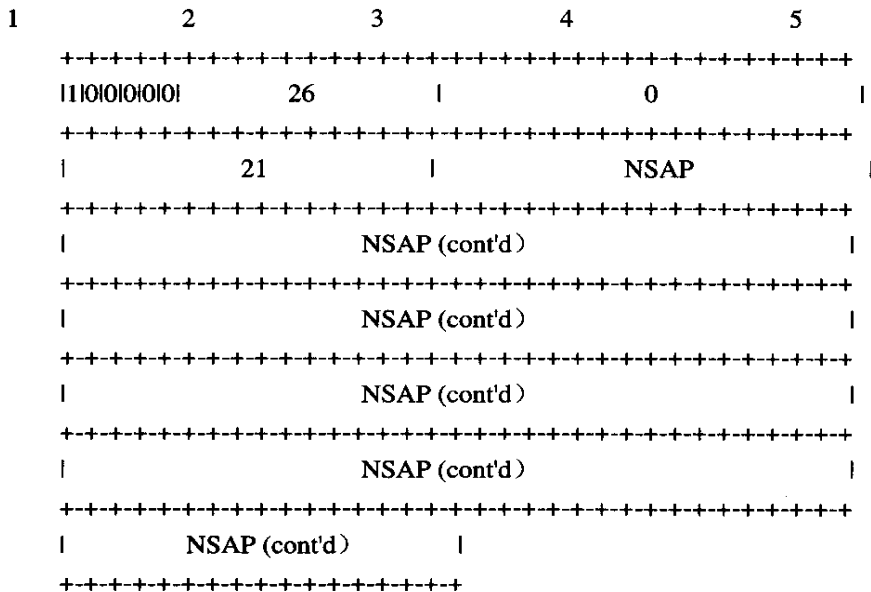


图 27 Dialed Number AVP 示意

被叫号码 AVP 被用来指定虚拟拨入用户的地址，这个 AVP 必须包括在 OCRQ 信息中并且可以包括

在 ICRQ 信息中。当在载体类型 AVP 中 B 位置位时, 被叫号码 AVP 被解释位二进制编码。NSAP 二进制编码地址提供了一个比 ASCII 码更宽范围的地址封装。

如果被叫号码 AVP 全为 0, 则服务名 AVP 提供进一步的消息以便将 L2TP 呼叫捆绑到指定的虚电路连接。

—— Sub-Address AVP

当被叫号码是一个全为 0 的 NSAP 地址时, 子地址 AVP 应当被忽略。

9.6 IPSec 协议 (可选)

IPSec 协议是一组开放的网络安全协议的总称, 提供访问控制、无连接的完整性、数据来源验证、防重放保护、加密以及数据流分类加密等服务。IPSec 在 IP 层提供这些安全服务。

IPSec 协议主要包括:

—— 报文验证头协议 AH (Authentication Header): 该协议主要提供数据来源验证、数据完整性验证和防报文重放功能;

—— 报文安全封装协议 ESP (Encapsulating Security Payload): 该协议在 AH 协议的功能之外再提供对 IP 报文的加密功能;

—— Internet 安全联盟及密钥管理协议 ISAKMP (Internet Security and Key Management Protocol): 该协议提出了一种自动建立安全联盟及管理密钥的方法。

9.6.1 报文验证头协议 (AH)

AH 协议有两种操作模式, 见图 28。

1) 传送模式 (Transport Mode)

传送模式是在 IP 数据包的数据部分运行, 而不是在报头。这个数据部分包含两个主机之间的上层协议 (TCP,UDP)。

2) 隧道模式 (Tunnel Mode)

在另一个数据包中封装了完整的数据包, 该数据包的地址为 IPSec 网关。

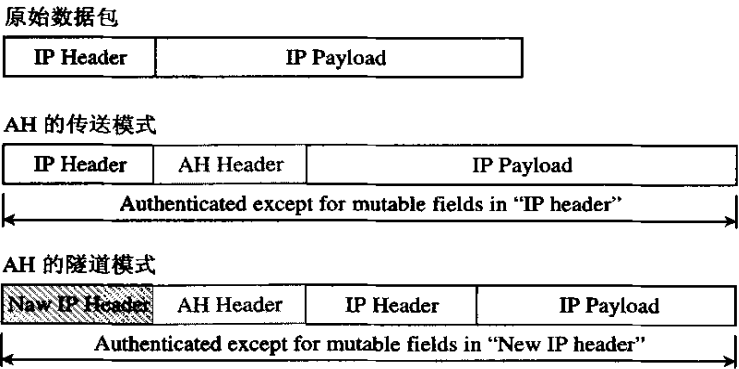


图 28 AH 协议的操作模式

9.6.2 报文安全封装协议 ESP

ESP 与 AH 协议的不同之处在于可以对数据报进行加密, 并且可以实现 AH 的所有功能。

a) ESP 加密算法

ESP 算法采用对称密钥的加密算法, 在国际标准中规定使用 DES 算法。但这与我国的国家密码政策相冲突, 这里暂时将 DES 作为标准算法是为了方便测试及对加密特性的验证, 等待信息产业部和国家密码管理委员会一起确定我国的标准加密算法。

b) ESP 的操作模式

与 AH 协议相同，ESP 也有 2 种操作模式，如图 30 所示。

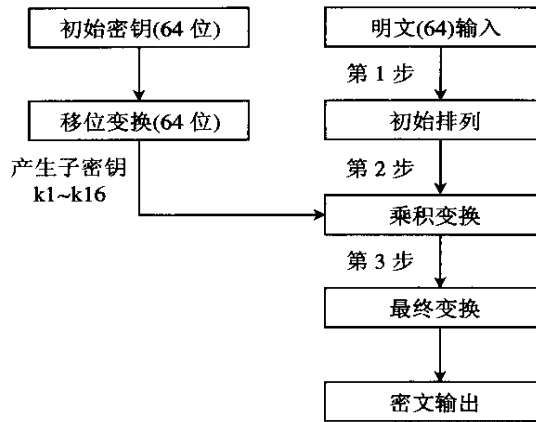


图 29 DES 算法过程图

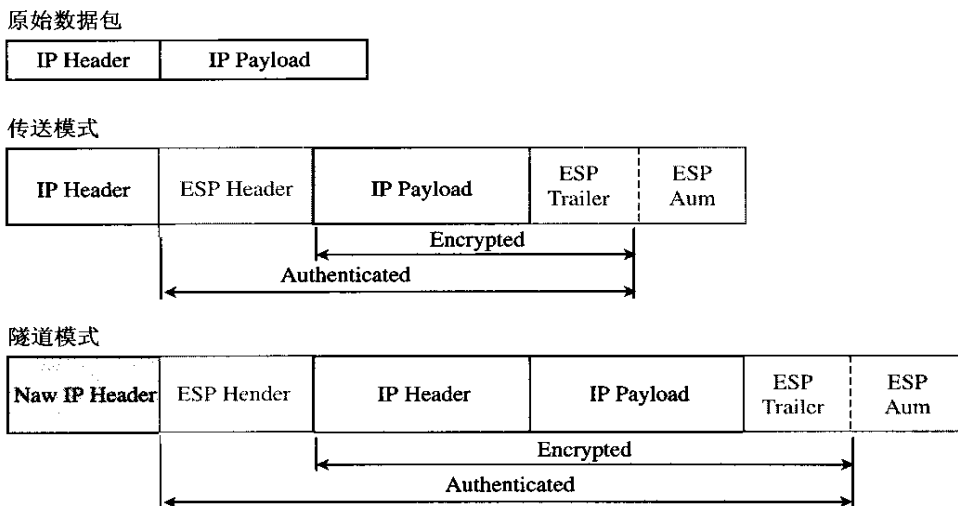


图 30 ESP 的操作模式

1) 传送模式

在该模式下，原始数据包的 IP 头仍然保留，只有原始信息和 ESP Trailer 被加密，原始的 IP 报头不被加密。

2) 隧道模式

在该模式下，产生了一个新的 IP 报头，整个原始数据包和 ESP Trailer 被加密。

IP AH 为上层协议提供认证和数据完整性，同时提供静态值，如版本号，长度，协议和源/终端地址。AH 利用带有 MD5 或 SHA-1 的散列消息认证码（HMAC）在 IP 数据包上进行密码校验和的计算。

MD5 和 SHA-1 可以在可变消息上提供冲突验证值，不需要对等层之间的共享密钥。HMAC 算法使用有密钥的散列功能的密码强度来产生密码校验和。

ESP 提供保密性、数据原始验证，无连接完整性和反重放功能。ESP 使用对称密码算法。每个 ESP 数据包都有用于建立密码同步的必要信息。

与 ESP 一起提供的还有可选的认证功能，该功能使用与 AH 相同的算法。这可以使破坏性数据包在

解密之前被拒绝接受。为防止数据包的重放，ESP 数据包中包含一个序列号码。

9.6.3 Internet 安全联盟及密钥管理协议

IPSec 对数据流最终提供的安全服务通过安全联盟（Security Association）实现。在一个安全联盟中通过使用 AH 或 ESP 协议提供安全服务，但不能在一个安全联盟中同时提供 AH+ESP 的安全服务，即 AH+ESP 的服务必须通过建立两个安全联盟来提供。

安全联盟具有单向性，类似于一条单向“连接”，输入数据流和输出数据流由输入安全联盟和输出安全联盟分别处理。可通过手工配置和自动协商两种方式建立，但都是基于安全策略库生成的。自动协商方式就是由通信双方基于各自的安全策略库经过匹配和协商，最终建立安全联盟。IPSec 的实现必须同时支持这两种方式。

安全联盟由对端地址、协议号和安全参数索引（SPI）组成的三元组唯一标识。

必须支持 IKE 协议实现自动协商方式，建立安全联盟及进行密钥管理。

无论手工方式还是自动方式建立的安全联盟，必须能够通过手工进行删除。

关于 Internet 密钥交换协议（IKE）的要求如下。

IKE 是基于 ISAKMP 架构的密钥协商协议，运行在 UDP 500 号端口上。其作用是可以在不传送密钥的情况下为协商双方生成共享的密钥。IKE 的基本过程是通过一种自保护的手段开始协商一个 ISAKMP SA，然后在 ISAKMP SA 的保护下为 IPSec 协商 SA。IKE 实现的密钥交换提供了身份保护、身份验证、防重放、不可否认性和 PFS 特性等功能。

1) 交换模式

通信双方之间的报文应答称之为交换（Exchange），IKE 就是通过各种交换来实现 SA 协商的。协商 ISAKMP SA 的交换为阶段 1 交换，有主交换模式和主动交换模式两种情况；协商 IPSec SA 的交换为阶段 2 交换，又称之为快速交换模式；另外，还有一些辅助的交换模式，包括信息交换模式和组交换模式。IKE 的实现必须支持主交换模式和快速交换模式，推荐支持信息交换模式和主动交换模式，组交换模式视需要实现。

主交换模式：三对消息完成了策略协商、DH 交换和验证。可以实现完整的 SA 属性协商，同时提供对身份数据保护的机制。第一对消息完成策略协商；第二对消息进行 DH 交换；第三对消息进行验证。不同的验证方法会影响每对消息传送的内容，但不影响整个交换的结构。主交换模式的消息功能如图 31 所示。

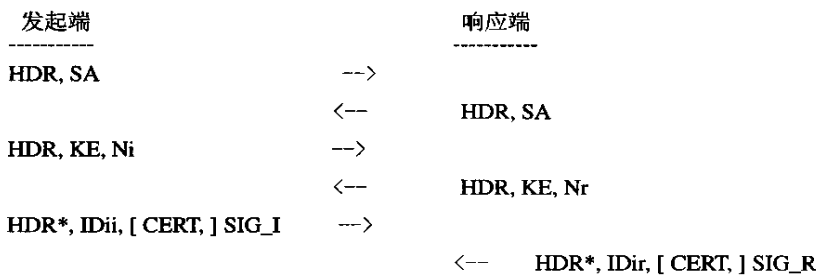


图 31 主交换模式的消息功能

- 其中：
- HDR：数据报头；
 - CERT：认证数据；
 - KE：密钥交换数据；
 - SA：安全联盟数据；
 - Ni：发起端现时的数据；

Nr: 响应端现时的数据;
SIG-I: 发起端的特征数据;
SIG-R: 响应端的特征数据;
IDii: 发起端的标识;
IDir: 响应端的标识。

主动交换模式以更少的消息完成交换: 前两条消息协商了策略, 进行了 DH 交换, 交换身份数据; 第二和第三条消息完成了验证。但由于消息结构的改变, 有些属性无法协商, 而且不能对身份数据进行保护。主动交换模式的消息功能如图 32 所示。

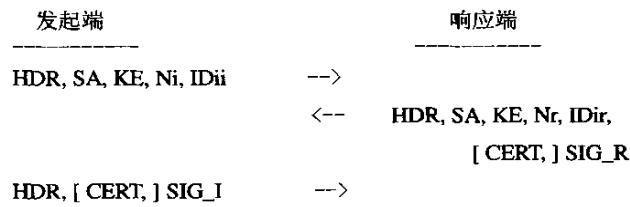


图 32 主动交换模式的消息功能

快速交换模式由非 ISAKMP 的 SA (如: IPSec SA) 完成策略协商和派生密钥, 快速模式不能单独使用, 必须是在阶段 1 交换成功之后使用, 利用 ISAKMP SA 进行加密保护。一次 SA 的协商同时建立了两个 SA, 分别对应于入报文 (Inbound Traffic) 和出报文 (Outbound Traffic)。快速模式交换同时支持多 SA 的协商。

信息交换模式用于在通信双方之间传递一些简单的信息, 如一端的 SA 删除时, 可通知对端也将相应的 SA 删除。信息交换在阶段 1 之前或之后进行均可, 但在阶段 1 之前进行的话则为明文传送。并且它是一种单向的报文, 即接收方不产生应答报文, 发起方也没有重传机制。

在阶段 1 的 DH 交换中, 需要用到 DH 组, 一般使用公开的 DH 组, 而在安全性要求非常高的场合, 组交换模式可以为用户协商建立私有的 DH 组, 同时具有隐藏组信息的功能。组交换模式在阶段 1 交换成功之后使用。

2) 数据流分类信息协商

在阶段 2 的快速交换模式中, IKE 必须支持数据流分类信息协商。

协商的发起方将希望进行安全通信的数据流信息作为快速交换模式中的身份数据发送, 接收方根据身份数据和本地配置检查是否要对此数据流进行保护, 如果是则进行策略匹配建立安全联盟, 从而实现 IPSec 的数据流分类加密。其中, 传递的数据流分类信息至少要包括触发协商的 IP 报文中的源、目的地址信息。

3) 身份验证与数据验证

身份验证用于验证协商对端身份的真实性, 而数据验证可保证协商过程中交换的报文的完整性。验证方法包括: 共享验证字 (Pre-shared Key) 验证、数字签名 (Digital Signature) 验证、公钥加密 (Public Key Encryption) 验证等。作为基本的手段, 共享验证字的验证方法必须实现。

4) 加密算法与验证算法

IKE 所使用的加密算法必须实现 DES, 验证算法必须实现 MD5、SHA。

5) DH 组

RFC2409 中规定了 4 种公开的 Oakley DH 组，在 IKE 中至少要实现其中的 Group 1，其表达式为： $2^{768} - 2^{704} - 1 + 2^{64} * \{ [2^{638} \text{pi}] + 149686 \}$

可以用 16 进制表示为：

```
FFFFFFFF FFFFFFFF C90FDAA2 2168C234 C4C6628B 80DC1CD1
29024E08 8A67CC74 020BBEA6 3B139B22 514A0879 8E3404DD
EF9519B3 CD3A431B 302B0A6D F25F1437 4FE1356D 6D51C245
E485B576 625E7EC6 F44C42E9 A63A3620 FFFFFFFF FFFFFFFF
```

其发生器为 2。

其余的推荐实现。在安全性要求很高的场合，可使用组交换模式协商私有的 DH 组。

6) PFS

IKE 可以实现密钥和身份数据的 PFS 特性。密钥的 PFS 通过交换过程的 DH 交换得以实现，对于非 ISAKMP SA 的密钥只需要在快速模式中完成 DH 交换。而对于要实现身份数据的 PFS，必需在建立了阶段 2 的 SA 后删除阶段 1 的 ISAKMP SA。PFS 的实现视应用情况而定。

7) 身份数据

在 IKE 的协商过程中，身份数据 (ID) 有以下几个作用：

- 标识安全隧道，对不同的数据流，将数据送入相应的安全隧道；
- 协商时，接收方根据发起方的身份数据检查本地策略，建立相应的安全隧道。

阶段 1 的 ID 数据应是协商双方的 IP 地址。阶段 2 的 ID 数据缺省时也是协商双方的 IP 地址，发起方还包括数据流信息。如果阶段 2 协商是客户模式的（为用户协商的安全联盟），其传送的应该是用户的 ID 数据。阶段 2 协商必需实现和支持类型为 ID_IPV4_ADDR 的 ID 数据。

8) 安全联盟的生存时间与更新

安全联盟的生存时间 (Lifetime) 是需要协商的一个参数。当协商双方配置的 Lifetime 不一致时，协商的应答方可能选择接受、拒绝或选择最小者。建议应答方选择最小的 Lifetime 作为安全联盟的生存时间。建议 IKE 阶段 1 的 Lifetime 配置在 300~86400s 之间。

安全联盟的 Lifetime 到时，旧的安全联盟需要被新协商的安全联盟替代。建议在 lifetime 超时之前完成新的安全联盟的协商，保证安全联盟的更新过程不影响安全隧道的通信。

9.7 RADIUS 协议

参见标准 YD/T 1045-2000 网络接入服务器 (NAS) 技术规范 8.5 节。

9.8 Telnet 协议

参见标准 YD/T 1045-2000 网络接入服务器 (NAS) 技术规范 8.5 节。

9.9 SNMP 协议

参见标准 YD/T 1045-2000 网络接入服务器 (NAS) 技术规范 8.6 节。

10 性能和技术指标

10.1 设备容量

小容量级的要求如下：

系统交换容量位于 2~9.9Gbit/s 之间；

最少可以同时支持 1000 个活动会话；

最少配置 5000 个用户；

最少配置 100 个 L2TP 隧道。

中大容量级要求如下:

系统交换容量 $\geq 10\text{Gbit/s}$;

最少可以同时支持 10000 个活动会话;

最少配置 50000 个用户;

最少配置 5000 个 L2TP 隧道。

10.2 处理能力

PPP 的平均建链时间 $< 5\text{ s}$ (含 RADIUS 认证时间)。

每秒同时建链数 $>$ 设备端口数的 10%。

包转发能力至少达到 1Mpack/s 以上。

10.3 服务质量

1) 用户优先级

支持多用户优先级,用户优先级至少 4 级。

2) 带宽管理

支持每端口、每 VC 的带宽管理,可以设置每端口、每 VC 的接收和发送速率,并对每端口、每 VC 的接受包、发送包和包丢失率进行统计。

3) 接口转发时延

在最坏情况下, 1518B 长度及以下的包时延均应 $< 1\text{ms}$ 。

10.4 用户接入认证技术指标

参见 YD/T 1045-2000《网络接入服务器(NAS)技术规范》中 6.3 节。

10.5 可靠性、可用性要求

1) 系统必须达到 99.99% 的可用性。

2) 无故障连续工作时间

系统的无故障工作时间: $\text{MTBF} > 10000\text{h}$ 。

3) 故障恢复时间

系统故障恢复时间 $< 1\text{h}$ 。

4) 控制和数据通道必须分开。

5) 对电信级网络接入服务器的要求

要求设备具有高可靠性和高稳定性。主处理器、主存、交换矩阵、电源、总线仲裁器和管理接口等要求热冗余备份。线路卡要求 $m+n$ 备份并提供远端测试诊断功能。

11 环境要求

11.1 温度、湿度条件

a) 长期工作条件: 温度保持 $15\sim 30^{\circ}\text{C}$, 相对湿度保持 40%~65%。

b) 短期工作条件: 温度保持 $0\sim 45^{\circ}\text{C}$, 相对湿度保持 20%~90%。

注:

1) 宽带网络接入服务器的正常工作的温度和相对湿度的测量点指在地板以上 2m 和接入服务器前方 0.4m 处测量值。

2) 短期工作条件系指连续不超过 48h 和每年累计不超过 15 天。

3) 相对湿度低于 20% 的环境应采用防静电地面。

11.2 防尘要求

机房内直径大于 $5\mu\text{m}$ 的灰尘浓度应 $\leq 3 \times 10^4$ 粒/ m^3 ; 灰尘粒子应是非导电、非导磁和非腐蚀性的。

11.3 防电磁干扰要求

宽带网络接入服务器产生的电磁干扰应满足以下要求。

a) 由接入服务器射出的无线电电磁干扰应符合表 2 的规定。

表 2 由接入服务器发射的无线电电磁干扰的要求

频率 (MHz)	电磁强度 dB(μ V/m)	频率 (MHz)	电磁强度 dB (μ V/m)
0.01~0.024	$148.6-60\lg d$	$47.7/d-88$	$59.1-20\lg d$
0.024~0.8	$116.2-60\lg d-20\lg f$	88~216	$63.6-20\lg d$
0.8~1.59	$118.2-60\lg d$	2160~10000	$66.6-20\lg d$
1.59~47.7/d	$120.2-60\lg d-40\lg f$		
注:			
1 d 为测试天线与靠近被测物间水平距离; 单位为 m, d 限于 30m 内。			
2 f 为频率, 以 MHz 为单位。			
3 dB (μ V/m) 表示以微伏 (μ V/m) 为参考单元的分贝数。			

b) 由接入服务器进入交流馈电线的无线电电磁干扰应符合表 3 的规定。

表 3 由接入服务器进入交流馈电线的天线电电磁干扰的要求

频率 (MHz)	最大线路电流 (dB μ A)
0.000061~0.001	$I-20\lg f-84.4$
0.001~0.01	$(124.4-I)\lg f+348.8-2I$
0.01~0.8	$-21.05\lg f+57.9$
0.8~100	60
注:	
1 f 为频率, 以 MHz 为单位。	
2 I 为接入到交流电源处的输入线路电流电平。	
3 dB μ A 表示以微安 (μ A) 为参考单元的分贝数。	

c) 由接入服务器进入直流馈线和信号线的无线电电磁干扰应符合表 4 的规定。

表 4 由接入服务器进入直流馈线和信号线的无线电电磁干扰要求

频率 (MHz)	最大线路电流 (dB μ A)
0.01~0.8	$-21.05\lg f+57.9$
0.8~100	60

11.4 抗电磁干扰的能力

宽带网络接入服务器在受到 0.01~1000MHz 频率范围内电场强度为 140dB (μ V/m) 的外界电磁干扰时应不出现故障和性能下降。

在直流或交流电源线受到表 5 所示, 0.01~100MHz 频率范围的外界电磁干扰电流时应不出现故障和性能下降。

表 5 外界电磁干扰的要求

频率 (MHz)	最大线路电流 (dB μ A)
0.01~0.8	$-21.05\lg f+67.9$
0.8~100	70

12 电源与接地

12.1 电源

a) 直流电压及其波动范围要求

额定电压：为 -48V 的直流电源。

电压波动范围：在直流输入端子处测量 -48V 电压允许变动范围为 $-57 \sim -40\text{V}$ 。宽带网络接入服务器在此范围内应工作正常。

b) 杂音电压指标

在直流配电盘输出端子处测量的限值如下：

$300 \sim 3400\text{Hz}$ ，杂音电压 $\leq 2\text{mV}$ 。

$0 \sim 300\text{Hz}$ ，峰值杂音电压 $\leq 4\text{mV}$ 。

$3.4 \sim 15\text{kHz}$ ，宽带杂音电压 $\leq 100\text{mV}$ 有效值。

$150\text{kHz} \sim 30\text{MHz}$ ，宽带杂音电压 $\leq 30\text{mV}$ 有效值。

c) 离散频率杂音电压

$3.4 \sim 15\text{kHz}$ ， $\leq 5\text{mV}$ 有效值。

$150 \sim 200\text{kHz}$ ， $\leq 3\text{mV}$ 有效值。

$200 \sim 500\text{kHz}$ ， $\leq 2\text{mV}$ 有效值。

$500 \sim 2\text{MHz}$ ， $\leq 1\text{mV}$ 有效值。

d) 交流电压及其波动范围要求

单相 $220\text{V} \pm 10\%$ ，频率 $50\text{Hz} \pm 5\%$ 。

线电压波形畸变率 $< 5\%$

12.2 接地要求

a) 接地方式应符合工作地、保护地和建筑防雷接地公用一组接地体的联合接地方式。

b) 接地线面积。

接地线截面积根据可能通过的最大电流负荷确定。应采用良导体导线，不能使用裸导线布放。

接地电阻值：联合接地的电阻值应 $< 3\Omega$ 。

13 例行试验

13.1 低温试验

应符合 GB2423.1 的要求。

13.2 高温试验

应符合 GB2423.2 的要求。

13.3 恒定湿热试验

应符合 GB2423.9 的要求。

13.4 运输试验

宽带网络接入服务器按包装文件要求完整包装后，置于载重汽车中后部，在三级公路上以 $25 \sim 40\text{km/h}$ 的速度行驶 200km 后，包装箱应完好无损。开箱检查宽带网络接入服务器无机械损伤，紧固件无松脱，接通电源，开机工作应符合质量要求。

13.5 贮存要求

产品的贮存要求应符合 GB3873 的有关规定。

13.6 标志、包装、运输和贮存

13.6.1 产品标志

在产品适当位置应有铭牌，铭牌的形式和尺寸应符合相关标准的规定。

13.6.2 包装标志

外包装应有包装贮运图示标志，应按 GB191 有关规定执行。

13.6.3 包装

随机文件：包括产品合格证、使用说明书和产品随机备附件清单。

产品包装要求：应符合 GB3873 的有关规定。

13.6.4 运输

产品可由火车、汽车、飞机和轮船等运输，但在运输过程中必须有遮蓬，不应有剧烈的震动和撞击，并按包装箱上标明方向放置。
