ICS 33 040 40
M 32

YD

# 中华人民共和国通信行业标准

YD/T 1658-2007

# 宽带网络接入服务器安全技术要求

Technical Specification for Broadband Network Access Server Security



2007-07-20 发布　　2007-12-01 实施

中华人民共和国信息产业部　发布

# 目　　次

# 前　言

本标准是“宽带网络接入服务器安全”系列标准之一。该系列标准预计的结构及名称如下：

1．YD/T 1658-2007　宽带网络接入服务器安全技术要求

2．YD/T 1659-2007　宽带网络接入服务器安全测试方法

其中，YD/T 1659-2007《宽带网络接入服务器安全测试方法》是本标准的配套标准。

本标准在制定过程中还参考了YD/T 1148-2005《网络接入服务器技术要求——宽带网络接入服务器》和YD/T 1358-2005《路由器设备安全技术要求——中低端路由器（基于IPV4）》。

本标准的附录A、附录B均为资料性附录。

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：信息产业部电信研究院

本标准主要起草人：马军锋、魏　亮

# 宽带网络接入服务器安全技术要求

## 1 范围

本标准规定了宽带网络接入服务器安全技术的基本要求，包括数据转发平面、控制平面和管理平面的安全威胁和安全服务要求，以及标识验证、数据保护、系统功能保护、资源分配、安全审计、安全管理、可信信道/路径和系统访问共8个安全功能需求。

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/T 18336.2　信息技术 安全技术 信息技术安全性评估准则 第2部分：安全功能要求

YD/T 1045-2000　网络接入服务器（NAS）技术规范

YD/T 1148-2005　网络接入服务器技术要求——宽带网络接入服务器

YD/T 1358-2005　路由器设备安全技术要求——中低端路由器（基于IPv4）



## 3 定义和缩略语

下列定义和缩略语适用于本标准。

### 3.1 定义

**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（PATN/ISDN）与 IP 网之间，将拨号用户接入 IP 网，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。

**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 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。

**访问控制（access control）**

防止未经授权使用资源。

**可确认性（accountability）**

确保一个实体的行为能够被独一无二地跟踪。

**授权（authorization）**

授予权限，包括根据访问权进行访问的权限。

**可用性（availability）**

根据需要，信息允许授权实体访问和使用的特性。

**保密性（confidentiality）**

信息对非授权个人、实体或进程是不可知、不可用的特性。

**数据完整性（data integrity）**

数据免遭非法更改或破坏的特性。

**拒绝服务（denial of service）**

阻止授权访问资源或延迟时间敏感操作。

**数字签名（digital signature）**

附在数据单元后面的数据，或对数据单元进行密码变换得到的数据。允许数据的接收者证明数据的来源和完整性，保护数据不被伪造，并保证数据的不可否认性。

**加密（encryption）**

对数据进行密码变换以产生密文。

注:加密可以是不可逆的， 在这种情况下， 相应的解密过程便不能实际实现了。

**基于身份的安全策略（identity-based security policy）**

这种安全策略的基础是用户或用户群的身份或属性，或者是代表用户进行活动的实体以及被访问的资源或客体的身份或属性。

**密钥（key）**

控制加密与解密操作的一序列符号。

**密钥管理（key management）**

根据安全策略产生、分发、存储、使用、更换、销毁和恢复密钥。

**冒充（masquerade）**

一个实体伪装为另一个不同的实体。

**完整性破坏（integrity compromise）**

数据的一致性通过对数据进行非授权的增加、修改、重排序或伪造而受到损害。

**抵赖（repudiation）**

在一次通信中涉及到的那些实体之一不承认参加了该通信的全部或一部分。

**基于规则的安全策略（rule-based security policy）**

这种安全策略的基础是强加于全体用户的总体规则。这些规则往往依赖于把被访问资源的敏感性与用户、用户群或代表用户活动的实体的相应属性进行比较。

**安全审计（security audit）**

对系统的记录及活动独立的复查与检查，以便检测系统控制是否充分，确保系统控制与现行策略和操作程序保持一致、探测违背安全性的行为，并通告控制、策略和程序中所显示的任何变化。

**安全策略（security policy）**

提供安全服务的一套准则，包括“基于身份的安全策略”与“基于规则的安全策略”。

**安全服务（security service）**

由参与通信的开放系统层所提供的服务，它确保该系统或数据传送具有足够的安全性。

## 3.2 缩略语

| | | |
|---|---|---|
| 3DES | Triple DES | 三重数据加密标准 |

| | | |
|---|---|---|
| AAA | Authentication Authorization Accounting | 鉴别、授权、计费 |
| ACL | Access Control List | 访问控制列表 |
| ACCM | Asynchronous-Control-Character-Map | 异步控制字符映射 |
| ACFC | Address-and-Control-Field-Compression | 地址、控制域压缩 |
| AES | Advanced Encryption Standard | 高级加密标准 |
| AH | Authentication Header | 验证报文头协议 |
| ARP | Address Resolution Protocol | 地址解析协议 |
| ATM | Asynchronous Transfer Mode | 异步转移模式 |
| BGP | Border Gateway Protocol | 边界网关协议 |
| CAR | Committed Access Rate | 承诺接入速率 |
| CHAP | Challenge Handshake Authentication Protocol | 质询握手认证协议 |
| CMTS | Cable Modem Terminal System | 线缆调制解调器终端系统 |
| CPU | Central Processing Unit | 中央处理单元 |
| DHCP | Dynamic Host Configuration Protocol | 动态主机配置协议 |
| DoS | Denial of Service | 拒绝服务攻击 |
| DLCI | Data Link Control Identity | 数据链路控制标识 |
| DNS | Domain Name System | 域名解析系统 |
| DSLAM | Digital Subscriber Line（DSL）Access Module | 数字用户线接入模块 |
| CHAP | Challenge Authentication Protocol | 质询认证协议 |
| EAP | Extensible Authentication Protocol | 扩展认证协议 |
| ESP | Encapsulation Secure Payload | 封装安全净荷协议 |
| FCAPS | Fault，Configuration，Accounting，Performance and Security | 故障，配置，计费，性能，安全 |
| FCS | Field Check Sequence | 域校验序号 |
| FR | Frame Relay | 帧中继 |
| FTP | File Transfer Protocol | 文件传输协议 |
| GTSM | Generalized TTL Security Mechanism | 通用 TTL 安全机制 |
| HMAC | Hashed Message Authentication Code | 散列消息验证码 |
| ICMP | Internet Control Message Protocol | 互联网控制报文协议 |
| IKE | Internet Key Exchange | 互联网密钥交换协议 |
| IP | Internet Protocol | 互联网协议 |
| IPsec | IP Security | IP 安全机制 |
| ISDN | Integrated Service Digital Network | 综合业务数字网 |
| IS-IS | Intermediate System to Intermediate System | 中间系统—中间系统 |
| L2TP | Layer Two Tunneling Protocol | 二层隧道协议 |
| LAC | L2TP Access Concentrator L2TP | 接入集中器 |
| LDP | Label Distribution Protocol | 标记分发协议 |

| | | |
|---|---|---|
| LL | Leased Line | 专线 |
| LNS | L2TP Network Server | L2TP 隧道网络服务器 |
| LSP | Label Switch Path | 标记交换路径 |
| MAC | Media Access Control | 媒质访问控制 |
| MD5 | Message Digest 5 | 报文摘要 5 |
| MIB | Management Information Base | 管理信息库 |
| MPLS | Multi Protocol Label Switching | 多协议标记交换 |
| MRU | Maximum Receive Unit | 最大接收单元 |
| NATP | Network Address Port Translation | 网络地址端口翻译 |
| NAT | Network Address Translation | 网络地址翻译 |
| OAM&P | Operation，Administration，Maintenance and Provisioning | 操作，管理，维护和配置 |
| OSPF | Open Shortest Path First | 最短路径优先 |
| PAP | Password Authentication Protocol | 密码认证协议 |
| PPP | Point-to-Point Protocol | 点到点协议 |
| PPPoA | PPP over ATM | ATM 承载 PPP 协议 |
| PPPIFR | PPP In Frame Relay | 帧中继承载的 PPP 协议 |
| PPPoE | PPP over Ethernet | 以太网承载 PPP 协议 |
| PSTN | Public Switched Telephone Network | 公众电话网 |
| PVC | Permanent Virtual Circuit | 永久性虚电路 |
| RAS | Remote Access Server | 远程接入服务器 |
| RIP | Route Information Protocol | 路由信息协议 |
| RSVP | Resource Reservation Protocol | 资源预留协议 |
| SHA-1 | Secure Hash Algorithm 1 | 安全散列算法 1 |
| SLA | Service Level Agreement | 服务水平协议 |
| SMC | Service Management Center | 业务管理中心 |
| SNMP | Simple Network Management Protocol | 简单网管协议 |
| SSH | Secure Shell | 安全外壳程序协议 |
| TCP | Transmission Control Protocol | 传输控制协议 |
| TTL | Time to Live | 生命周期 |
| UDP | User Datagram Protocol | 用户数据报协议 |
| USM | User-based Security Model | 基于用户的安全模型 |
| uRPF | Unicast Reverse Path Filter | 单播反向路径检查 |
| VLAN | Virtual Local Area Networks | 虚拟局域网 |
| VCI | Virtual Channel Identity | 虚信道标识 |
| VPI | Virtual Path Identity | 虚通道标识 |
| VPN | Virtual Private Network | 虚拟专用网 |

## 4 安全框架模型

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，主要用于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。

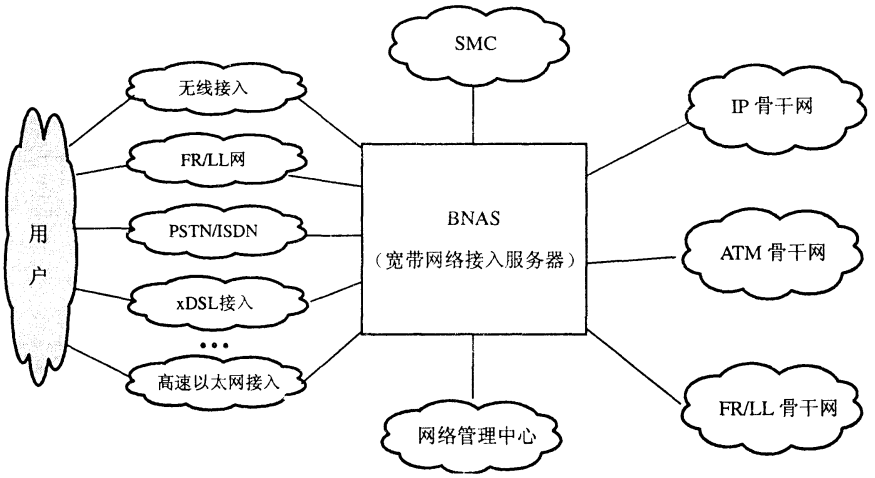


**图1 宽带网络接入服务参考结构**

宽带网络接入服务器在网络中处于汇接层面，通常面向各种类型的接入设备（如DSLAM、CMTS、RAS等），因此很容易遭受到来自网络和其他方面的威胁，这些安全威胁可以利用设备自身的脆弱性或者是配置上的策略漏洞，给设备造成一定的危害，而且设备一旦被攻击，性能和正常运行都将会受到很大的影响，甚至造成拒绝对正常用户的访问服务。

本标准将宽带网络接入服务器的功能划分为三个平面。

（1）数据平面：主要是提供用户数据的转发。宽带网络接入服务器应当可以工作在下述模式下：PPP 终结模式，即由宽带网络接入服务器终结用户发起的 PPP 连接；PPP 中继模式，即宽带网络接入服务器透传用户的 PPP 连接由后继设备（如路由器）终结用户的 PPP 连接；DHCP+Web 以太网接入模式。

（2）控制平面：主要包括路由协议（单播及组播路由协议）等控制信令，提供与建立会话连接、控制转发路径等有关的功能，并且可以采用两种方式（即 DHCP 中继或者是自身作为 DHCP 服务器）来负责用户地址的动态分配与管理；应支持 PPPoE、DHCP+Web 用户接入认证方式。

（3）管理平面：主要是指与 OAM&P 有关的功能，如 SNMP、管理用户 Telnet 登录、日志等，支持 FCAPS 功能。管理平面的消息传送可以采用带内和带外两种形式。

为了抵御来自网络和用户的攻击，宽带网络接入服务器必须提供一定的安全功能。本标准裁减 GB/T 18336-2 中定义的安全功能并应用到宽带网络接入服务器中，这些安全功能包括：

- 标识和验证。识别并确认用户的身份。
- 用户数据保护。保护用户数据的完整性、可用性和保密性。
- 系统功能保护。对实现系统关键功能包括安全功能所需要的数据（如用户身份和口令）的保护，确保相关数据的完整性、可用性和保密性。
- 资源分配。控制用户对资源的访问，不允许用户过量占用资源，避免因为非法占用资源造成系统对合法业务拒绝服务。
- 安全审计。能够提供日志等审计记录，这些记录可以用来分析安全威胁活动和指定安全对策，

探测违背安全性的行为。

- 安全管理。安全功能、数据和安全属性的管理能力。
- 可信信道/路径。宽带接入服务器同其他设备间通信的信道/路径要求可信，对于安全数据的通信要同其他通信隔离开来。
- 系统访问。管理和控制用户会话的建立。

宽带网络接入服务器安全框架如图 2 所示。

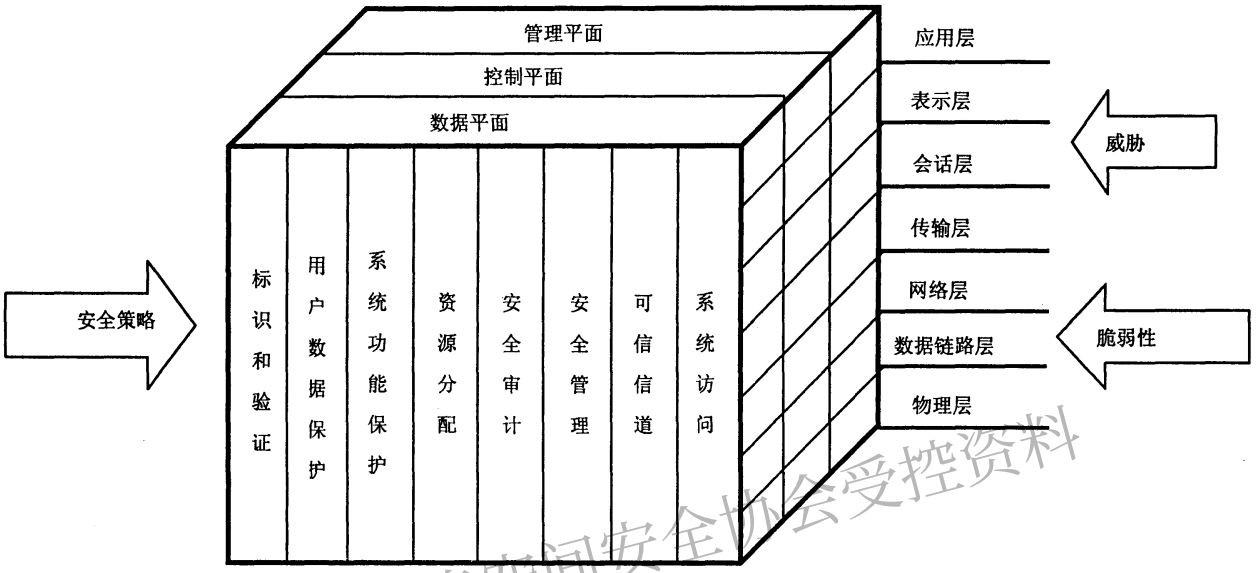


图 2 宽带网络接入服务器安全框架



为了确保宽带网络接入服务器自身和转发数据的安全，需要在实际组网中制定相应的安全控制策略，并将该策略分别映射到数据平面、控制平面和管理平面。

## 5 数据平面安全

### 5.1 安全威胁

宽带网络接入服务器面向不同类型的接入设备，是一种能够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。在网络侧，用户的数据都必须经由此设备来处理，因此基于流量的攻击会对设备的性能造成很大影响，如大流量攻击可能会影响设备对正常用户数据进行处理，处理畸形报文可能会占用大量的CPU和内存资源，所以需要提供安全机制来限定用户流量行为，抵御来自网络攻击者对数据平面的恶意攻击。

此外，对数据流未经授权的观察、修改、插入和删除操作，会破坏数据流的完整性、可用性和保密性。宽带网络接入服务器数据平面的安全威胁主要有以下方面，但不局限在这些方面：

- 对数据流进行流量分析，从而获得用户数据的敏感信息；
- 未经授权的观察、修改、插入和删除用户数据；
- 利用用户数据流进行分布式的 DoS 攻击。

### 5.2 安全功能

#### 5.2.1 标识和验证

##### 5.2.1.1 标识

宽带网络接入服务器可以支持不同类型的用户接入方式，包括：

- PPP 用户接入；
- 以太网用户接入；
- 专线用户接入。

#### 5.2.1.1.1 PPP 用户接入

宽带网络接入服务器可以工作在PPP终结和PPP中继两种模式下，在终结模式下对于不同的封装格式，应当采用不同的用户标识方法：

1）采用PPPoE的封装格式，可以采用MAC地址、VLAN_ID、端口号、IP地址、账号等组合绑定的形式来标识用户，并结合PPPoE_Session_Id来标识用户会话。

PPPoE（RFC2516）建议进行魔数（magic number）选项协商，不建议进行协议域压缩选项协商，实现中必须不请求进行下面的选项协商，并且必须拒绝此类选项协商的请求：

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

MRU必须不能大于1492。

2）采用PPPoA的封装格式，可以采用VCI/VPI、端口号、IP地址、账号等组合绑定的形式来标识用户。

3）采用PPPIFR的封装格式，可以采用DLCI、端口号、IP地址、账号等组合绑定的形式来标识用户。

#### 5.2.1.1.2 以太网用户接入

对于以太网用户接入方式，宽带网络接入服务器可以采用VLAN_ID、MAC地址、端口号、IP地址、账号等组合绑定的形式来标识一个用户。

#### 5.2.1.1.3 专线用户接入

对于专线用户接入，宽带网络接入服务器可以采用端口号和账号绑定的形式来标识一个用户。

### 5.2.1.2 验证

#### 5.2.1.2.1 概述

宽带网络接入服务器应当设置不同的访问控制策略来控制用户的接入，同时应可以选择不同的认证协议（如CHAP、802.1x）对用户进行身份验证。此外，为增强系统安全性，应可选支持EAP协议和RADIUS扩展协议，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用户的连接进行接入验证。

宽带网络接入服务器宜采用两种认证方式：

- 本地认证，即认证点就在宽带网络接入服务器上；
- 远端认证，即宽带网络接入服务器将用户认证信息通过认证协议（如 RADIUS）传递到认证服务器进行认证。

#### 5.2.1.2.2 PPP 用户认证

对于PPP用户的接入，宽带网络接入服务器应采用CHAP、PAP或者EAP协议进行认证。对于PPP中继模式，则由宽带网络接入服务器按照上行链路的封装格式封装后交由后继设备（如汇聚路由器）进行认证。为保证认证信息在传输过程中的安全，可以考虑通过建立L2TP隧道或IPSec隧道提供保护。

#### 5.2.1.2.3 以太网用户认证

对于以太网接入用户，宽带网络接入服务器宜实现802.1x认证协议，具体内容参见附录B部分。此外也可选实现Web Portal认证方式。

### 5.2.2 数据保护

宽带网络接入服务器应当可以为用户提供IP安全服务，通过建立IPSec隧道，为用户数据提供完整性、数据源身份认证、保密性以及防重放攻击的保护。应支持AH和ESP协议，支持传输模式和隧道模式，支持安全联盟手工建立和IKE协议自动建立两种方式。

AH协议应支持HMAC-SHA1-96验证算法，可支持HMAC-MD5-96验证算法。

ESP协议应支持HMAC-SHA1-96验证算法，可支持HMAC-MD5-96验证算法。

加密算法应支持空加密算法、3DES-CBC加密算法，可支持DES-CBC、AES-CBC和国家规定的标准分组加密算法。

如果宽带网络接入服务器支持动态密钥管理IKE协议，则应支持IKE的下列特性：

- 支持安全联盟的手工管理和 IKE 自动管理。在手工管理安全联盟时，可支持以十六进制配置算法所需密钥，应支持任意长度字符串形式配置密钥；
- 支持预共享密钥验证，可支持数字证书验证和 RSA 加密 Nonce 验证；
- 应支持 3DES 加密算法，应支持 SHA1 完整性验证算法，可支持 MD5 完整性验证算法，同时还可支持 DES、AES 加密算法和国内的分组加密算法；
- 在 IKE 的 DH 交换中，应支持 MODP-Group1、MODP-Group2；
- 阶段 2 交换中应支持完美前向保护特性；
- 阶段 1 应支持主模式和野蛮模式，阶段 2 应支持快速模式，还应支持信息交换；
- 可支持 NAT 穿越；
- 在 IKE 阶段 1 中应该能指定发起模式；
- 在 IKE 的阶段 2 协商中，应支持 ID_IPv4_ADDRESS 和 ID_IPV4_SUBNET 身份载荷。

此外，宽带网络接入服务器应能够建立 L2TP 隧道为用户数据提供保护，实现 LAC 功能特性，可选实现 LNS 的功能特性。



### 5.2.3 系统功能保护

对于用户数据，系统要提供妥善的保护手段，通过基于角色的分级访问控制机制来实现控制对此类数据的访问（包括用户、系统进程等）。

### 5.2.4 资源分配

宽带网络接入服务器应能够提供有效的控制机制（如队列调度机制、接入带宽控制）保障网络带宽的合理利用，特别是要能够抵御来自网络的各种侵占网络资源类的攻击，如Ping Flooding、TCP SYN Flooding等，要确保网络在遭受攻击的情况下仍旧能够为合法用户提供必需的数据转发服务。

宽带网络接入服务器应能构抵御以下的常见攻击类型，但并不局限于这些方面。

- 大流量攻击。大流量可以分成两种类型：一种是流经流量，即需要宽带接入服务器转发的流量，对于这类攻击，宽带网络接入服务器宜具有端口线速转发的能力，对于超过端口处理能力的流量可以采用按比例丢弃的策略；另一种流量的目的地就是宽带网络接入服务器本身，这类攻击可能会占用被攻击设备的大量 CPU 处理时间和内存，严重的甚至会造成设备崩溃，导致中断无法为用户提供正常服务。对这类攻击流量，宽带网络接入服务器宜采取过滤和丢弃策略，同时应将必要的信息（如报文类型、源地

址以及攻击时间等）记录到安全日志中。

- 畸形包处理。宽带网络接入服务器应能够处理各种类型的畸形包（如超长、超短包）、链路层错误包、网络层错误包、上层协议错误包等，对于这些报文应采取丢弃策略，不能影响设备的正常功能。此外，也要保证宽带网络接入服务器自身不会产生上述类型的畸形包。
- 定向广播报文攻击。SMURF 攻击是一种利用定向广播报文的分布式 DoS 攻击方法。对于此类攻击，宽带网络接入服务器应能够提供控制策略，禁止该类报文转发或者以广播形式转发，对于分布式 DoS 攻击，应能够提供简单策略阻止这种分布式 DoS 攻击向其他设备扩散。
- IP 地址哄骗。针对网络中源地址哄骗报文，宽带网络接入服务器宜实现单播逆向路径转发（uRPF）技术来过滤这类报文，禁止其在网络中传播。

宽带网络接入服务器应能够提供相应机制来控制同一用户建立 TCP 会话的数量，以防止用户过渡消耗网络资源；而且应能够根据用户类型对能够建立的 TCP 会话数量进行配置。

宽带网络接入服务器应实现IP filter和IP Pool功能，来控制用户接入和过滤用户数据。IP filter提供IP包过滤功能，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则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。

宽带网络接入服务器应实现基于ACL的用户流量控制，通过CAR操作，对用户数据流进行整形，然后依据与用户签订的SLA协定，为用户分配带宽资源。SLA协议包含承诺速率、峰值速率，承诺突发流量、峰值突发流量等，对于超出SLA协定的流量可以采取降级、丢弃等操作。

#### 5.2.5 安全审计

对于用户流量，宽带网络接入服务器应能够提供流量日志能力，相关的要求参见7.2.5节有关安全日志方面的规定。

#### 5.2.6 安全管理

要能够提供对本章节提供的安全功能和数据的管理能力，管理方式包括但不限于控制台、远程连接或网络管理接口/系统等方式。

#### 5.2.7 可信信道/路径

宽带网络接入服务器同其他设备通信的信道/路径要求可信，对于传送敏感数据（如专线用户数据）的通信同传送其他数据的通信隔离开来，可以采用物理隔离或者是VPN逻辑隔离。

#### 5.2.8 系统访问

##### 5.2.8.1 访问控制列表

访问控制是一种安全手段，它控制用户和系统与其他的系统和资源进行通信和交互。它能够保护系统和资源免受未经授权的访问，并且在认证过程成功结束后授权访问的等级。访问控制能够提供控制、限制、监控以及保护资源的可用性、完整性和机密性等能力。

宽带网络接入服务器应能够提供基于源/目的IP地址、源/目的端口和协议类型等元素的过滤，支持对ICMP报文进行过滤，支持对报文优先级进行过滤，支持对报文匹配情况进行统计计数和记入日志等。

##### 5.2.8.2 NAT 功能（可选）

NAT可以解决IPv4地址资源缺乏的问题，同时通过NAT可以实现内网和外网的隔离，同时内网能够访问外网资源。

宽带网络接入服务器实现NAT宜支持如下的功能：

- 支持网络地址翻译和网络地址/端口翻译；
- 支持混合编制方式，对于来自私网地址的报文直接进行转发；
- 支持黑名单，对于黑名单中的地址不进行地址转换和转发；
- 支持对不同等级用户并发连接数的限制；
- 支持 FTP、DNS 等应用网关协议；
- 支持输出 NAT 日志。

如果宽带网络接入服务器实现 NAT 功能，不应当对设备的处理性能造成显著影响。

#### 5.2.8.3 VPN 功能

宽带网络接入服务器宜实现 VPN 功能，通过 VPN 来实现不同用户数据的隔离，阻止公网用户对 VPN 内的设备和业务进行攻击。在实现上要确保不同 VPN 信息不能够相互泄漏，同时应采取必要的路由过滤策略保证 VPN 路由表和 MAC 表的容量不会溢出。

## 6 控制平面安全

### 6.1 安全威胁

宽带接入服务器的控制平面主要负责路由信息的学习、客户端地址的动态管理以及与AAA服务器协同完成用户的认证授权。

控制平面的安全威胁主要有以下几个方面，但不局限于这些方面：

- 未授权对协议流进行探测、或者进行流量分析，从而获得转发路径信息或者是用户的认证信息；
- 获得设备服务的控制权，暴露转发路径信息，包括将转发路径信息暴露给非授权设备，VPN 路由的泄漏；
- 利用协议的拒绝服务攻击，如利用 ICMP 协议的 Smurf 攻击，利用路由协议、MPLS 标签分配协议的拒绝服务攻击，利用面向连接协议的半连接攻击等；
- 非法设备进行身份哄骗，建立路由协议、MPLS 标签分配协议等的实体信任关系，非法获得转发路径信息；
- 针对路由协议、MPLS 标签分配协议等的转发路径信息的欺骗；
- 针对 DHCP 地址资源耗尽型的拒绝服务攻击。

### 6.2 安全功能

#### 6.2.1 标识验证

##### 6.2.1.1 用户标识

控制层面的用户标识验证可参见5.2.1节。

##### 6.2.1.2 路由认证

宽带网络接入服务器通过路由协议来传递路由信息，计算到达目的网络的最佳路由，因此必须确保路由信息的完整性和可用性，并且对路由信息通告者的真实身份进行认证，以免造成恶意的攻击者冒充路由对等体通告不正确或者是不一致的路由信息导致网络服务的不可达。

宽带接入服务器应实现基于MD5算法的路由协议认证，具体要求如下：

- RIPv2 协议应支持 MD5 或 SHA-1 认证；
- OSPFv2 协议应支持 MD5 或 SHA-1 认证；

- IS-IS 协议应支持 MD5 或 SHA-1 认证；
- BGP4 协议应支持 MD5 或 SHA-1 认证。

对于MPLS，用于建立LSP的标签分配协议主要有RSVP-TE和LDP/CR-LDP两种。

- LDP/CR-LDP 协议。发现交换过程使用的消息是由 UDP 协议承载，对于基本 Hello 消息，宽带网络接入服务器应只接收与可信 LSR 直接相连接口上的基本 Hello 消息，忽略地址不是同一子网内组播组的基本 Hello 消息；对于扩展 Hello 消息，可利用访问列表控制只接收允许的源发送来的扩展 Hello 消息。LDP 会话过程使用的消息是由 TCP 协议承载，应通过 TCP MD5 签名选项对会话消息进行真实性和完整性验证。
- RSVP-TE 协议。应通过加密的散列函数支持邻居验证，从而实现逐跳验证机制，应支持 HMAC-MD5 算法，建议实现 HMAC-SHA1 算法。

此外，宽带网络接入服务器也可选实现通用TTL安全机制（GTSM）来提供对控制信令的简单保护，具体内容参见附录A。

#### 6.2.2 数据保护

宽带网络接入服务器控制平面的信息主要包括路由信息、用户认证信息以及地址分配信息。对于这些信息要能够提供完整性、保密性和可用性保护，在实现上可以通过建立L2TP或IPSec逻辑安全隧道（IPSec的要求参见5.2.2节），并对数据进行加密保护。

#### 6.2.3 系统功能保护

用于系统控制平面的安全数据（如路由协议的认证密钥、用户地址池信息）应得到妥善的保护。

#### 6.2.4 资源分配

##### 6.2.4.1 物理资源分配

控制信息的运算和存储需要消耗大量的CPU运算资源和内存存储资源，因此在控制平面应支持路由控制策略和路由过滤，抑制攻击者利用路由协议的安全缺陷进行资源耗尽型的攻击。

##### 6.2.4.2 可关闭一些 IP 服务

###### 6.2.4.2.1 ICMP 协议

ICMP作为TCP/IP协议栈的基本协议之一，主要用于网络操作和故障排除，由于协议自身存在安全漏洞导致被利用于攻击网络，因此要求宽带网络接入服务器具有关闭相关ICMP功能的能力，包括：

- Type = 0 回显应答；
- Type = 3 目的地不可达；
- Type = 5 重定向；
- Type = 8 回显要求；
- Type = 11 超时。

###### 6.2.4.2.2 IP 源路由选项

IP源路由选项取消了报文传输路径中的各个设备的中间转发决策过程，可能被恶意攻击者利用，刺探网络结构或者是聚合用户流量对第三方设备进行攻击。宽带网络接入服务器如果提供该功能，应提供关闭IP源路由选项功能的能力。

注：IP源路由允许指定一条数据包必须经过的路径，它包括两种类型：宽松的源路由选项（发送端指明了流量或者数据包必须经过的IP地址清单，但如果它需要，也可以经过一些其他的地址）和严格的源路由选项（发送端指明IP数据包必须经过的确切地址，如果没有经过这一确切路径，数据包会被丢弃，并返回一个ICMP差错报文）。

#### 6.2.4.2.3 代理 ARP

代理ARP的功能就是网关设备代替被询问设备用自己的MAC地址应答ARP请求，它能够帮助一个子网的主机不用配置默认网关到达远端子网。该服务能够被攻击者利用导致拒绝服务或者是窃取敏感信息（中间人攻击），因此如果宽带网络接入服务器提供该功能，应提供关闭此功能的能力。

#### 6.2.4.2.4 其他服务开关

宽带网络接入服务器缺省关闭TCP和UDP小端口服务，或者不提供这些服务模型。缺省关闭或不提供下列小端口服务：

- Echo；
- Chargen；
- Finger；
- NTP；
- 其他小端口服务。

#### 6.2.4.3 DHCP 防盗用及攻击

宽带网络接入服务器应支持两种模式来管理接入用户的地址分配：一种模式是由宽带接入服务器作为DHCP的服务器；另一种模式是宽带接入服务器作为DHCP代理，中继DHCP客户请求到DHCP服务器。在地址分配过程中，应将地址分配与用户标识信息结合起来（如VLAN ID、PVC、MAC地址、端口等），以免非法用户盗取地址信息。同时也要控制在同一PVC或者是VLAN下用户申请的IP数目，防止地址资源被攻击耗尽，导致正常用户的请求被拒绝。

如果宽带网络接入服务器支持DHCP中继功能，DHCP中继宜支持选项82（option 82:Relay agent information option），这样宽带网络接入服务器不但在物理上隔离用户和DHCP服务器，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。

此外在无法实现二层隔离的情况下，应实现防范DHCP服务欺骗的功能。

### 6.2.5 安全审计

对控制平面的控制信息要提供日志记录功能，特别是对设备的路由表、动态地址分配等重要数据有影响的控制数据。

宽带网络接入服务器可以支持端口镜像功能，通过配置，将系统中某个端口的部分或者全部流量镜像到其他的端口，出方向的报文和入方向的报文可以分别镜像到不同的端口。此外可选支持向远端安全中心进行数据镜像的功能。

端口镜像时，对帧不进行修改，有如下两种镜像类型：

- 一对一端口镜像，把一个端口的流量全部原封不动地拷贝到指定地镜像端口；
- 多对一端口镜像。

### 6.2.6 安全管理

要能够提供控制平面的安全功能和安全数据管理能力，管理方式包括但不限于控制台、远程连接或网络管理接口/系统等方式。

#### 6.2.7 可信信道/路径

宽带网络接入服务器与其他设备之间交互的控制信息应保证其完整性、保密性和可用性，因此必须要确保通信信道是可信的，可以通过物理隔离或者是建立安全的逻辑隧道来实现。

#### 6.2.8 系统访问

宽带网络接入服务器在控制平面应对通告路由信息的对等体进行认证，如果认证不通过，则应丢弃该对等体通告的路由信息，并将相关信息记录到日志文件中。

对于MPLS VPN，VPN内部的控制信息在VPN之间和VPN与MPLS骨干之间应该相互隔离，互不干扰。

##### 6.2.8.1 路由策略和路由过滤

宽带网络接入服务器应支持路由控制策略和路由过滤，防止攻击者利用路由协议安全漏洞通告错误路由或者是倾泄大量路由信息导致内存溢出，设备瘫痪。

宽带网络接入服务器应支持如下的路由策略和过滤机制：

- 按照目的网段、自治系统路径、团体属性等特性进行过滤；
- 能够配置成 Passive（被动）模式，只接收处理路由信息，而不向邻居对等体通告路由信息；
- 在路由协议重分布过程中能够按照目的网段、自治系统号等信息过滤。

##### 6.2.8.2 MPLS VPN

宽带网络接入服务器实现L2 VPN和L3 VPN应满足如下的基本要求：

- 不同的 VPN 之间，地址空间应能够重用；
- 不同的 VPN 之间交互的控制信息应相互隔离；
- 可实现 VPN 所使用资源（如 CPU、内存）的相互隔离，防止因一个 VPN 独占资源而造成对其他 VPN 的 DoS 攻击；
- 应能够提供 VPN 路由过滤策略，防止 VPN 路由表、MAC 表的溢出。



## 7 管理平面安全

### 7.1 安全威胁

宽带接入服务器网络管理平面的主要功能是实现对设备系统参数配置以及设备状态信息的统计，其可能面临的主要安全威胁包括以下几个方面，但并不局限于这些方面：

- 对数据流进行流量分析，从而获得设备有关的系统配置信息；
- 未经授权地观察、修改、删除系统的配置信息；
- 未经授权地访问管理接口，控制整个设备；
- 利用管理信息流实施拒绝服务攻击。

### 7.2 安全功能

#### 7.2.1 标识和验证

管理接口应提供必要的用户身份标识和验证功能，只授权合法用户的访问。为了审计的需要，要确保用户标识的惟一性，不建议一个用户使用多个标识或者是多个用户使用同一个标识。

##### 7.2.1.1 串口访问

宽带网络接入服务器应当支持串口访问功能，管理员通过直接相连串口进行访问，应提供与7.2.1.2节相同的安全保护能力。

##### 7.2.1.2 Telnet 访问

宽带网络接入服务器应当提供远程登录 Telnet 访问模式，对登录用户的访问应符合下述要求：

- 提供对用户身份的验证，在日志文件中记录用户的访问活动；
- 提供对用户账号的分级管理，不同的用户分配不同的访问权限；
- 提供对 Telnet 用户密码试探攻击的保护，可对同一个 IP 地址使用延时响应机制，也可以限定 来自同一个 IP 地址的登录尝试次数；当用户连续登录系统失败次数超过系统设定值时，系统管理员可以考虑将该用户账号锁定；
- 能够限制同时登录的 Telnet 用户数量；
- 在设定的时间周期内不进行交互应注销该用户；
- 应支持必要时关闭 Telnet 远程服务。

#### 7.2.1.3 SSH 访问

SSH是在不安全的网络上为远程登录会话和其他网络服务提供安全性的一种协议，对SSH服务的要求如下：

- 应支持 SSHv1 和 SSHv2 两种版本；
- 用户应通过身份认证才能进行后续的操作，用户地址和操作记入日志，宽带接入服务器应支持口令认证，建议支持公钥认证，可实现基于主机认证；
- SSH 服务器宜采用认证超时机制，在超时范围内没有通过认证应切断连接，建议限制客户端在一个会话上认证尝试的次数；
- SSHv2 应支持用于会话的加密密钥和认证密钥的动态管理，支持 Diffie-Hellman 组 14 或组 1 的密钥交换，在密钥交换过程中协商密钥交换算法、对称加密算法和认证算法等，并对服务器端进行主机认证；
- 应支持 HMAC-SHA1 认证算法，建议支持 HMAC-SHA1-96 认证算法，可实现 HMAC-MD5、HMAC-MD5-96 等认证算法；
- 应支持 3DES-CBC 对称加密算法，可实现 Blowfish-CBC、IDEA-CBC、CAST128-CBC、AES256-CBC、AES128-CBC 等对称加密算法；
- 对于非对称加密算法，应支持 SSH-DSS，建议实现 SSH-RSA；
- 可限定用户通过哪些 IP 地址使用 SSH 服务对设备进行访问；
- 应支持必要时关闭 SSH 服务。

#### 7.2.1.4 Web 管理

宽带网络接入服务器可以提供基于Web的管理模式，系统管理员能够通过Web方式配置系统参数，查看统计信息等，建议满足下列要求：

- 用户应提供用户名/口令才能进行后续的操作，用户地址、用户标识和操作应记入日志文件；
- 可限定用户通过哪些 IP 地址使用 HTTP 对设备进行访问；
- 应能够支持 SSL/TLS 协议，确保数据的完整性和机密性；
- 应支持必要时可关闭 HTTP 服务，支持 HTTPS 服务。

#### 7.2.1.5 SNMP 安全

宽带网络接入服务器应支持通过实现安全协议来保护网络管理操作的功能，提供数据完整性、数据源认证和数据保密性服务。

SNMP是最常用的网络管理协议，它提供了网管工作站和位于被管设备上的代理之间的通信接口。通过该接口，网络管理员能够将配置参数下载到被管设备，查看被管设备的运行状况和运行参数，因此确保网络管理接口的安全是非常重要的。

SNMP协议应当支持摘要认证协议和对称私有协议，实现消息摘要算法和对称加密算法。通过摘要认证协议来保证网管消息发送者/接收者之间网管信息的完整性，同时可以验证消息源；对称私有协议来保护网管信息防止泄密。

SNMPv1本身只能提供非常弱的安全保护能力，在SNMPv1中代理和管理站之间的通信除依靠团体串验证外不作任何安全设置，一旦团体串被泄漏，则会给网络设备带来很大的安全风险。

SNMPv2提供了一定的安全机制，但是没有得到广泛的实施，不支持SNMPv2安全机制的实现称为SNMPv2c。

SNMPv3是一个安全的网络管理协议，能够提供支持基于视图的访问控制（VACM）和基于用户的安全模型（USM）等安全机制，能够提供完善的安全保护。

宽带网络接入服务器可支持SNMPv1和SNMPv2c，但应提供禁用功能，并且缺省应该是禁用的；应支持SNMPv3的网络管理接口。提供SNMPv1和SNMPv2c应可以和访问控制列表相结合，控制非法网管接入设备，同时不使用public/private作为缺省团体名，缺省只读团体名和读写团体名称不能够相同，并且在适当的时机提示管理员修改团体名。



#### 7.2.2 数据保护

管理平面的用户数据主要是一些用户配置数据，需要保证数据的完整性和可用性，以防止配置数据出错而导致整个设备工作不正常，同时也要防止敏感数据被窃取导致网络遭受攻击。管理平面的用户数据可以采用带内和带外两种传送模式，带外模式通过物理隔离实现数据保护，带内模式则可以通过采用SSHv2或者是SNMP协议的安全扩展来实现。

#### 7.2.3 系统功能保护

用于管理平面管理的相关安全数据（如配置信息）应得到妥善的保护。

#### 7.2.4 资源分配

管理信息的处理需要占用系统的CPU、内存等资源，对这部分信息的处理一定要确保不能影响控制平面对路由信息和数据平面对用户数据转发的影响。此外，通过管理平面提供的设备补丁下载功能应该得到严格的管理，不应该被用来对设备资源实施恶意占用。

#### 7.2.5 安全审计

宽带网络接入服务器应当提供基本的日志功能，记录用户访问活动，以便于网络安全管理员根据日志信息监控网络运行情况和诊断网络故障。

日志应记录过滤规则、拒绝访问、配置修改等安全相关事件，告警记录发生的安全违章事件，并可以一定的方式提示管理员，审计可对记录的安全事件进行回顾和检查，分析和报告安全信息。

宽带网络接入服务器对日志的要求：

- 安全日志条目应包含用户 IP 地址、用户名、操作类型、访问时间、操作结果等基本访问信息；
- 应可以保存在本地系统（如磁盘介质），也可以发送到专用的日志主机上做进一步的处理；
- 应可以实时打印在专用打印机或连接宽带网络接入服务器的显示终端上；
- 应定义日志的严重程度等级，并能够根据严重程度级别过滤输出；

- 应支持和日志主机之间的通信接口。
- 宽带网络接入服务器对告警的要求：
- 应定义告警的严重程度级别，并根据严重程度级别确定是否以一定的方式（如声光显示）提示管理员；
- 应支持告警输出到打印机或显示终端，可根据严重程度级别输出到不同的显示终端；
- 告警应保存在本地或通过网络存储到其他主机。

#### 7.2.6 安全管理

##### 7.2.6.1 口令管理

宽带网络接入服务器应能够支持一定长度的口令字（不短于8个），并且由数字、字符或特殊符号组成，支持对简单口令的检查功能；支持以密文的形式在系统配置文件中存储用户口令，此外，登录用户在查看系统配置时用户口令也应当以密文形式回显。

#### 7.2.7 可信信道/路径

宽带网络接入服务器应预留独立的以太网管理接口支持带外管理方式，在配置中要确保仅有内网管理用户可以访问，如果不使用该接口则应当关闭。此外，也可以通过专用的逻辑信道（MPLS VPN）或者是加密信道（IPSec隧道）来提供网管数据的传送安全。

#### 7.2.8 系统访问

##### 7.2.8.1 设备的访问控制

宽带网络接入服务器提供管理功能来配置设备，系统管理员能够远程登录到设备上进行维护和管理。宽带网络接入服务器能够对系统管理员用户的访问实现控制：

- 验证登录用户的身份，核实用户的操作权限；
- 不允许使用不安全的口令登录宽带网络接入服务器；
- 用户所有的写操作、执行操作都应记录到日志文件中。

##### 7.2.8.2 版本管理的控制

宽带网络接入服务器宜提供完善的补丁或版本权限的管理功能，实现设备的软件升级，包括软件版本和设备的配置，可以通过本地和远程两种方式。

# 附 录 A
## （资料性附录）
## 通用 TTL 安全机制（GTSM）

大多数路由控制协议（如BGP、LDP）的对等体通常要么是在直接相连的物理接口建立，要么是在设备的逻辑环回接口建立，因此传递过程中报文的TTL值应当是可以预知的，所以可以通过TTL来提供简单有效的保护。

通用TTL安全机制设计用于保护控制平面基于CPU消耗的攻击。其基本原理是：

假设前提：

1）攻击者能够接入到网络中并且发送有效的路由协议攻击报文；

2）在协议报文传送的路径上，路由设备都能够正确的处理TTL字段。

设置协议报文TTL字段的初始值为255（最大可能值，TTL字段8个比特）；对每一个配置协议的对等体，更新接收路径接入控制列表或防火墙的配置只允许具有正确的<source，detination，TTL>三元组的协议报文通过。对于物理直连对等体，TTL值应当是255；多跳环境，TTL值应当是255-（range-of-acceptable-hops），如果不符合上述条件，就放入低优先级队列，记录到日志文件，并且丢弃但不发送ICMP消息。

在多跳环境下，设置报文的TTL为255-（configured-range-of-acceptable-hops），这种方式提供了一种实现简单但安全级别较低的保护措施，在理论上，还是存在遭受DDoS攻击的危险。而且GTSM这种机制也很难适应网络拓扑的变化。此外，GTSM不支持自动协商机制，只能通过手工静态配置。

# 附 录 B
## （资料性附录）
## 基于 802.1x 用户接入认证

IEEE802.1x是一种基于端口的认证协议，是一种能够对用户进行认证的方法和策略。802.1x认证的最终目的就是确定一个端口是否可用。对于一个端口，如果认证成功那么就“打开”这个端口，允许所有的报文通过；如果认证不成功就使这个端口保持“关闭”，此时只允许802.1x的认证报文通过。

802.1x的系统结构如图B.1所示。

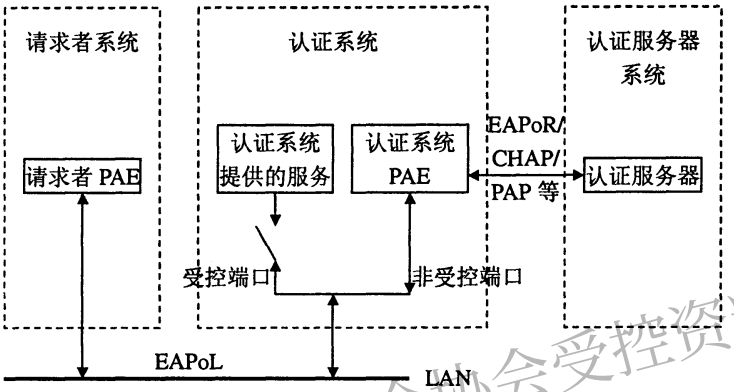


图 B.1 802.1x 的系统结构

IEEE 802.1x的体系结构中包括三个部分：请求者系统（Supplicant System）、认证点（Authenticator System）和认证服务器系统（Authentication Sever System）。

请求者和认证点之间运行802.1x定义的EAPoL协议。

当认证点工作于中继方式时，认证点与认证服务器之间同样运行EAP协议，EAP帧中封装了认证数据，将该协议承载在其他高层次协议中（如RADIUS），以便穿越复杂的网络到达认证服务器；当认证点工作于终结方式时，认证点终结EAPoL消息，并转换为其他认证协议（如RADIUS PAP/CHAP消息机制）传递用户认证信息给认证服务器系统。

认证点每个物理端口内部有受控端口和非受控端口。非受控端口始终处于双向连通状态，主要用来传递EAPoL协议帧，可保证随时接收认证请求者发出的认证EAPoL报文；受控端口只有在认证通过的状态下才打开，用于传递用户数据流。受控端口可配置为双向受控、仅输入受控两种方式，以适应不同的应用环境，输入受控方式应用在需要桌面管理的场合，如管理员远程唤醒一台终端。

中 华 人 民 共 和 国
通 信 行 业 标 准
宽带网络接入服务器安全技术要求
YD/T 1658-2007
*
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
北京新瑞铭印刷有限公司印刷

*
开本：880×1230　1/16　　2007 年 12 月第 1 版
印张：1.75　　2007 年 12 月北京第 1 次印刷
字数：42 千字
ISBN 978 - 7 - 115 - 1533/07 - 196
定价：15 元
本书如有印装质量问题，请与本社联系　电话：(010)67114922