YD

中华人民共和国通信行业标准

YD/T 1148-2005

代替 YD/T 1148-2001

网络接入服务器技术要求
——宽带网络接入服务器

Technical requirements of network access server
——Broadband Network Access Server(BNAS)

2005-05-11 发布　　2005-11-01 实施

中华人民共和国信息产业部　发布

目　　次

前　言

本标准是网络接入服务器系列标准之一，该系列标准名称及结构如下：

1. YD/T 1045-2000 网络接入服务器技术规范
2. YD/T 1075-2000 网络接入服务器测试方法
3. YD/T 1265-2003 网络接入服务器测试方法——宽带网络接入服务器
4. YD/T 1148-2005 网络接入服务器技术要求——宽带网络接入服务器

本标准是 YD/T 1265-2005 网络接入服务器测试方法——宽带网络接入服务器的配套标准。

本标准代替 YD/T 1148-2001 网络接入服务器技术要求——宽带网络接入服务器。

本标准与 YD/T 1148-2001 相比主要变化如下。

1. 在第 2 章“规范性引用文件”中增加和更新了以下引用文件：

1）增加 YD/T 1177-2002 IP 组播路由协议；
2）增加 RFC 1938（1996）A One-Time Password System 一次性口令系统；
3）RADIUS 协议由 RFC 2138 更新为 RFC 2865（2000）RADIUS 协议；
4）RADIUS 计费协议由 RFC 2139 更新为 RFC 2866（2000）RADIUS 计费协议；
5）增加 RFC 2869（2000）RADIUS 扩展协议；
6）增加 RFC 2284（1998）PPP 可扩展认证协议；
7）增加 RFC 1112（1989）IGMPv1 协议；
8）增加 RFC 2236（1997）IGMPv2 协议；
9）增加 IEEE Std 802.1x（2001）基于端口的网络接入控制；
10）增加 YD/T 1190-2002 基于网络的虚拟 IP 专用网（IP-VPN）框架；
11）增加 IETF RFC 1349（1992）Internet 协议组中的服务类型；
12）增加 IETF RFC 3046 （2001）DHCP 代理信息选项。

2. 在第 3 章“定义”中修改了以下内容：

1）增加认证者（Authenticator）的定义；
2）增加对等实体（Peer）的定义。

3. 在第 4 章“缩略语”中修改了以下内容：

1）增加 AC （Attachment Circuit）附加电路；
2）增加 ACL （Access Control List）访问控制列表；
3）增加 DHCP（Dynamic Host Configuration Protocol）动态主机配置协议；
4）增加 DSCP（Differentiated Service Code Point）差别服务代码点；
5）增加 EAP（Extensible Authentication Protocol）可扩展认证协议；
6）增加 EAPoL（EAP over LANs）局域网承载的 EAP；
7）增加 GE（Gigabit Ethernet）千兆位以太网；
8）增加 PAE（Port Access Entity）；
9）增加 IGMP（Internet Group Management Protocol）互联网组管理协议；
10）增加 OTP（One Time Password）一次性口令；
11）增加 PAE（Port Access Entity）端口接入实体；
12）增加 Port（Network Access Port）网络接入端口；
13）增加 PW（Pseudo Wire）伪线路；
14）增加 QoS（Quality of Service）服务质量；

15）增加 SMC（Service Management Center）业务管理中心；

16）增加 TCP（Transfer Control Protocol）传输控制协议；

17）增加 TOS（Type Of Service）服务类型；

18）增加 UDP（User Datagram Protocol）用户数据报协议；

19）增加 VLL（Virtual Leased Line）虚拟租用线；

20）增加 VPLS（Virtual Private LAN Segments）虚拟专用 LAN 网段；

21）增加 VPRN（Virtual Private Routed Network）虚拟专用路由网；

22）增加 VS（Virtual Switch Instance）虚拟交换实例。

4. 在第 5 章“设备功能”中修改以下内容：

1）5.3.1 中宽带网络接入服务器在接入侧 ATM 功能接口由必选改为可选；

2）5.3.1 中宽带网络接入服务器在接入侧增加 1000Mbit/s 以太网接口（可选）；

3）5.3.2 中接入侧的通信协议增加了 EAP 协议（可选）、802.1x（可选）、IGMP 协议（可选）；

4）5.3.2 中网络侧的通信协议 L2TP 由必选改为可选；

5）5.3.2 中网络侧的通信协议部分增加如果 BNAS 不支持规定的路由协议，则使用静态路由；

6）5.3.2 中网络侧的通信协议增加了扩展 RADIUS 协议（可选）、IGMP 协议（可选）；

7）5.3.4 增加了增加对 EAP 协议和 RADIUS 协议，以及用户优先级和认证的规定；

8）5.3.4 对集中的接入认证与授权、计费和统计功能增加了更详细的描述，以及增加了用户权限下发和 RADIUS 计费缓存；

9）将 5.3.6 修改为 DHCP Relay，增加 DHCP Relay 和防攻击。在支持 DHCP Relay 的情形下建议支持 DHCP Option 82；

10）增加了 5.3.7 节“VPN 功能”，将旧版本中的 IP 安全网关功能合并至 5.3.7.5 并增加虚拟专用 LAN 网段 VPLS（可选），虚拟专用拨号网 VPDN（可选），虚拟专用路由网 VPRN（可选），5.3.7 中还增加了可选支持 VPN 按流量计费的功能；

11）将旧版中的 5.3.7 节修改为 5.3.8 节“网管接口功能部分”，删除用户访问的平均时长、用户访问的平均费用、日均用户曲线，月均用户曲线；

12）将旧版中的 5.3.8 节修改为 5.3.9 节，并将设备的监控和管理功能部分的拨号接入改为 Telnet；

13）增加了 5.3.10 组播功能，在该节中增加对组播功能的描述，要求 BNAS 支持 IGMP Proxy 和用户组播数据流的复制分发，可选支持组播计费功能和权限控制。

5. 在第 7 章“通信流程”中删除了 7.1.3 中的用户上网流程的范例。

6. 在第 9 章“协议要求”中修改了以下内容：

1）9.5 L2TP 协议由必选改为可选；

2）增加 9.5.1 L2TP over UDP/IP/Ethernet（可选）；

3）增加 9.10 EAP 协议（可选）；

4）增加 9.11 扩展 RADIUS 协议（可选）；

5）增加 9.12 IGMP 协议（可选）；

6）增加 9.13 802.1x 认证（可选）。

7. 在第 10 章“性能和技术指标”中修改以下内容：

1）10.1 设备容量的划分进行了修改；

2）10.2 对处理能力进行了修改；

3）10.3 服务质量中对用户的优先级定义进一步明确化；

4）增加 10.3.1 服务质量（QoS）定义；

5）10.3.2 流量分类以及优先级服务；

6）10.3.3 接入带宽控制及保证；

7）服务质量增加 10.3.7 用户访问控制权限的规定；

8）服务质量增加 10.3.4 拥塞的避免和管理的规定；

9）增加 10.3.5 QoS 监控；

10）增加 10.3.6 QoS 性能指标；

11）用户接入认证技术指标增加了 EAP 认证和 RADIUS 扩展的支持（可选）；

12）10.4 用户接入认证技术指标增加对于 PPPoE 实现，认证可在 PPP 层实现，或者在 Ethernet 层以 802.1x 方式实现的规定；

13）为了保证用户安全，10.4 用户接入认证技术指标增加对于 LAN 接入提供 IP+VLAN+MAC 绑定；对于 ADSL 接提供 IP+VC+MAC 绑定；

14）对 10.4 用户计费技术指标进行修改，规定了用户计费时长精度，用户计费相对流量精度，绝对流量精度和用户计费差错率；

15）10.4 增加了 RADIUS 负荷分担（可选）；

16）10.5 删除可靠性部分，线路卡 m+n 备份删除。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：上海贝尔阿尔卡特股份有限公司
中国电信集团公司
中兴通讯股份有限公司
武汉邮电科学研究院
华为技术有限公司

本标准主要起草人：姚亦峰　于洪斌　顾方方　张　涛　黄　兵　余少华

网络接入服务器技术要求
——宽带网络接入服务器

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。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB 191–2000	包装储运图示标志
GB/T 2423.1–2001	电工电子产品环境试验 第2部分：试验方法 试验A：低温
GB/T 2423.2–2001	电工电子产品环境试验 第2部分：试验方法 试验B：高温
GB/T 2423.9–2001	电工电子产品环境试验 第2部分：试验方法 试验Cb：设备用恒定湿热
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
YD/T 1177–2002	IP组播路由协议
YD/T 1190–2002	基于网络的虚拟IP专用网（IP–VPN）框架
YDN 099–1998	SDH技术体制
IETF RFC 0768（1990）	UDP协议
IETF RFC 0791（1990）	IP协议
IETF RFC 0792（1990）	ICMP协议
IETF RFC 0793（1990）	TCP协议
IETF RFC 0854（1990）	Telnet协议
IETF RFC 0855（1990）	Telnet协议选项规范
IETF RFC 0858（1990）	Telnet抑制前进选项
IETF RFC 0894（1990）	在以太网上传输IP数据包的标准
IETF RFC 1112（1989）	IGMPv1协议
IETF RFC 1144（1992）	低速串行链路上的TCP/IP头的压缩算法（SLHC协议）
IETF RFC 1155（1990）	基于TCP/IP的互连网管理信息的结构和标识
IETF RFC 1157（1990）	简单网络管理协议（SNMP）
IETF RFC 1213（1991）	基于TCP/IP的互连网的网络管理信息库：MIB–II
IETF RFC 1321（1992）	MD5算法
IETF RFC 1332（1992）	IPCP协议
IETF RFC 1334（1992）	PAP协议
IETF RFC 1349（1992）	Internet 协议组中的服务类型
IETF RFC 1483（1993）	AAL5上的多协议封装

IETF RFC 1490（1993） 帧中继 上的多协议封装
IETF RFC 1631（1994） IP 网络地址转换器（NAT）
IETF RFC 1661（1994） PPP 协议
IETF RFC 1662（1994） 在类 HDLC 帧中的 PPP 协议
IETF RFC 1938（1996） 一次性口令系统
IETF RFC 1973（1996） 帧中继中的 PPP
IETF RFC 1990（1996） PPP 多链协议
IETF RFC 1994（1996） CHAP 协议
IETF RFC 1994（1996） 网络互连设备的性能测试方法
IETF RFC 2236（1997） IGMPv2 协议
IETF RFC 2284（1998） PPP 可扩展认证协议
IETF RFC 2328（1998） OSPF v2 协议
IETF RFC 2364（1998） PPP over AAL5
IETF RFC 2453（1998） RIP v2 协议
IETF RFC 2516（1999） 传输 PPPoE 之方法
IETF RFC 2615（1999） PPP over SONET/SDH 协议
IETF RFC 2661（1999） L2TP 协议
IETF RFC 2865（2000） RADIUS 协议
IETF RFC 2866（2000） RADIUS 计费协议
IETF RFC 2869（2000） RADIUS 扩展协议
IETF RFC 3046 （2001） DHCP 代理信息选项
IEEE Std 802.1x 基于端口的网络接入控制
ITU-T Q.2931 宽带综合业务数字网（B-ISDN）——No.2 数字用户信令系统——用于基本呼叫/连接控制的用户网络接口第三层规范

3 定义

下列定义适用于本标准。

3.1

网络接入服务器 Network Access Server（NAS）

网络接入服务器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。

3.2

宽带网络接入服务器 Broadband Network Access Server（BNAS）

宽带网络接入服务器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 *x*DSL/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。

3.3

认证者 Authenticator

链路上需要进行认证的一端。认证者指定在链路建立阶段所使用的认证协议。

3.4

对等实体 Peer

点对点的链路上的另一端，即被认证者进行认证的一端。

4 缩略语

下列缩略语适用于本标准。

AC	Attachment Circuit	附加电路
ACL	Access Control List	访问控制列表
ADSL	Asymmetric Digital Subscriber Line	非对称数字用户线
ATM	Asynchronous Transfer Mode	异步传递模式
BGP	Bounder Gateway Protocol	边界网关协议
CMTS	Cable Modem Termination Systems	Cable Modem 端接系统
DDN	Digital Data Network	数字数据网
DHCP	Dynamic Host Configuration Protocol	动态主机配置协议
DSCP	Differentiated Service Code Point	差别服务代码点
EAP	Extensible Authentication Protocol	可扩展认证协议
EAPoL	EAP over LANs	局域网承载的 EAP
FR	Frame Relay	帧中继
GE	Gigabit Ethernet	千兆位以太网
IGMP	Internet Group Management Protocol	互联网组管理协议
IPSec	IP Security Protocol	IP 网络安全协议
ISDN	Integrated Service Digital Network	综合业务数字网
L2TP	Layer 2 Tunneling Protocol	第二层隧道协议
LAN	Local Area Network	局域网
LL	Leased Line	租用线路
MP	Multi-link PPP	PPP 多链路协议
OSPF	Open Shortest Path First Protocol	最短路径优先开放协议
OTP	One Time Password	一次性口令
PAE	Port Access Entity	端口接入实体
PPP	Point to Point Protocol	点到点协议
PPPiFR	PPP in Frame Relay	帧中继承载的 PPP
PPPoA	PPP over AAL5	AAL5 承载的 PPP
PPPoE	PPP over Ethernet	以太网承载的 PPP
PSTN	Public Switched Telephone Network	公共交换电话网
PW	Pseudo Wire	伪线路
QoS	Quality of Service	服务质量
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
SMC	Service Management Center	业务管理中心
SNMP	Simples Network Management Protocol	简单网络管理协议
TCP	Transfer Control Protocol	传输控制协议
TOS	Type Of Service	服务类型
UDP	User Datagram Protocol	用户数据报协议
VLL	Virtual Leased Line	虚拟租用线
VPDN	Virtual Private Dial Network	虚拟专用拨号网
VPLS	Virtual Private LAN Segments	虚拟专用 LAN 网段

VPN	Virtual Private Network	虚拟专用网
VPRN	Virtual Private Routed Network	虚拟专用路由网
VS	Virtual Switch Instance	虚拟交换实例

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。

宽带网络接入服务器的参考结构如图 1 所示。

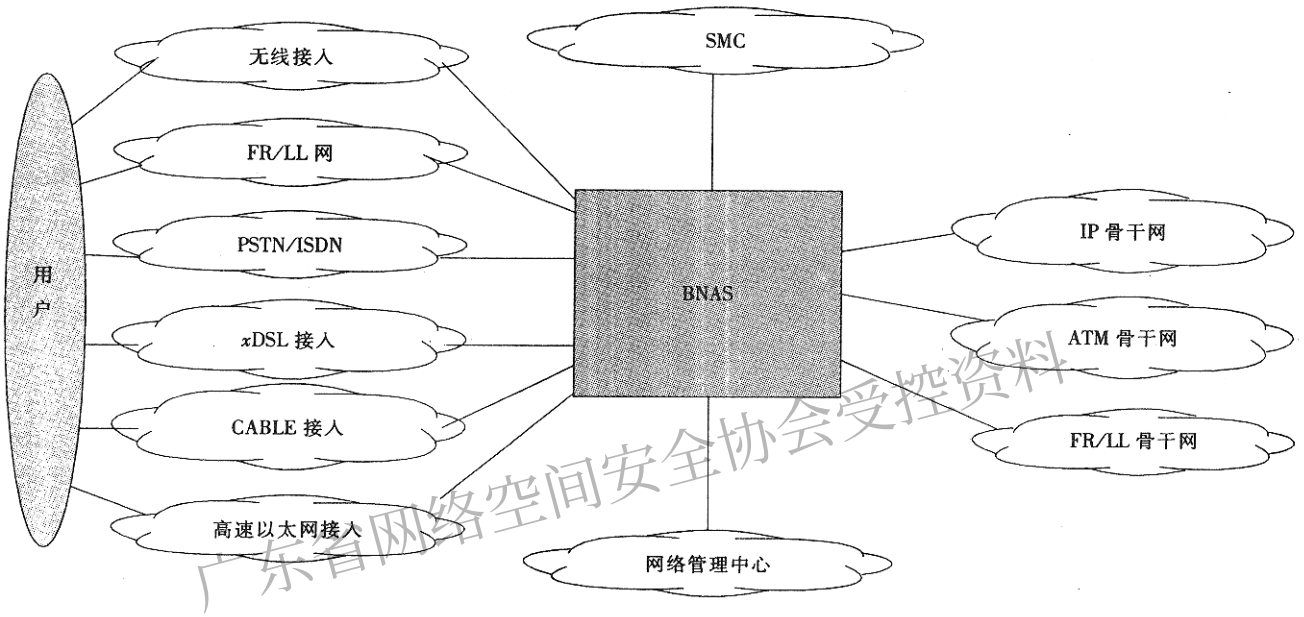


图 1 宽带网络接入服务器的参考结构

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、*x*DSL/接口接入、CABLE 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、千兆比以太网接口及 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、IEEE 802.3/IEEE 802.3u/IEEE 802.3z）和网络侧通信协议（例如，TCP/IP、IEEE 802.3z、IP over SDH/IP over WDM、L2TP 和 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 3 种途径，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（可选）

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 *x*DSL 接入设备的接口，功能是终结或中继 *x*DSL 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、远程接入服务器、无线接入局端设备等的接口。

3）E1 接口（可选）

宽带网络接入服务器的 E1 接口，主要是指与 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，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，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。

5）1000Mbit/s 以太网接口（可选）

宽带网络接入服务器的 1000Mbit/s 以太网接口，主要是指与远程接入服务器、无线接入局端设备、CABLE Modem 接入的 CMTS 等的接口。

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。

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）千兆比以太网接口（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比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 和 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有：

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）；
i）EAP 协议（可选）；
j）802.1x（可选）；
k）IGMP 协议 （可选）。

2）网络侧的通信协议

a）LAN 协议（IEEE 802.3z）；
b）L2TP 协议（可选）；
c）IP over SDH 协议（RFC 2615）；
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），如果 BNAS 不支持上述路由协议，则使用静态路由；
h）接入认证协议 RADIUS；
i）扩展 RADIUS 协议（可选）；
j）网管协议 SNMP；
k）Telnet 协议；
l）IGMP 协议（可选）。

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，保证对用户协定的服务质量。

5.3.4 集中的接入认证与授权、计费和统计功能

宽带网络接入服务器应能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 *x*DSL 用户可采取虚拟拨号方式进行类似于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。

宽带网络服务器应能够设置不同的访问控制策略对用户的接入进行控制。例如，宽带网络服务器可以根据用户上网时长、带宽、用户优先级、业务支援的使用授权状况等对用户实施接入控制。在进行接入控制的时候，宽带网络接入服务器可以结合不同的接入控制等级选择不同的认证协议对用户进行身份认证。

为了增强系统安全性，宽带网络接入服务器应支持 EAP 协议（可选）和 RADIUS 扩展协议（可选），从而可以根据不同的安全性要求选择不同安全等级的认证协议来对不同的用户连接进行接入认证。

宽带网络接入服务器应支持不计费、按时长计费、按流量计费和预付费功能。

计费功能包括以下几个方面：

1）基于时长的预付费（必选）

BNAS 应具有基于时长的预付费功能，支持由计费服务器在认证响应报文中下发的标准属性 Session_Timeout（27），以 s 为计费单位。当剩余时长耗尽，BNAS 应主动切断用户连接，同时上报用户计费信息。

2）基于流量的预付费（可选）

BNAS 可以支持基于流量的预付费功能，支持由计费服务器在认证响应报文中下发的扩展私有属性，

单位为 kByte。当用户剩余流量耗尽，BNAS 应该主动切断用户连接，同时上报用户计费信息。

3）卡号漫游（建议）

建议 BNAS 支持预付费卡号在宽带网中的漫游功能。

4）一卡通（可选）

BNAS 可以支持一个卡号既可以用于宽带上网业务，也可用于窄带语音业务。

5）支持 VPN 用户时长和流量计费（可选）

BNAS 若支持 VPN 则可以针对不同 VPN 实施不同的计费方式，并支持将拨入的 VPN 用户的时长和流量进行统计，并上报计费服务器。实现对 VPN 用户的计费管理。上报的计费属性同上。

6）RADIUS 计费缓存（可选）

当计费服务器发生故障后，如果没有备用的计费服务器，应该要求 BNAS 可以进行一定话务量的缓存，使得用户的计费信息不会丢失。当计费服务器故障排除后，BNAS 能够将缓存的计费信息发送到计费服务器，此时才清除缓存中的用户计费信息。计费缓存的信息存储空间宜大于最大并发用户数的计费信息存储空间。

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，相应路由器则确定对不同主叫 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 DHCP Relay（可选）

当用户使用 IP 接入方式通过 BNAS 上网时，其 IP 地址主要是通过 DHCP Server 动态分配，为了保证网络的安全性，建议 BNAS 提供 DHCP Relay 功能，把用户和 DHCP Server 隔离开。同时它还需要提供连接用户和 DHCP Server 的功能，能够把用户的 DHCP 发现和请求报文送给 DHCP Server，同时把 DHCP Server 下发的响应报文转发给用户。如果 BNAS 支持 DHCP Relay 的功能，DHCP Relay 宜支持选项 82（option 82:Relay agent information option）。这样 BNAS 不但在物理上隔离用户和 DHCP Server，还可以把用户的 MAC 地址、VLAN 和 IP 地址等进行绑定，防止某条 VLAN 上的用户过多， 把 DHCP Server 地址池中地址耗尽的攻击。

5.3.7 VPN 功能

宽带接入服务器应当提供 VPN 功能。宽带接入服务器满足的 VPN 特性应当符合 YD/T 1190-2002 《基于网络的虚拟 IP 专用网（IP-VPN）框架》。具体来说，应至少提供 IPSec VPN， 虚拟租用线 VLL（Virtual Leased Line）、虚拟专用 LAN 网段 VPLS（Virtual Private LAN Segments）、虚拟专用拨号网 VPDN（Virtual Private Dial Network）和虚拟专用路由网 VPRN（Virtual Private Routed Network）实现技术的 VPN 中的一种。宽带接入服务器可选支持 VPN 按流量计费的功能。

5.3.7.1 虚拟租用线 VLL（Virtual Leased Line）（可选）

虚拟租用线采用点到点链接模型，通过运营商的边缘节点对用户提供点到点链接服务。应用组网如图 2 所示。

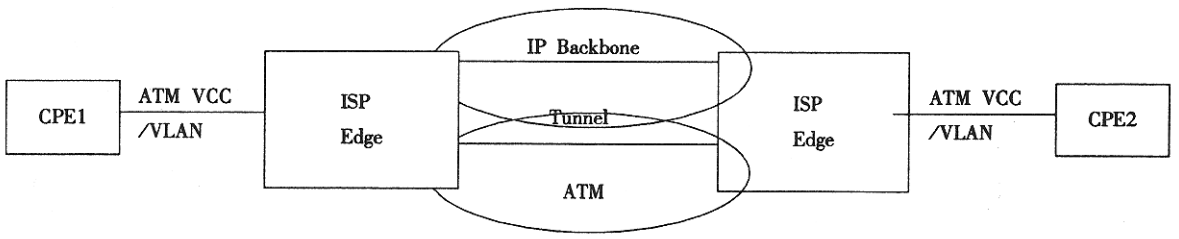


图 2 VLL 组网模型

运营商提供一条对两个 CPE 用户设备点到点的连接，两个 CPE 用户设备连接在 ISP 的两个 PE 设备上，两个 PE 设备间建立一条隧道，CPE 设备之间通过该隧道进行通信。本标准对如下方面进行定义，未涉及的请参见 YD/T 1190-2002《基于网络的虚拟 IP 专用网（IP-VPN）框架》中相关章节。

（1）同一个 VPN 网络不同 CPE 之间可能采用不同的接入协议。比如 CPE1 采用 RFC 1483B 方式接入，CPE2 采用 VLAN 方式接入。

（2）对于 VCC 接入方式的 VLL，不同 CPE 接入 VCC 不要求一致。

（3）对于 VLAN 接入方式的 VLL，不同 CPE 接入 VLAN 不要求一致。

（4）VLL 隧道不做要求，典型的可采用 ATM 隧道（VCC）方式和 IP Tunnel 技术实现。

（5）IP Tunnel 技术可参照 YD/T 1190-2002《基于网络的虚拟 IP 专用网（IP-VPN）框架》，典型的可采用 VLAN、GRE 和 L2 MPLS VPN。

5.3.7.2 虚拟专用 LAN 网段 VPLS（Virtual Private LAN Segments）（可选）

VPLS 网络模型如图 3 所示。

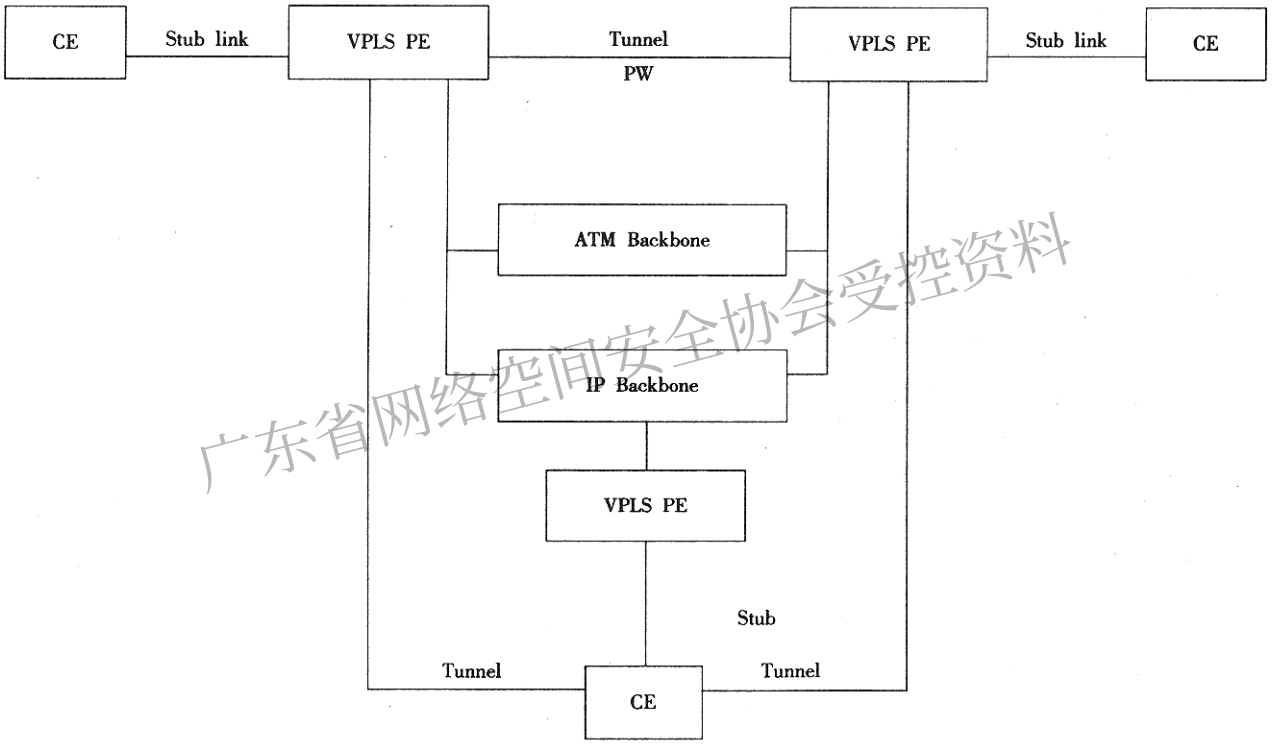


图 3 VPLS 网络模型示意

网络模型主要内容如下：

（1）CE 设备属于 Stub 类型。实际上对于 VPLS 网络模型，CE 接入设备自然属于 Stub 类型。

（2）CE 接入 ISP 协议为 XoE 模型（IPoE、IPoVLANoE、PPPoE、PPPoVLANoE），即 CE 通过以太网链路层协议接入 ISP 边缘节点。其中二层链路协议主要指以太网协议。CE 与 PE 之间的链路称为附加电路（Attachment Circuit），简称 AC。AC 可以是 Frame Relay DLCI、ATM VPI/VCI、Ethernet Port、VLAN、L2TPv3 和 MPLS LSP 等。

（3）PE 设备之间进行多点对多点的交换。PE 设备间的拓扑结构可以是网状结构（Full Mesh），也可以是树形结构，或者二者的组合。PE 设备之间的链路称为伪线路（Pseudo Wire），简称 PW。PW 的作用是将以太网包透传经过运营商的网络，从一个 PE 到达另一个 PE。PW 的形式可以是 VLAN、VLAN in VLAN、ATM VPI/VCI、L2TPv3、MPLS LSP 和 GRE 等。

（4）对每一个 VPLS VPN，在 PE 设备中提供一个虚拟交换实例（Virtual Switch Instance），即 VS。因为一个 PE 同时为多个 VPLS VPN 服务，故在一个 PE 设备中会有多个 VS 同时存在，各个 VS 之间是完全隔离的。VS 的功能如同一个以太网交换机，完成 MAC 地址学习和老化，根据以太网的目的 MAC 查转发表得到出口进行交换，在 VS 的“逻辑端口”范围内进行广播等。

（5）针对 ATM 网络和 IP 网络进行设计；ATM 网络承载二层以太网时，利用 ATM PVC 天然的隔离性和丰富的业务属性，网络可以具有很高的安全性和 QoS。针对 IP 网络设计，现阶段也能实现简单的端到端的安全性和 QoS，结合 MPLS，可实现更加强大的特性。

CE 到 PE 的 Attatchment Circuits 采用 VLAN 和 ATM VPI/VCI；PE 设备之间的 Pseudo Wires 采用 VLAN、ATM VPI/VCI 和 GRE。将来还会支持 MPLS LSP 和 L2TPv3 等。

5.3.7.3 虚拟专用拨号网 VPDN（Virtual Private Dial Network）（可选）

宽带接入服务器通过支持 L2TP 功能支持 VPDN。从网络功能上讲，要求宽带接入服务器支持 LAC 功能，可选支持 LNS 特性。

特性要求参见 9.2 节。

5.3.7.4 虚拟专用路由网 VPRN（Virtual Private Routed Network）（可选）

宽带接入服务器选择通过支持基于 BGP4 扩展方式实现的 MPLS VPN 支持 VPRN。从网络形态进行分析，要求宽带接入服务器支持 PE 设备特性，可选支持 P 设备特性。

MPLS VPN 相关技术参数的要求参见 YD/T 1097-2001《路由器设备技术规范——高端路由器》。

5.3.7.5 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。

5.3.8 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（RFC 1157）、MIB II（RFC 1213）、MIB II Traps（RFC 1215）、ATM MIB（RFC 1695）、Ethernet MIB（RFC 1643），可选地支持 RIP MIB（RFC 1389）、OSPF MIB（RFC 1253）、BGP4 MIB（RFC 1657）及 Frame Relay MIB（RFC 1315）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、闲时概率、忙时概率、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。

5.3.9 设备的监控和管理功能

宽带网络接入服务器应提供 Telnet 接入监控功能和本地控制台（Console）管理功能。远程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启动（Reboot）功能，实现对其维护和监控功能；远程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；远程终端或本地控制台还应能实现设备故障定位功能。

5.3.10 组播功能

作为宽带接入设备，BNAS 支持宽带用户的宽带组播业务需求。BNAS 应支持 IGMP Proxy 和用户组播数据流的复制分发。宽带网络接入服务器可选支持组播计费功能和权限控制。

6 通信接口

6.1 接入侧

1）xDSL 通信接口（必选）

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。

2）CABLE Modem 通信接口（必选）

宽带网络接入服务器的 CABLE Modem 通信接口的物理层接口应支持 10/100BaseT 以太网接口（符合 IEEE 802.3/IEEE 802.3u）。

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 IEEE 802.3/IEEE 802.3u）和千兆以太网接口（符合 IEEE 802.3）。千兆以太网接口为可选。

4）FR/DDN 接口（可选）

宽带网络接入服务器的 Frame Relay/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 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 YD/T 1097。

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。

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 1045，10/100BaseT 以太网接口符合 IEEE 802.3/IEEE 802.3u 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 YD/T 1097。STM-16、STM-64 接口应符合 YDN 099 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 IEEE 802.3z）。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 。

3）FR/LL 接口（可选）

宽带网络接入服务器的 Frame Relay/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。STM-16、STM-64 接口应符合 YDN 099-1998《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，WDM 接口具体技术要求参见相应标准。

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会话端结（PPP Terminated Aggregation）两种。

7.1.1 PPP会话续传（PPP Tunneling Aggregation）业务流程

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：

1）用户以PPPoE或PPPoA方式上网。

2）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隧道中发出去，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。

3）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。

这种方式可选。

7.1.2 PPP会话端结（PPP Terminated Aggregation）

BNAS完成PPP端结并支持多个ISP。这种组网方式的特点是：

1）用户以PPPoE或PPPoA方式上网。

2）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。

3）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。

这种方式必选。

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。该种方式为可选。

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。

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。

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。

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取分布式、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。

有以下两种情况：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

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。

以上两种方式必选。

3）IAC 方式的地址分配

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。

该种方式为可选。

9 协议要求

9.1 PPP

参见标准 YD/T 1045 的 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 层把下层的 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 RFC 1483 和 RFC 2364。

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 ITU-T Q.2931《宽带综合业务数字网（B-ISDN）——No.2 数字用户信令系统——用于基本呼叫/连接控制的用户网络接口第三层规范》附录 C“用户的测试套件结构和测试目的”中的过程进行协商。目前 BNAS 只支持 PVC 方式。PPPoA 的协议栈结构如图 4 所示。

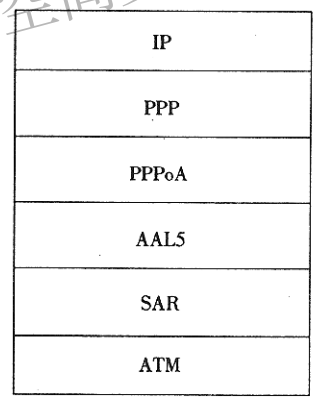


图 4 PPPoA 的协议栈

9.2.3 AAL5 层业务接口要求

PPP 层把下层的 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 业务接口必须符合下面要求：

1）接口格式：PPP/AAL5 层边界向 AAL5 层提供一个字节业务接口。

2）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。

3）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

1. AAL5 PDU 格式

ALL5 PDU 帧格式如图 5 所示，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 64 比特。当只用于 64 比特调整功能时，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。

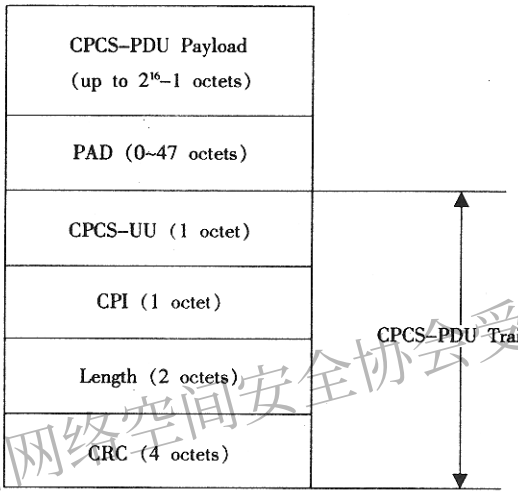


图 5 AAL5 PDU 帧格式

2. VC 复用 PPP 帧格式

VC 复用 PPP 帧格式如图 6 所示。

VC 复用 PPP 帧构成 CPCS-PDU 的净荷。

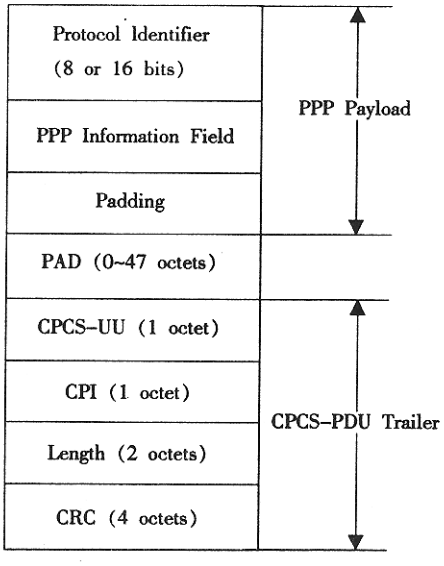


图 6 VC 复用 PPP 帧格式

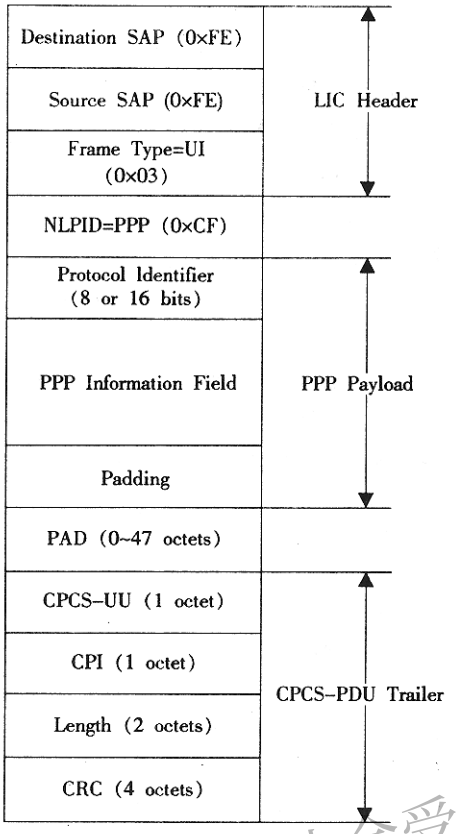


图 7 LLC 封装 PPP 帧格式

3. LLC 封装 PPP 帧格式

LLC 封装 PPP 帧格式如图 7 所示，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 或两个八位组长。

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 RFC 1483 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（RFC 2364）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，并建立一个惟一的 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 RFC 2516。

PPPoE 实现 PPP 帧在 Ethernet 上的适配，并提供 Ethernet 上的 PPP 连接。图 8 和图 9 分别是以太网上的 PPPoE 协议栈和 AAL5 上的 PPPoE 协议栈。

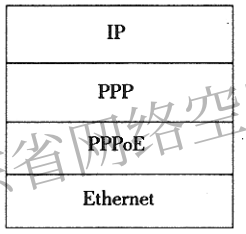


图 8 以太网上的 PPPoE 协议栈

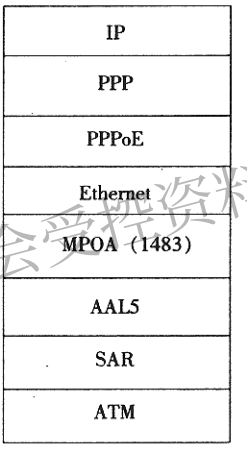


图 9 AAL5 上的 PPPoE 协议栈

9.3.3 PPPoE 连接示意图

典型的 PPPoE 的连接方式如图 10 所示。

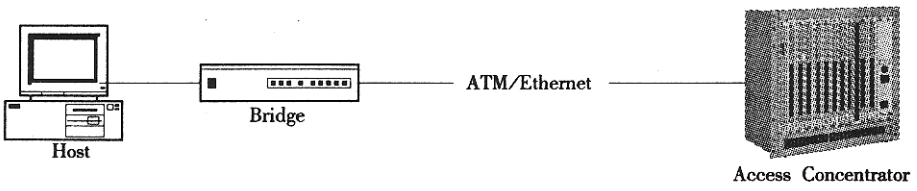


图 10 典型的 PPPoE 的连接示意

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，它必须首先进行发现阶段以识别对端以太网 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它们在以太网上建立 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。PPPoE 通信流程如图 11 所示。

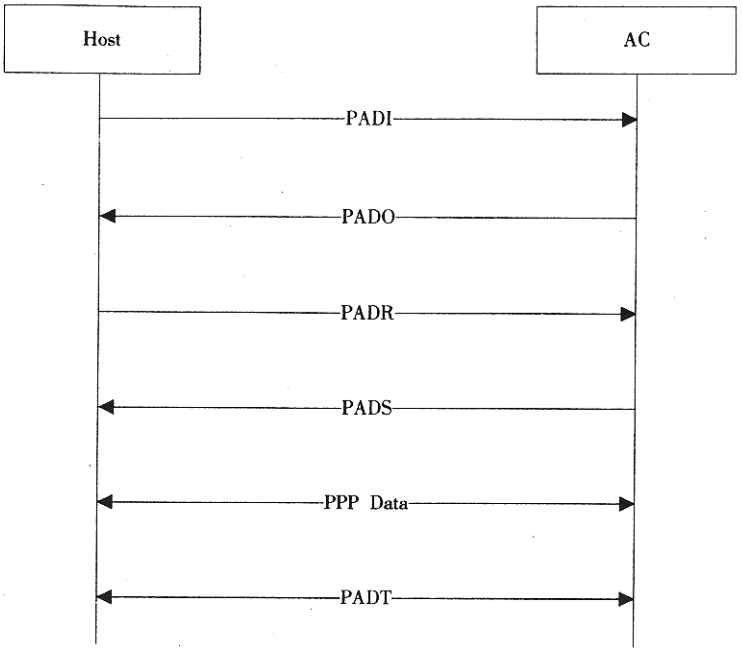


图 11 PPPoE 通信流程

1. 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 和对端以太网地址，它们一起惟一定义 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。

2. 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

1. 以太网帧格式

以太网帧格式如图 12 所示，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。

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）。

2. PPPoE 帧格式

PPPoE 帧格式如图 13 所示。

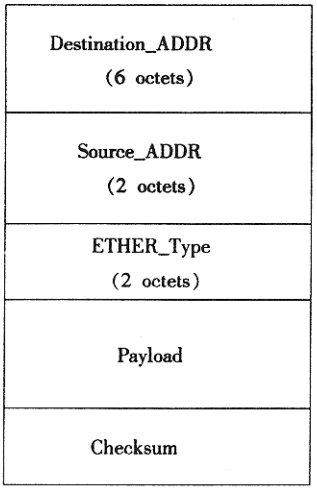


图 12　以太网帧格式

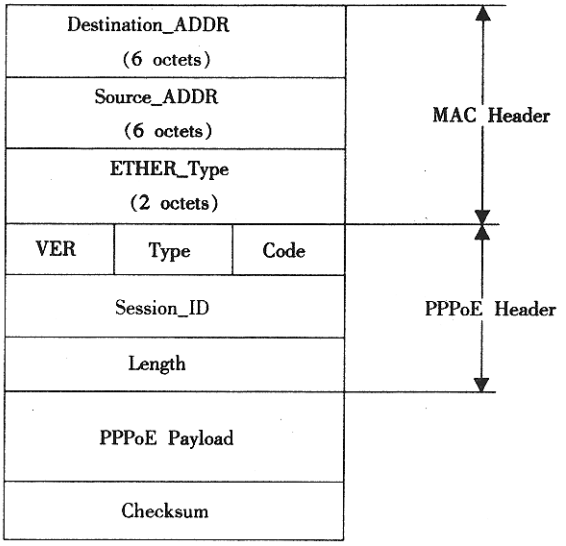


图 13　PPPoE 帧格式

用于 PPPoE 的以太网净荷的各字段的含义如下：

1）VER：版本域是 4 比特，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 4 比特，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 8 比特，由发现阶段和 PPP 会话阶段分别定义。

4）Session_ID：会话标识域是 16 比特，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 16 比特。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）。

3. 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 14 所示。

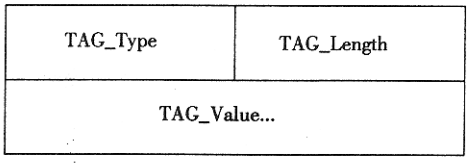


图 14　PPPoE 发现阶段净荷的 TLV 格式

TLV 各字段的含义如下：

1）TAG_Type：标记类型是网络字节顺序的 16 比特字段。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 RFC 2516 中有其他说明。PPPoE 目前包含的标记类型及其相应的标记值见表 1。

表 1 PPPoE 的标记类型及相应的标记值

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 16 比特，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（RFC 2516）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（RFC 1973）规定的是标准 PPP 帧在帧中继链路上的帧封装方法和格式，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 协议参见 RFC 1973。

PPPiFR 完成 PPP 帧在帧中继链路上的适配，PPPiFR 的协议栈结构如图 15 所示。

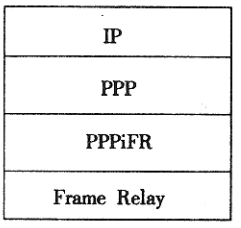


图 15 PPPiFR 的协议栈

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

PPPiFR 的帧格式如图 16 所示，各字段的含义如下：

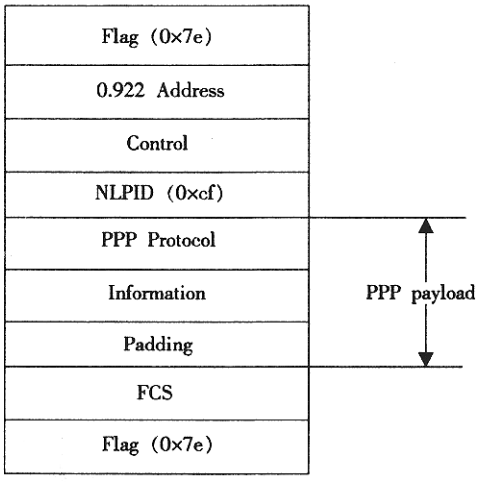


图 16 PPPiFR 的帧格式

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 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）

注意，不像 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 RFC 1490 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 字节。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 L2TP 协议（可选）

L2TP2 协议要求主要参见标准 YD/T 1045 的 8.3 节。

以下介绍 L2TP over UDP/IP/Ethernet 和 L2TP over ATM 。

9.5.1 L2TP over UDP/IP/Ethernet（可选）

L2TP over UDP/IP/Ethernet 指 LAC 与 LNS 之间采用以太网作为其传输媒介，其报文封装格式如图 17 所示。

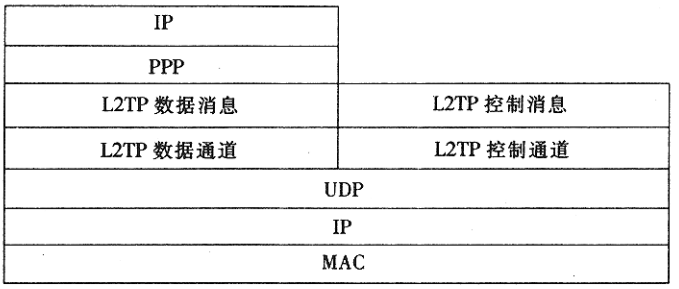


图 17 L2TP over UDP/IP/Ethernet 协议栈

L2TP 使用特定的 UDP 端口（1701 [RFC 1700]）进行承载数据和传送 L2TP 头数据。

如果 L2TP 报文需要分片或者重组， 将会降低 L2TP 的隧道封装性能，这种情况可以通过要求 PPP LCP 协商合适的 MRU/MTU 参数来保证 L2TP 报文不需要分拆重组。

基于 UDP 的传输是不可靠传输，因此任何可靠传输都需要通过 UDP 之上的协议来保证。在 L2TP 协议中控制消息是可靠消息传递，有重发机制，而数据消息是允许消息包丢失的，是不可靠传送。

9.5.2 L2TP over ATM（可选）

隧道技术（Tunneling）是 VPDN（虚拟拨号专网）技术的核心。L2TP 协议则是其中一种隧道技术，它是 Internet 工程任务组 IETF 的国际标准。隧道协议所采用的方法是将用户的整个数据包（包括附加的协议成分）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：一是指定使用 ATM 网络作为 LNS 与 LAC 之间的通信链路；二是指定使用 ATM 网络作为接入网络。

9.5.3 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 13 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。

a）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；

b）HELLO 信息传输是为了维护隧道的连通性；

c）WEN 用于 LAC 向 LNS 报告差错信息；

d）SLI 用于设定 PPP 协商选项。

2）控制连接状态机

（1）隧道建立

LAC or LNS　　LAC or LNS

SCCRQ------->

<----------SCCRP

SCCCN------->

<----------ZLB

（2）入呼叫建立

LAC　　LNS

ICRQ---------- >

< ----------ICRP

ICCN---------- >

< ----------ZLB

（3）出呼叫建立

LAC　　LNS

< ----------OCRQ

OCRP---------->

(Bearer Detected)

OCCN---------- >

<----------ZLB

（4）关闭呼叫

LAC or LNS　　LNS or LAC

CDN---------- >

< ----------ZLB

（5）拆除隧道

LAC or LNS　　LNS or LAC

StopCCN-------->

< ----------ZLB

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 的协议结构如图 18 所示。

<table>
<tr><td colspan="2">PPP Frames</td></tr>
<tr><td>L2TP Data Messages</td><td>L2TP Control Messages</td></tr>
<tr><td>L2TP Data Channel
(Unreliable)</td><td>L2TP Control Channel
(Reliable)</td></tr>
<tr><td colspan="2">Packet Transport (UDP、FR、ATM etc.)</td></tr>
</table>

图 18　L2TP 协议结构

4） L2TP 数据格式

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

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；

隧道标识：指定控制连接的隧道标识；

会话标识：用于指定隧道中会话的标识；

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，如下所示。

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

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

H 标志位：当置 1 时，指定这个 AVP 的属性值域数据已经隐藏起来。

长度：AVP 的长度（包含长度字段和标志位）。长度字段可以按照属性值的长度加 6 计算。长度字段为 10 比特，允许的最大长度为 1023 字节，最小的长度为 6。当长度为 6 时，没有属性值字段。

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。

9.5.4 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 AAL5 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 链路相对应于一个 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。

1）采用 ATM 作为传输媒介需要考虑的问题包括。

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隧道的 MTU 和用这个隧道的所有 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 PVCs 上的 LLC 封装 L2TP；

b）可以支持 SVCs 上的 LLC 封装 L2TP；

c）可以支持在 PVCs 或 SVCs 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 的载荷域采用的编码格式如图 19 所示。

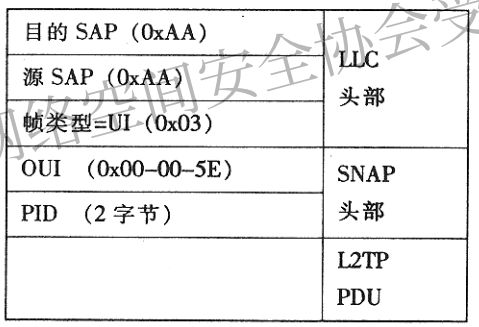


图 19 LLC 封装

a）IEEE 802.2 LLC 头部：包括源和目的 SAP，值都为 0xAA，接着时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 个字节的团体惟一标识符 [Organizationally Unique Identifier （OUI）]（值为 0x00-00-5E 标识 IANA（Internet Assigned Numbers Authority））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 格式显示如图 20 所示。

<table>
<tr><td>CPCS-PDU 载荷
（最大 2^{16}-1 字节）</td><td>L2TP
PDU</td></tr>
<tr><td>PAD（0~47 字节）</td><td></td></tr>
<tr><td>CPCS-UU（1 字节 ）</td><td rowspan="4">CPCS-PDU
尾部</td></tr>
<tr><td>CPI（1 字节）</td></tr>
<tr><td>长度（2 字节）</td></tr>
<tr><td>CRC（4 字节）</td></tr>
</table>

图 20 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 差错检查能力。

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

（1）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。

（2）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。

（3）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的清除连接。

（4）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。

9.5.5 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。

（1）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 应当决定是否接收这个呼叫。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。

（2）隧道建立

如果在 LAC 和指定的 LNS 之间没有隧道连接存在，就需要建立一个隧道。在隧道建立过程中，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，将不能建立隧道。

（3）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（最大和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。

（4）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

（1）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。

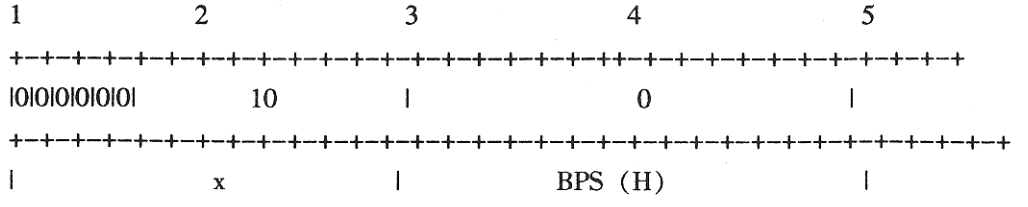
（2）授权

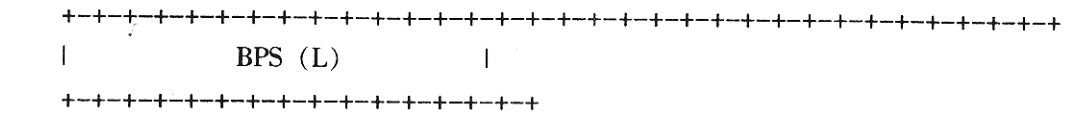
因为建立 ATM 连接的复杂性，从而造成在接收 ATM 连接建立以前就需要一些授权。非授权的访问请求会造成连接释放。

3）新的和扩展 AVP

（1）新的 AVP 定义

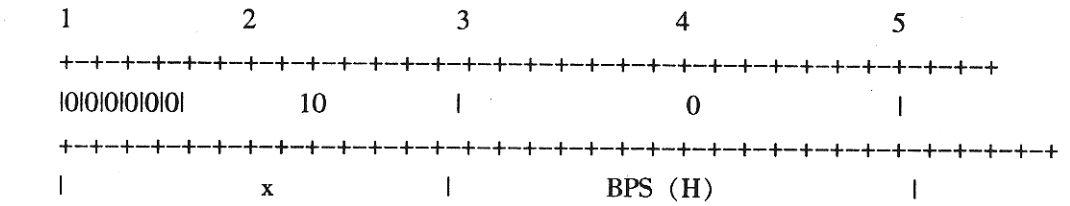
a）接收的最小 BPS





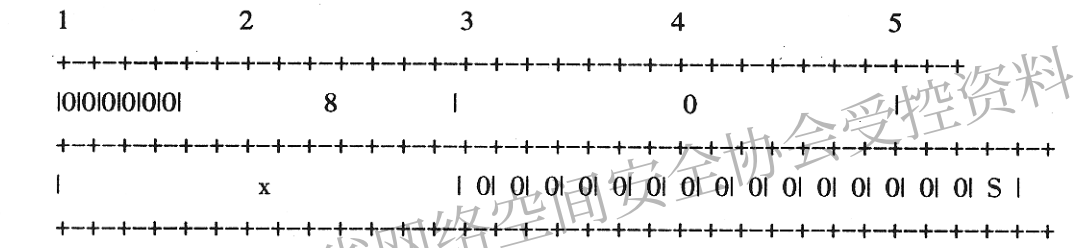
接收的最小 BPS AVP 指定在非对称传输中接收方向的最小可接收的线速率。这个 AVP 可以包括在 OCRQ 消息中，并且当 LAC 指定 ATM 支持时只能包括在 OCRQ 中。

b）接收的最大 BPS



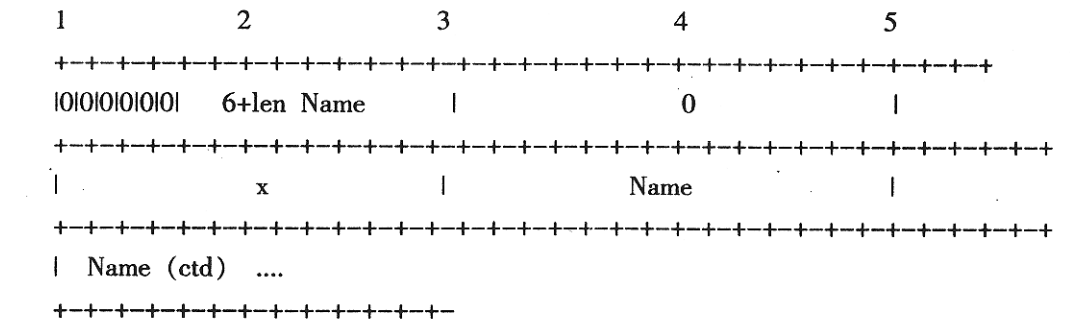
接收的最大 BPS AVP 指定在非对称传输中接收方向的最大可接收的线速率。这个 AVP 可以包括在 OCRQ 消息中，并且当 LAC 指定 ATM 支持时只能包括在 OCRQ 中。

c）服务种类



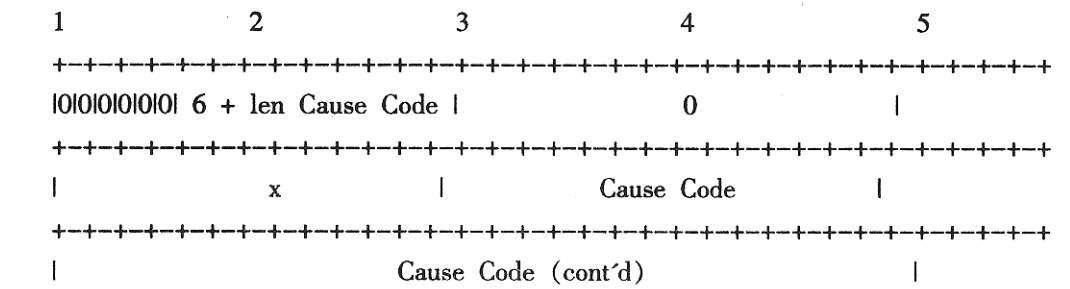
服务种类 AVP 对于呼叫建立希望的服务质量提供了可选附加信息。S 位指定了是实时的（S 位是 1）还是非实时的（S 位是 0）。其他位保留为将来使用。这个 AVP 可以包括在 OCRQ 和 ICRQ 信息中。

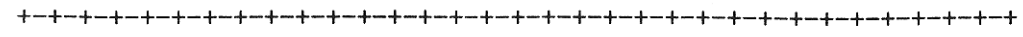
d）服务名



服务名 AVP 仅仅当被叫号码域全为 0 时才提供，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。

e）ATM Cause Code



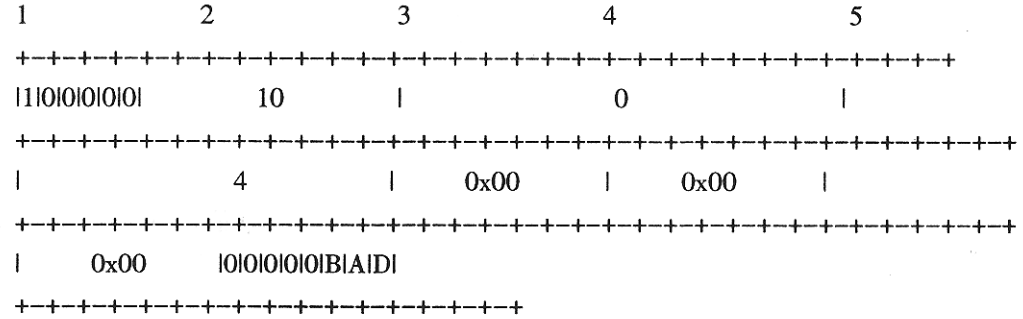


当 ATM 连接失败时，ATM 原因码（Cause Code）AVP 指定失败原因。这个 AVP 必须包括在 CDN 信息中。

（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。

a）Bearer Capabilities



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。

b）（Tx）Minimum BPS

发送最小 BPS AVP 指定在发送方向的最小可接收线速率。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。

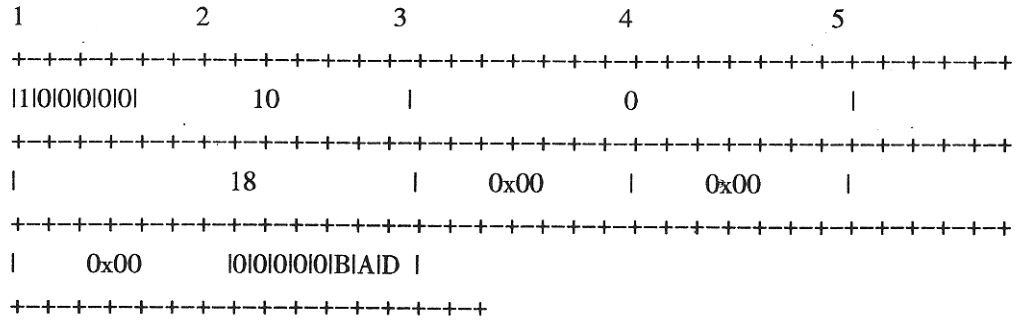
发送最小 BPS 的单位是比特/s，并且对于 ATM 网络可以被映射成 PCR（Peak Cell Rate，峰值信元速率）单位是信元/s。

c）（Tx）Maximum BPS

发送最大 BPS AVP 指定在发送方向的最小可接收线速率。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。

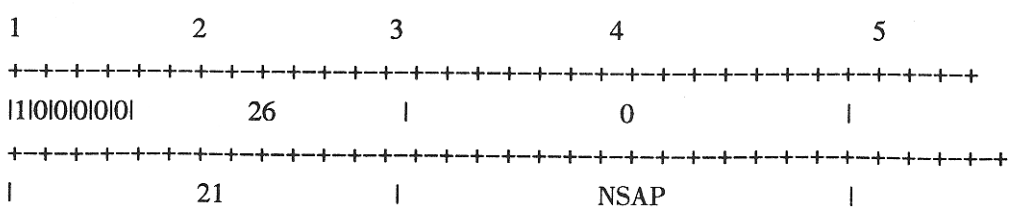
发送最大 BPS 的单位是比特/s 并且对于 ATM 网络可以被映射成 PCR（Peak Cell Rate，峰值信元速率）单位是信元/s。

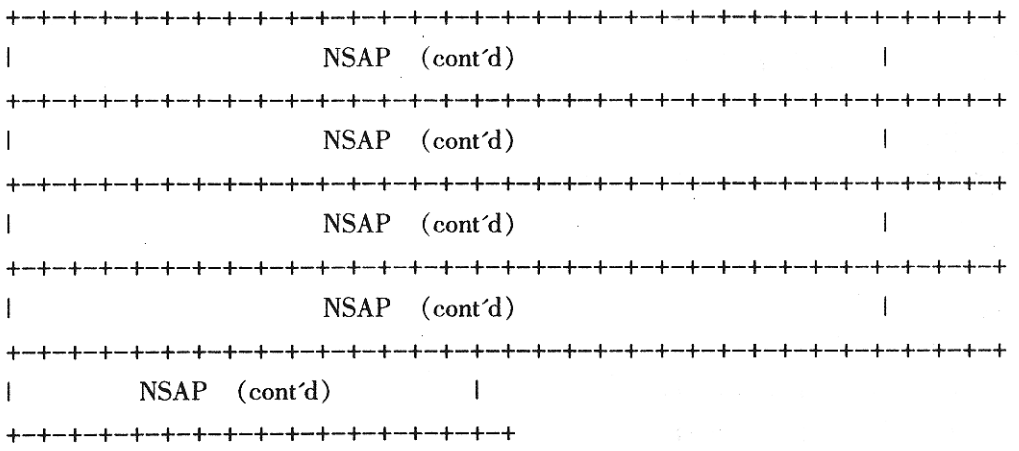
d）载体类型



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。

e）Dialed Number





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 被解释为二进制编码。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。

f) Sub-Address

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 协议主要包括以下协议。

— 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发功能；

— 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，如图 21 所示。

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 和 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。

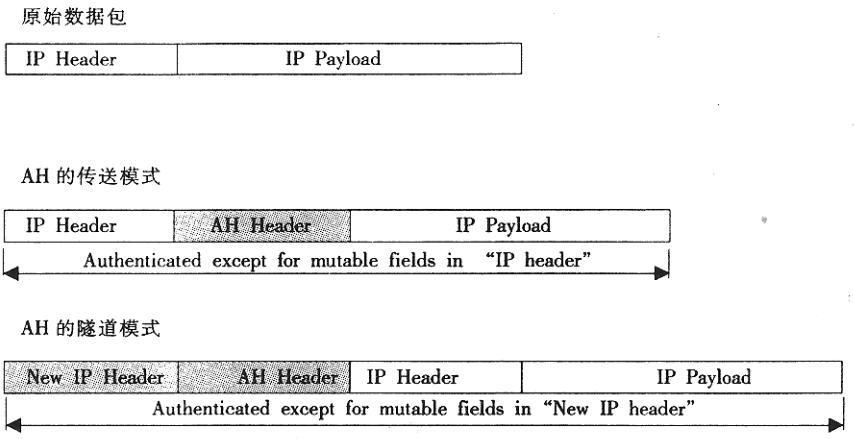


图 21 AH 协议的操作模式

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。

1. ESP 加密算法

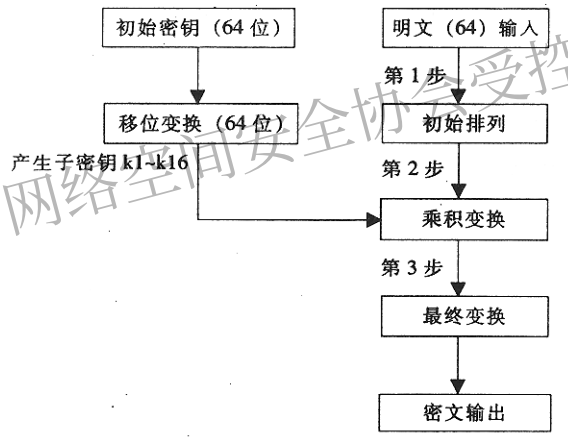


图 22 DES 算法过程

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。（这是和国家密码政策相冲突的，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。）

2. ESP 的操作模式

与 AH 协议相同，ESP 也有 2 种操作模式，如图 23 所示。

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。

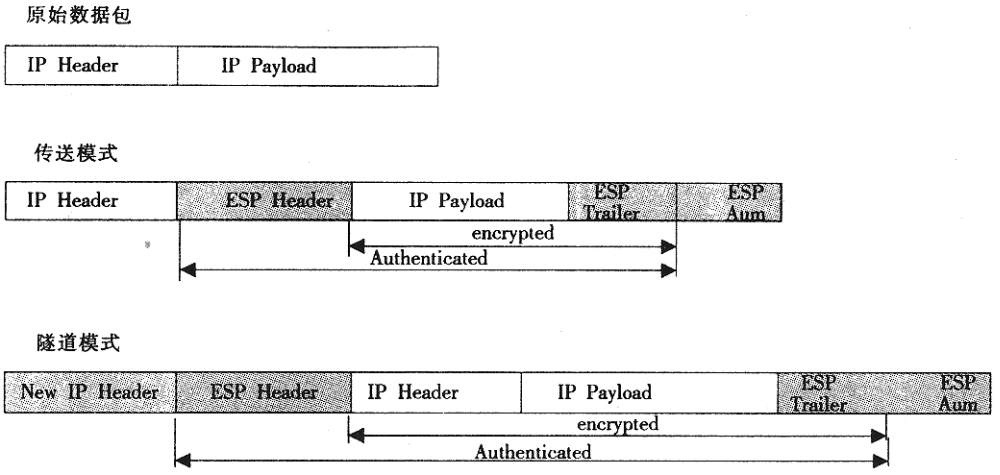


图 23 ESP 的操作模式

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收。为防止数据包的重发，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）组成的三元组惟一标识。

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。

1. Internet 密钥交换协议（IKE）

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：3 对消息完成策略协商、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。

```
    发起端                                  响应端
------------                            ------------
HDR, SA                    ---->
                           <----        HDR, SA
HDR, KE, Ni                ---->
                           <----        HDR, KE, Nr
HDR*, IDii, [ CERT,] SIG_I ---->
                             <----      HDR*, IDir, [CERT,] SIG_R
```

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。


```
    发起端                                  响应端
--------------                          ---------------
HDR, SA, KE, Ni, IDii      ---->
                           <----        HDR, SA, KE, Nr, IDir,
                                          [ CERT,]  SIG_R
HDR, [ CERT,] SIG_I        ---->
```

快速交换模式为非 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 之前或之后均可进行，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）验证和公钥加密（Public Key Encryption）验证等。作为基本手段，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

RFC 2409 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 YD/T 1045 中 8.5 节。

9.8 Telnet 协议

参见 YD/T 1045 中 8.5 节。

9.9 SNMP 协议

参见 YD/T 1045 中 8.6 节。

9.10 EAP 协议（可选）

PPP 协议提供了在点对点的链路上传输多协议数据报的方法。PPP 协议同时定义了可扩展的链路控制协议，它提供了对网络层在链路上传输数据之前对对等实体实施认证的认证协议进行协商的机制。

为了在点对点的链路上进行通信，PPP 链接的每一端在连接建立阶段应先发送 LCP 包。在数据链路建立之后，网络层协议阶段之前，PPP 提供了一个可选的认证阶段。

在默认的情况下，认证不是强制的。如果需要对连接进行认证，应在连接建立阶段指明认证协议配置选项。连接建立阶段和认证阶段，以及认证协议配置选项在 PPP 协议中规定。

PPP 可扩展认证协议是一个通用协议，它能支持多种认证机制。EAP 不在链路控制阶段选择特定的认证协议，而是延迟到认证阶段。

9.10.1 配置选项格式

协商 EAP 认证协议的认证协议配置选项的格式如下，各字段应按从左到右的顺序发送。

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |     Authentication-Protocol   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type: 3；

Length: 4；

Authentication-Protocol: C227 （Hex） PPP 可扩展认证协议。

9.10.2 包格式

每个 PPP EAP 包封装在一个 PPP 数据链路帧的信息字段中，协议字段指明类型 C227（HEX）（PPP EAP）。EAP 包的格式如下，各字段应按从左到右的顺序发送。

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Code      |  Identifier   |            Length             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Data ...
```

（1）EAP 代码（Code）

Code 字段长度为一个字节，用于识别 EAP 包的类型。EAP 代码的指派如下：

1— Request；

2— Sponse；

3— Success；

4— Failure。

（2）标识符（Identifier）

Identifier 字段长度为一个字节，用来对请求和应答进行匹配。

（3）长度（Length）

Length 字段的长度为两个字节，指明包含 Code、Identifier、Length 和 Data 字段在内的 EAP 包的长度。接收到超过长度字段指明的字节应按照数据链路层填充处理，并丢弃。

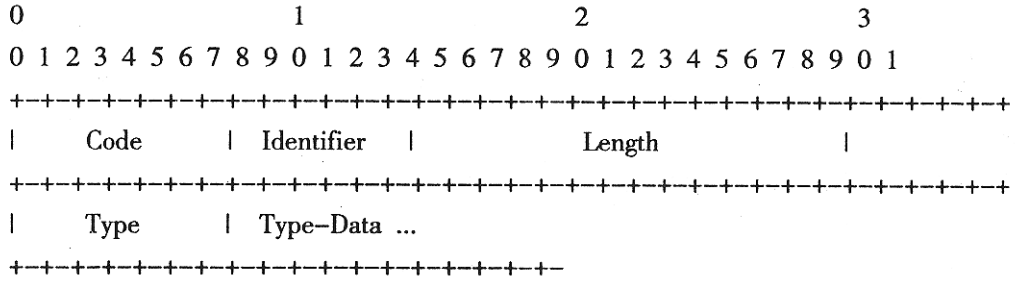
（4）数据（Data）

Data 字段包含零个或者多个字节，数据字段的格式由 EAP 代码字段决定。

1. 请求和应答

请求包由认证者发送给对等实体。每个请求包含类型字段。认证者应将 EAP 包的类型字段设置为 1（请求）。认证者应发送额外的请求包，直至接收到有效的应答包，或者到达重试限额（可选）。重发的请求包应包含相同的标识符，以便同新的请求区分。数据字段的内容依赖于请求的类型。对等实体应发送应答以响应接收到的请求，并且不应重发应答包。应答包的标识符字段应与请求包的标识符字段匹配。

请求和应答包的格式描述如下，各字段按照从左到右的顺序发送。



（1）EAP 代码（Code）

1— 请求（Request）；

2— 应答（Response）。

（2）标识符（Identifier）

Identifier 字段长度为一个字节。如果因等待应答超时重发，标识符字段应保持不变。如果是新的请求（非重发），应修改标识符字段。如果对等实体接收到重复的请求并且已经发送了应答，也应重发应答包。如果对等实体接收到重复的请求，但还没有发送应答，应将重复的请求包丢弃。

（3）长度（Length）

Length 字段为两个字节指明包含 Code、Identifier、Length 和 Data 字段在内的 EAP 包的长度。接收到超过长度字段指明的字节应按照数据链路层填充处理，并丢弃。

（4）类型（Type）

Type 字段为一个字节，该字段指示请求和应答的类型。通常应答的类型字段和请求的类型字段相同。然而有一个类型为 Nak 的应答类型，指出请求类型对等实体不能接受。当发送一个类型为 Nak 的应答的时候，对等实体可指出一个它能够支持的认证类型，以供选择。

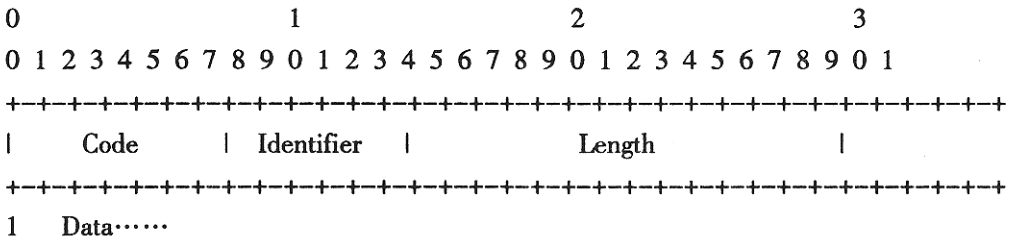
（5）Type-Data

Type-Data 字段因请求类型和关联的应答而不同。

2. 认证成功和认证失败

认证成功包是由认证者发送的，对对等实体认证成功的应答。认证者应发送 EAP 包，并将 EAP 代码字段设置为 3（Success）。如果认证者不能鉴别对等实体（对一个或者多个应答不能接受），应发送 EAP 包，并将 EAP 代码字段设置为 4（Failure）。认证者可以在发送认证失败包之前发送多个认证请求，以允许用户纠正输入错误。

认证成功和认证失败包的格式描述如下，各字段按照从左到右的顺序发送。



（1）EAP 代码（Code）

3— 认证成功（Success）；

4— 认证失败（Failure）。

（2）标识符（Identifier）

Identifier 字段为一个字节，用来匹配请求和应答。标识符字段应与对应的应答包的标识符相同。

（3）长度（Length）

Length 字段的长度为两个字节，指明包含 Code、Identifier、Length 和 Data 字段在内的 EAP 包的长度，接收到超过长度字段指明的字节，应按照数据链路层填充处理，并丢弃。

3. 初始 EAP 请求/应答类型

本节定义在请求/应答交换中使用的初始 EAP 类型。新的类型可在后续的文献中定义。类型字段为一个字节，用来识别 EAP 请求或者应答包的结构。开头的 3 种类型为特殊类型，而其他的类型定义认证交换。Nak 类型仅适用应答包，不应在请求包中发送。Nak 类型应仅在对包含认证类型的请求进行应答的时候使用。所有 EAP 的实现应支持类型 1~4。这些类型包括 5、6 在 RFC 2284 中定义。后续的 RFC 将定义附加的 EAP 类型。

1— 身份（Identity）；

2— 通知（Notification）；

3— Nak（Response only）；

4— MD5-Challenge；

5— 一次性口令 One-Time Password （OTP） （RFC 1938）；

6— 通用标记卡片（Generic Token Card）。

3.1 身份（Identity）

身份类型用来询问对等实体的身份。通常认证者在初始请求中下传。对这种请求应发送包含类型 1（身份）的应答。

Type 1

Type-Data

在请求包中该字段可包含可显示的消息，在请求包中该字段返回身份。如果身份未知，该字段为零字节。该字段不应以空字符结束。字段的长度从请求/应答的长度字段推导，因此空字符是不必要的。

3.2 通知（Notification）

通知类型是可选的，认证者用来向对等实体传递可显示的消息。对等实体应向用户显示该消息或者在日志中记录该消息。

Type 2

Type-Data

在请求包中该字段包含长度大于零的可显示的消息。消息的长度由请求包的长度字段确定。消息不应以空字符结束。对包含类型字段 2（Notification）的请求，应发送应答。应答的 Type-Data 字段的长度为零字节。应答应立即发送，与消息显示或者写日志的方式无关。

3.3 Nak

Nak 类型仅在应答消息中有效。它在对一个包含不能接受的认证类型的请求消息的应答中认证类型编号大于等于 4。在应答中包含对等实体希望的认证类型。

Type 3

Type-Data

该字段应包含单个字节，指出希望的认证类型。

3.4 MD5-Challenge

MD5-Challenge 类型 类似 PPP CHAP Protocol（以 MD5 作为指定的算法）。实现的细节参见 RFC 1994。在请求中包含给对等实体的质询（Challenge）。对该种请求应发送应答，应答的类型可为类型 4（MD5-Challenge） 或者类型 3 （Nak）。Nak 应答指出对等实体希望的认证机制类型。所有 EAP 实现应

支持 MD5-Challenge 机制。

Type 4

Type-Data

该字段内容概述如下。参见 RFC 1994。

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Value-Size   |  Value ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Name ...
```

3.5 One-Time Password (OTP)

一次性口令系统在 RFC 1938 中定义。请求包含一个可显示的消息，该消息包含一个 OTP 质询。对该种请求应发送应答，应答的类型应为 5（OTP）或者 3（Nak）。Nak 应答指出对等实体希望的认证机制类型。

Type 5

Type-Data

该字段包含 OTP 质询（challenge），作为请求中的可显示消息。在应答中该字段被 OTP 字典中的 6 个字（Word）使用。消息不应以空字符结束。该字段的长度从请求/应答包的长度字段推导。

3.6 通用标记卡片（Generic Token Card）

Generic Token Card Type 为使用各种需要用户输入的通用标记卡片的实现定义。请求包含 ASCII 码文本消息，应答包含用来认证的标记卡片信息。

Type 6

Type-Data

请求中包含字节长度大于零的可显示的消息，消息的长度由请求中的长度字段确定。消息、不应以空字节结束。对于每个请求应发送类型字段为 6（Generic Token Card）的应答。应答包含从标记卡片上获取的用来认证的数据，数据的长度由应答的长度字段确定。

9.10.3 安全性

EAP 协议主要关注系统安全性，在 PPP 协议中，认证协议的相互作用与实现方式高度相关。例如，在认证失败的情况下，一些实现不终止连结，而是将网络层的通信限制在一个经过筛选的子集之内，从而使得用户可以修改密码或者通知网络管理员有关的网络问题。

本标准没有规定认证失败后重试的次数。LCP 状态机能在任何时候重新协商认证机制，从而允许新的尝试。除连结终止或者认证成功之外，本标准不建议重置与认证失败相关的计数器。

在服务器中，针对一个特定的用户名不应支持使用不同的认证机制。这种使用方式导致在协商过程中可选择最弱的认证机制，从而使用户易受攻击。每一个用户名，只支持一种特定的认证机制。如果用户需要在不同的环境下使用不同的认证方式，用户宜使用不同的身份，每种身份对应不同的认证方式。

9.11 扩展 RADIUS 协议（可选）

本节定义在宽带网络接入服务器和计费服务器之间使用 RADIUS 协议传递认证、授权和计费信息的附加属性。

EAP 对 PPP 协议进行了扩展以便在 PPP 协议中支持附加的认证协议，本节描述如何使用 EAP 消息（EAP-Message）和消息认证者（Message-Authenticator）属性以使得 RADIUS 支持 EAP 协议。

所有属性由包含类型-长度-属性值的可变长的三元组构成，新的属性的增加并不影响已有的 RADIUS 协议的实现。

9.11.1 RADIUS 对 EAP 协议的支持

EAP 协议提供了支持附加认证协议的标准机制，通过使用 EAP 协议，可以增加认证方案，例如，智能卡、Kerberos、公钥密码和一次性口令等。为了使 RADIUS 支持 EAP 协议需要增加两个属性：EAP 消息（EAP-Message）和消息认证者（Message-Authenticator）属性。在建议方案中，RADIUS 服务器用来在宽带网络接入服务器和后台的安全服务器之间传递 RADIUS 封装之后的 EAP 包。RADIUS 服务器和后台安全服务器之间的会话使用专用协议，不属于本标准的范围。

对等实体和宽带网络接入服务器的 EAP 会话以 LCP 的 EAP 协商开始。一旦 EAP 协商完成，BNAS 应发送 EAP 请求/身份或身份消息给对等实体，除非对等实体的身份已经能够通过其他方式确定。然后对等实体发送 EAP 应答/身份消息给 BNAS。BNAS 将这些数据封装在 RADIUS Access-Request 包的 EAP 消息（EAP-Message）属性中转发给 RADIUS 服务器。RADIUS 服务器通常使用 EAP 应答/身份来决定用户使用的 EAP 类型。

为了使不支持 EAP 的 RADIUS 代理能够转发接入请求（Access-Request）包，如果 BNAS 发送 EAP 请求/身份，BNAS 应将内容复制到用户名属性（User-Name Attribute），并且应将 EAP 请求/身份包含在后续的接入请求的用户名属性中。为了使不支持 EAP 的 RADIUS 代理能够转发接入应答（Access-Reply），如果在接入请求中包含了用户名属性，RADIUS 服务器应在后续的接入接受包（Access-accept）中包含用户名属性。

如果用户的身份是通过其他的方式（Called Station ID 或者 Calling Station ID）来确定的，BNAS 应在每一个接入请求中包含身份属性。虽然这种方法节约了一轮交换，但并不通用。在某些场合并不需要用户身份（基于 Called Station ID 或者 Calling Station ID 的认证和计费），因此 BNAS 不需向被认证的对等实体发送 EAP 请求/身份包。

在 BNAS 不发送 EAP 请求/身份的情形下，BNAS 向 RADIUS 服务器发送包含 EAP 消息属性的接入请求包，表示 EAP 启动。EAP 的启动通过发送长度为 2 的 EAP 消息属性（无数据）。由于在接入请求中不包含用户名，这种方法与 RADIUS 不兼容，也不能在配置代理的情形下使用（如漫游、共享网络）。

如果 RADIUS 服务器支持 EAP，应以包含 EAP 消息属性的接入质询包（Access-Challenge）作为应答。如果 BNAS 不支持 EAP，它应以接入拒绝包（Access-Reject）作为应答。EAP 消息属性（EAP-Message）包含封装后的 EAP 包，它被转发给对等实体。在 BNAS 不发送初始的 EAP 请求/身份消息给对等实体的情形下，接入质询通常包含 EAP 消息属性，它封装了一个 EAP 请求/身份，要求接入用户确定身份。BNAS 用 RADIUS 接入请求包作为应答，它包含了封装 EAP 应答（EAP-Response）的 EAP 消息属性。会话持续到接收到 RADIUS 接入拒绝或者接入接受。

在接收到包含或者不包含封装 EAP-Failure 的 EAP 消息属性的 RADIUS 接入拒绝包，BNAS 应发送 LCP 终结请求（LCP Terminate Request）给对等实体。包含封装 EAP 成功的 EAP 消息属性的 RADIUS 接入接受包终结认证阶段。RADIUS 接入接受/EAP 消息/EAP 成功包应包含期望在 RADIUS 接入接受包中返回的所有参数。

9.11.2 包格式

同 RFC 2865 和 RFC 2866。

9.11.3 包类型

同 RFC 2865 和 RFC 2866。

9.11.4 属性

RADIUS 属性包含请求和应答中特定的认证、授权和计费细节。某些属性可以包含多于一次。

属性格式的定义同 RFC 2865。

```
0                   1                   2
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

```
|     Type      |     Length     |  Value ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

本标准涉及到属性 79（EAP-Message）和属性 80（Message-Authenticator）。

属性 79：EAP 消息（EAP-Message），该属性用来封装 EAP 包，使得 BNAS 在不理解 EAP 的情形下通过 EAP 协议对用户进行认证。BNAS 将从用户得到的 EAP 消息封装在一个或者多个 EAP 属性中，并作为 RADIUS 接入请求的一部分转发给 RADIUS 服务器。RADIUS 服务器在接入质询、接入接受、接入拒绝包中返回 EAP 消息。

接收到不能理解的 EAP 消息的 RADIUS 服务器宜返回 RADIUS 接入拒绝。BNAS 将从对等实体处接收到的 EAP 消息放入一个或者多个 EAP 消息属性中，并在 RADIUS 接入请求消息中转发给 RADIUS 服务器。如果在一个接入请求或者接入质询中包含了多个 EAP 消息属性，它们应按序放入，并且是连贯的。RADIUS 接入接受或者接入拒绝中应只包含一个 EAP 消息属性，它包含 EAP 成功或者 EAP 失败。

EAP 被用来实现各种认证方式，包括强密码系统。为了防止攻击者通过攻击 RADIUS/EAP 来破坏 EAP（例如，修改 EAP 成功或 EAP 失败包），对 RADIUS/EAP 提供和 EAP 认证方法相当的完整性保护是必要的。

因消息认证子属性应用来保护所有包含 EAP 消息属性的 RADIUS 接入请求、接入质询、接入接受和接入拒绝。

RADIUS 服务器宜丢弃包含 EAP 消息属性但不包含消息认证子的 RADIUS 接入请求。支持 EAP 的 RADIUS 服务器应正确地计算消息认证子，并将传送的认证子和计算的认证子不匹配的包丢弃。不支持 EAP 的 RADIUS 服务器在接受到包含 EAP 消息属性的接入请求时应返回接入拒绝。RADIUS 服务器在接受到不能理解的 EAP 消息属性时应返回接入拒绝。

BNAS 宜丢弃包含 EAP 消息属性但不包含消息认证子属性的 RADIUS 接入质询、接入接受和接入拒绝。BNAS 应正确地计算消息认证子并将计算得到的消息认证子和发送的消息认证子不匹配的包丢弃。

EAP 消息属性的格式如下，各字段从左到右发送。

```
0                   1                   2
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |     Length     |     String...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

（1）类型（Type）

79：EAP-Message。

（2）长度（Length）

长度≥3。

（3）字符串（String）

该字段包含 EAP 包。如果在一个包中包含了多个 EAP 消息属性，它们的值将被连接从而使得长度大于 253 字节的 EAP 包能够被 RADIUS 通过 。

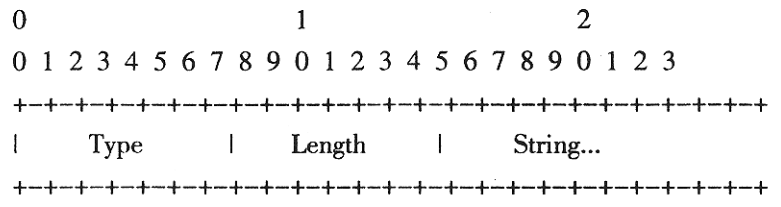
（4）消息认证子（Message-Authenticator）

该属性用来对 RADIUS 接入请求进行签名以阻止对 CHAP、EAP 认证进行欺骗。它可使用于接入请求。该属性应使用于包含 EAP 消息属性的接入请求、接入接受、接入拒绝或者接入质询。

RADIUS 服务器在接收到出现消息认证子的接入请求时应计算正确的消息认证子，并将计算出的消息认证子和发送的消息认证子不匹配的包丢弃。

RADIUS 客户端在接收到出现消息认证子的接入接受、接入拒绝或者接入质询的时候，应计算正确的消息认证子，并将计算出的消息认证子和发送的消息认证子不匹配的包丢弃。

消息认证子属性的格式描述如下，各字段从左到右发送。



（1）类型（Type）

80：Message-Authenticator。

（2）长度（Length）

长度为 18。

（3）字符串（String）

出现在接入请求包（Access-Request Packet）中的时候，消息认证子（Message-Authenticator）是将整个接入请求包（包括类型、ID、长度和认证子（Authenticator））作为输入，使用共享秘密作为密钥，按照 HMAC-MD5 计算出来的校验和，计算方法为：

Message-Authenticator=HMAC-MD5（Type、Identifier、Length、Request Authenticator、Attributes）

计算校验和的时候，签名字符串被认为是长度为 16 的零字节。

对于接入质询（Access-Challenge）、接入接受（Access-Accept）和接入拒绝（Access-Reject）包，消息认证子按照下面的方式计算（使用该包作为应答包的接入请求中的 Request-Authenticator）：

Message-Authenticator = HMAC-MD5（Type、Identifier、Length、Request Authenticator、Attributes）

计算校验和的时候，签名字符串被认为是长度为 16 的零字节。共享秘密作为 HMAC-MD5 散列算法的密钥。

在含有用户口令（User-Password ）属性的时候，该属性是不必要的，但对于阻止针对其他类型的认证的攻击是十分有用的。该属性用来阻止攻击者建立假的网络服务器，然后对 RADIUS 服务器实施在线字典式攻击。但不能防止离线的字典式攻击（攻击者先截获包含如 CHAP 质询和应答的包，然后对这些包进行离线字典攻击）。

该属性为过渡措施，IP 安全的实施将使得该属性是多余的。

9.12 IGMP 协议（可选）

参见 YD/T 1177-2002《IP 组播路由协议》第 5 章 “互联网管理协议 IGMPv2”。

9.13 802.1x 认证（可选）

参见 IEEE Std 802.1x（2001）“基于端口的网络接入控制”。

10 性能和技术指标

10.1 设备容量

宽带网络接入服务器（BNAS）在组网应用中通常放置在网络的汇聚层或汇聚层以下接入层，因此，有必要将宽带网络接入服务器设备从容量上加以划分以适应网络中不同位置对设备容量的需要。

在各地宽带城域网的发展过程中呈现出不均衡状态。对于规模较大的城域网，需要多个汇聚点分散在多处将各自区域的流量进行汇聚，组网时往往会在汇聚层各个汇聚点放置中大型 BNAS 来管理和运营。然而对于规模较小的城域网，接入网分散在各地，在接入层放置小型的 BNAS 就能实现管理和运营。

划分 BNAS 的容量级别主要是以宽带网络接入服务器管理的用户数量为依据。从目前宽带城域网运营模式看，规模较大的城域网在汇聚层的汇聚点需要管理的用户并发数量在 10，000~20，000 之间。而规模较小的城域网接入层汇聚点管理的用户并发数为数千。根据宽带数据网络的发展现状，综合考虑网络扩容和业务的发展，将 BNAS 划分为小容量级和中大容量级两个级别。

小容量级：

系统交换容量位于 2~9.9G 之间；

最少可以同时支持 1000 个活动会话；

最少配置 100 个 VPN 隧道；

包转发速率为 1~5Mpps。

中大容量级：

系统交换容量≥10G；

最少可以同时支持 10000 个活动会话；

最少配置 2000 个 VPN 隧道；

包转发速率≥5Mpps。

10.2 处理能力

PPP 的平均建链时间<5s（含 RADIUS 认证时间）；

每秒处理用户接入认证数≥设备整机并发用户数的 1%。

10.3 服务质量

10.3.1 BNAS 设备的 QoS 支持要求

BNAS 设备作为宽带网络中的重要设备，承担着接入用户管理、业务承载、汇聚及控制等重要功能。目前骨干带宽比较充裕，QoS 保证的瓶颈主要在接入部分，所以在 BNAS 实现流量管理功能，从接入侧实现 QoS 保证，对于全网提供高品质的服务质量将起到十分重要的作用。

10.3.2 流量分类以及优先级服务

BNAS 设备应该能够按照以下规则对流量进行分类，并按照相应的规则映射到 MAC 帧中的 COS 位或 IP 包的 TOS/DSCP 位或 MPLS Exp 位，以实现不同优先级服务，至少应支持 4 种不同的优先级。

a）实现 MAC 层业务类别（可选）

MAC 层业务类别用来对数据帧进行标识和划分优先级。BNAS 设备根据帧的优先级确定帧所属的传输队列，从而实现在桥接 LAN 环境中支持时延敏感业务流的功能，提供 MAC 层的 QoS。

MAC 层业务类别功能遵循 IEEE 802.1p 标准。

b）实现基于端口的优先级分类（可选）

		可用的队列数目（≥4）				
		4	5	6	7	8
用户优先级	0（缺省）	1	1	1	1	2
	1	0	0	0	0	0
	2	0	0	0	0	1
	3	1	1	2	2	3
	4	2	2	3	3	4
	5	2	3	4	4	5
	6	3	4	5	5	6
	7	3	4	5	6	7

能够根据端口号设置优先级，该端口进入的数据帧都属于该优先级，并且在 IP 的 TOS 位标记该优先等级。

c）实现基于 VLAN 的优先级分类（可选）

能够根据 VLAN 设置优先等级，属于该 VLAN 的进入数据帧都属于该优先级，并且在 IP 的 TOS 位标记该优先等级。

d）实现基于用户账号的优先级分类（必选）

该分类方法主要针对采取 PPPoE 接入认证方法的用户。BNAS 设备可以根据 RADIUS 返回的用户属性也可根据本地配置的用户属性获取用户的优先级信息，该用户的业务流都属于该优先级，并且在 IP 的 TOS 位标记该优先等级。

e）实现基于 IP 流或者应用的优先级分类（必选）

能够根据源、目的 IP 地址，或者根据第四层端口号或者它们之间的任意组合来划分优先级，属于该 IP 流或该应用的 IP 包都属于同一个优先级，这个优先级标志在 IP 的 TOS 中设置。

f）实现基于 DiffServ 的优先级分类（可选）

支持 DiffServ 规范所规定的优先级设置。

10.3.3 接入带宽控制及保证

BNAS 设备应支持带宽控制管理功能，可够对用户接入的带宽进行控制和管理，具体要求如下。

a）实现基于用户的带宽控制（必选）

能够根据 RADIUS 服务器返回的用户属性或本地配置的用户属性对用户的接入带宽进行控制。能够实现对用户双向的业务流进行带宽控制，带宽控制的粒度不大于 64k，控制范围可以配置。

b）实现基于端口的带宽控制（可选）

能够对端口的接入带宽进行双向控制，控制范围可以配置。

c）实现基于 VLAN 或 PVC 的带宽控制（必选）

能够对 VLAN 电路或 PVC 的接入带宽进行双向控制，控制范围可以配置，带宽控制的粒度不大于 64k。

d）实现基于应用的带宽限制（可选）

能够对某类应用的带宽进行限制，如限制 FTP 报文不能占用超过 50%的网络带宽。

e）实现基于用户或者应用的带宽保证（必选）

能够为重要的用户或者应用指定恒定的带宽，预先进行资源预留，在网络拥塞时，使它们可获得恒定的带宽保证。

10.3.4 拥塞管理及拥塞避免

10.3.4.1 BNAS 设备拥塞管理的队列机制有以下几种

a）先进先出队列（FIFO）（可选）

先进先出队列（简称 FIFO）不对报文进行分类，按报文到达接口的先后顺序让报文进入队列，在队列的出口让报文按进队的顺序出队，先进的报文将先出队，后进的报文将后出队。

b）优先队列（PQ）（可选）

优先队列（简称 PQ）对报文进行分类，将所有报文依据预先配置分成最多 4 类，按照先进先出的策略分别进入 4 个优先级不同的队列。在报文出队的时候，高优先级的队列相对于低优先级的队列具有绝对的优先权，只有高优先级队列报文发送完毕，较低优先级才得到发送，而且较低优先级的报文会在发生拥塞时被较高优先级的报文抢断。因此采用这种队列机制可以保证在网络发生拥塞的情况下，重要业务（高优先级）的数据传输得到绝对的优先传送。但在较高优先级的报文的速度总是大于接口的速度时，会使较低优先级的报文始终得不到发送的机会。

c）订制队列（CQ）（可选）

订制队列（简称 CQ）根据设置将所有报文分成最多至 17 类，按照先进先出的策略分别进入 1 个系统队列和 16 个用户队列。在出队调度上，系统队列具有绝对的优先权，系统总是先处理完该队列后再处理用户队列；16 个用户队列占用出口带宽的比例可以设置，CQ 按定义的比例使各队列之间在占用的接口带宽上满足管理员预先配置的比例关系。采用这种队列机制，当拥塞发生时，能保证不同业务根据比例获得相应的带宽占用，从而既保证关键业务能获得较多的带宽，又不至于使非关键业务得不到带宽，避免 PQ 的一些缺点。另外，没有拥塞时，各业务可以根据流量中业务的相对比例充分使用接口带宽，提高资源利用率。

d）加权公平队列（WFQ）（必选）

加权公平队列（简称 WFQ）对报文按流进行分类（相同用户会话、源 IP 地址、目的 IP 地址、源端口号、目的端口号、协议号、TOS 相同的报文属于同一个流），每一个流分配到一个队列。在出队发送的时候，WFQ 根据报文分类时设置的流的优先级（Precedence）来分配每个流应占有出口的带宽。优先级的数值越小，所得的带宽越少。优先级的数值越大，所得的带宽越多。在拥塞发生时，它能保证任何流量的流（业务），都能公平地得到一定的带宽占用，减少这个网络的时延，并当流（业务个数）的数目减少时，能自动增加现存流可占的带宽。

10.3.4.2 BNAS 设备避免拥塞的机制可采用以下几种

a）随机早期丢弃（RED）（必选）

将队列的平均占有率作为决定是否触发拥塞避免机制的随机函数的参数。

b）加权随机早期检测（WRED）（必选）

将 IP 优先级和 RED 结合起来，为优先通信流（高优先级）提供与标准通信流（优先级较低）有差别的丢弃阈值。

c）前端丢弃（可选）

通过对队列前端的分组进行丢弃，以避免拥塞。

d）后端丢弃（可选）

通过对队列尾端的分组进行丢弃，以避免拥塞。

10.3.5 QoS 监控

通过对系统 QoS 的监控，可以动态监视网络资源占用情况，以便可以及时调整，具体要求：

a）基于用户的 QoS 监控（必选）

能够针对用户账号，统计其接收包、发送包和包丢失率。

b）基于端口的 QoS 监控（必选）

能够针对接入端口，统计其接收包、发送包和包丢失率。

c）基于 VLAN 或者 PVC 的 QoS 监控（必选）

能够针对 VLAN 电路或者 PVC，统计其接收包、发送包和包丢失率。

d）基于 IP 流或者应用的 QoS 监控（可选）

能够根据源、目的 IP 地址，或者根据第四层端口号或者它们之间的任意组合，统计其接收包、发送包和包丢失率。

10.3.6 QoS 性能指标

a）转发时延<1ms（必选）

在最恶劣情况下，1518Byte 长度及以下的包时延均应<1ms。

b）性能影响率<5%（必选）

启动相关 QoS 支持功能后，系统性能指标下降比例应<5%。

10.3.7 用户访问控制权限

支持对每个用户实施不同的访问控制，如上网时长或时间区间、带宽、优先级、ACL、协议支持（如组播）、其他网络、协议、业务资源的授权使用等。

10.4 用户接入认证技术指标

宽带网络接入服务器对用户进网时用户的信用进行认证。宽带网络接入服务器是用户接入认证请求的发起端，它使用 RADIUS 协议向接入认证服务器发出用户接入认证的请求。它接收来自用户接入认证服务器的用户认证响应，据此响应授于请求接入用户接入的权限。接入服务器的接入认证由两阶段组成：

一是拨号用户和宽带网络接入服务器 BNAS 之间的接入认证，包括：PAP、CHAP、EAP（可选）、802.1x（可选）；

一是宽带网络接入服务器 BNAS 和 RADIUS 服务器之间的认证。应支持 PAP 和 CHAP 认证、支持 EAP 认证（可选）、支持 802.1x 认证（可选）。

PAP/CHAP 认证符合 RFC 1994 规范；EAP 认证符合 RFC 2284 规范和 802.1X 规范；RADIUS 认证、

授权、计费符合 RFC 2865、RFC 2866 和 RFC 2869 规范；RADIUS 服务器采用服务器/客户机结构，采用 UDP 协议作为传输协议。

除了标准的 AAA Client 外，接入服务器还有必要实现一个本地 AAA Server 子系统（可选），用于在本地对诸如具备系统管理权限的系统管理级用户进行鉴权和审计，以及在与远端 RADIUS Server 通信中断时在本地保存 AAA 信息等。

对于 PPPoE 实现，认证可根据实际需求在 PPP 这一层次实现，或者在 Ethernet 这一层次以 802.1x 的形式实现。在不同层次的实现可以实现不同的认证粒度。

对于 PPPoA、PPPiFR 实现认证在 PPP 这一层次实现。

可以实现接入用户主机的 MAC 地址、IP 地址、VLAN ID、端口号、用户名、口令等的用户参数的认证。进行认证是 BNAS 上报 MAC 地址。

为了保证用户安全，宽带接入服务器支持对用户主机的 MAC 地址、IP 地址、VLAN ID、端口号、账号、VC 等进行绑定的功能（可选）。参数绑定的具体组合方式为可选。

用户接入认证的平均响应时间<5s（不包括漫游用户）；

用户异常掉线重拨延时<10s；

每秒处理用户接入认证数≥设备整机并发用户数的 1%；

用户接入认证差错率（误判率）<0.1%。

用户接入认证的成功率：

负载为 90%时的认证成功率≥95%；

负载为 50%时的认证成功率≥96%；

负载为 10%时的认证成功率≥97%。

认证、授权的 RADIUS 服务器应有主备用和负荷分担；宽带网络接入服务器应支持一个主用 RADIUS 服务器和一个以上备用 RADIUS 服务器。

用户计费技术指标

用户计费时长精度≤1s；

用户计费相对流量精度≤10%；绝对流量精度≤1MBytes；

用户计费差错率≤0.01%。

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

系统的平均无故障工作时间：MTBF>10000h。

3）故障恢复时间

系统故障恢复时间<1h。

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。

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℃~30℃，相对湿度保持 40%~65%；

b）短期工作条件：温度保持 0℃~45℃，相对湿度保持 20%~90%。

注：

1）宽带网络接入服务器正常工作的温度和相对湿度的测量点，是指在地板上方 2m 和接入服务器前方 0.4m 处的测量值。

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%的环境应采用抗静电地面。

11.2 防尘要求

机房内直径>5μm 的灰尘浓度≤3 ×104 粒/m3；灰尘粒子应是非导电、导磁和腐蚀性的。

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）从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（μV/m）	频率（MHz）	电磁强度 dB（μV/m）
0.01~0.024	148.6-60lg*d*	47.7/*d*~88	59.1-20lg*d*
0.024~0.8	116.2-60lg*d*-20lg*f*	88~216	63.6-20lg*d*
0.8~1.59	118.2-60lg*d*	2160~10000	66.6-20lg*d*
1.59~47.7/*d*	120.2-60lg*d*-40lg*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（μV/m）表示微伏（μV/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无线电电磁干扰的要求

频率（MHz）	最大线路电流 dB（μA）
0.000061~0.001	I-20lg*f*-84.4
0.001~0.01	（124.4-I）lg*f*+348.8-2I
0.01~0.8	-21.05lg*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. dBμA 表示微安（μA）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（μA）
0.01~0.8	-21.05lg*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 140dBμV/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外界电磁干扰的要求见表 4，0.01~100MHz 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（μA）
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~-40V。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：

300~3400Hz 杂音电压≤2mV；

0~300Hz 峰值杂音电压≤4mV；

3.4~15kHz 宽带杂音电压≤100mV 有效值；

150kHz~30MHz 宽带杂音电压≤30mV 有效值。

c）离散频率杂音电压

3.4~15kHz，≤5mV 有效值；

150~200kHz，≤3mV 有效值；

200~500kHz，≤2mV 有效值；

500~2MHz，≤1mV 有效值。

d）交流电压及其波动范围要求

单相（220±10%）V，频率（50±5%）Hz；

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<3Ω。

13　例行试验

13.1　低温试验

应符合 GB 2423.1 的要求。

13.2　高温试验

应符合 GB 2423.2 的要求。

13.3　恒定湿热试验

应符合 GB 2423.9 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 3 级公路上以 25~40km/h 的速度行驶 200 km 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 GB 3873 的有关规定。

13.6 标志、包装和运输、储存

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

外包装应有包装储运图示标志，应按 GB 191 有关规定执行。

13.6.3 包装

随机文件：产品合格证、使用说明书以及产品随机备附件清单。

产品包装要求：应符合 GB 3873 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，并应按包装箱上标明方向放置。

中华人民共和国
通信行业标准
网络接入服务器技术要求
——宽带网络接入服务器
YD/T 1148-2005
*
人民邮电出版社出版发行
北京市崇文区夕照寺街14号A座
邮政编码：100061
电话：68372878
北京地质印刷厂印刷

*
开本：880×1230　1/16　　2005年7月第1版
印张：3.25　　2005年7月北京第1次印刷
字数：100千字
ISBN 7-115-1091/05-65
定价：35.00元
本书如有印装质量问题，请与本社联系　电话：(010)68372878