ICS 33.040.40
M 32

YD

中华人民共和国通信行业标准

YD/T 1905-2009

IPv6网络设备安全技术要求
——宽带网络接入服务器

Security Technical Requirements for
——Broadband Network Access Server IPv6 Network Equipment

2009-06-15 发布　　2009-09-01 实施

中华人民共和国工业和信息化部　发布

目　次

前　言

本标准是IPv6网络设备——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和名称如下：

1. 《IPv6网络设备安全技术要求——宽带网络接入服务器》
2. 《IPv6网络设备安全测试方法——宽带网络接入服务器》

本标准与《IPv6网络设备安全测试方法——宽带网络接入服务器》配套使用。

本标准附录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：工业和信息化部电信研究院

本标准主要起草人：杨剑锋

IPv6网络设备安全技术要求
——宽带网络接入服务器

1 范围

本标准规定了支持IPv6的宽带网络接入服务器安全技术的基本要求，包括数据平面、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/路径和系统访问等八个安全功能需求。本标准中出现的所有未指明的宽带网络接入服务器、接入服务器等均特指IPv6宽带网络接入服务器。

本标准适用于支持IPv6的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 1162.1-2005	多协议标记交换（MPLS）技术要求
YD/T 1466-2006	IP安全协议（IPSec）技术要求
YD/T 1897-2009	互联网密钥交换协议（IKEv2）技术要求
IETF RFC 1352（1992）	SNMP安全协议
IETF RFC 2385（1998）	通过TCP MD5选项保护BGP会话
IETF RFC 2472（1998）	PPP上的IPv6

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本标准。

3.1.1

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、实现虚拟专用拨号网（VPDN）构建企业内部Intranet等网络应用。

3.1.2

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，可以完成用户宽带的（或高速的）IP/ATM网的数据接入、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。

3.1.3

IPv6宽带网络接入服务器　IPv6 Broadband Network Access Server（IPv6 BNAS）

是基于IPv6协议簇工作在IPv6骨干网的边缘，具有IPv6用户接入管理和路由功能，面向IPv6网络应用的宽带网络接入服务器。

3.1.4

访问控制　Access Control（AC）

防止未经授权使用资源。

3.1.5

可确认性　Accountability

确保一个实体的行为能够被独一无二地跟踪。

3.1.6

授权　Authorization

授予权限，包括根据访问权进行访问的权限。

3.1.7

可用性　Availability

根据需要，信息允许授权实体访问和使用的特性。

3.1.8

信道　Channel

系统内的信息传输通道。

3.1.9

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。

3.1.10

数据完整性　Data Integrity

数据免遭非法更改或破坏的特性。

3.1.11

拒绝服务　Denial of Service

阻止授权访问资源或延迟时间敏感操作。

3.1.12

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。

3.1.13

加密　Encryption

对数据进行密码变换以产生密文。加密可以是不可逆的，在进行不可逆加密的情况下，相应的解密过程是不能实际实现的。

3.1.14

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。

3.1.15

完整性破坏I　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。

3.1.16

密钥　Key

控制加密与解密操作的一序列符号。

3.1.17

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。

3.1.18

冒充　Masquerade

一个实体伪装为另一个不同的实体。

3.1.19

路径　Path

数据信息按特定次序经由的通路或路线。

3.1.20

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。

3.1.21

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。

3.1.22

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。

3.1.23

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”等。

3.1.24

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

下列缩略语适用于本标准。

3DES　　Triple DES　　三重数据加密标准

AAA	Authentication Authorization Accounting	鉴别、授权、计费
ABK	Address Based Keys	基于密钥的地址
ACL	Access Control List	访问控制列表
AES	Advanced Encryption Standard	高级加密标准
AH	Authentication Header	认证头
ATM	Asynchronous Transfer Mode	异步转移模式
BGP	Border Gateway Protocol	边界网关协议
BGP4+	BGP version 4 Plus	支持 IPv6 的 BGP 协议版本 4
BNAS	Broadband Network Access Server	宽带网络接入服务器
CAR	Committed Access Rate	承诺接入速率
CAST	Carlisle Adams-Stafford Tavares encryption	CAST 加密算法
CBC	Cipher Block Chaining	密码块链
CGA	Cryptographically Generated Addresses	加密产生地址
CHAP	Challenge Handshake Authentication Protocol	质询握手认证协议
CPU	Central Processing Unit	中央处理单元
CR-LDP	Constraint Route-LDP	约束路由的 LDP 协议
DDoS	Distributed DoS	分布式 DoS 攻击
DES	Data Encryption Standard	数字加密标准
DH	Diffie-Hellman key	DH 密钥
DoS	Denial Of Service	拒绝服务攻击
DSS	Digital Signature Standard	数字签名标准
EAP	Extensible Authentication Protocol	扩展认证协议
EAPoL	Extensible Authentication Protocol over LAN	局域网扩展认证协议
ESP	Encapsulation Secure Payload	封装安全净荷
FCAPS	Fault，Configuration,Accounting,Performance and Security	故障，配置，账务，性能，安全
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
ICMPv6	ICMP version 6	ICMP 协议版本 6
ID	Identification	身份
IDEA	International Data Encryption Algorithm	国际数据加密算法
IKE	Internet Key Exchange	互联网密钥交换
IKEv1	IKE version 1	IKE 协议版本 1
IP	Internet Protocol	互联网协议
IPv6	Internet Protocol version 6	互联网协议版本 6
IPSec	IP Security	IP 安全机制

IPv6CP	IPv6 Control Protocol	IPv6 控制协议
ISDN	Integrated Serviced Digital Network	综合业务数字网
ISP	Internet Service Provider	互联网业务提供商
IS-IS	Intermediate System to Intermediate System	中间系统－中间系统
IS-ISv6	IS-IS version 6	IS-IS 协议版本 6
L2TP	Layer 2 Tunneling Protocol	二层隧道协议
L2VPN	Layer 2 VPN	二层 VPN
L3VPN	Layer 3 VPN	三层 VPN
LAC	L2TP Access Concentrator	L2TP 接入集中器
LAN	Local Area Networ	局域网
LDP	Label Distribution Protocol	标记分发协议
LNS	L2TP Network Server	L2TP 隧道网络服务器
LSP	Label Switch Path	标记交换路径
LSR	Label Switching Router	标记交换路由器
MAC	Media Access Control	媒质访问控制
MD5	Message Digest version 5	报文摘要版本 5
MODP	Modular Exponentiation Group	模求幂组
MPLS	Multi Protocol Label Switching	多协议标记交换
NAS	Network Access Server	网络接入服务器
ND	Neighbor Discovery	邻居发现
NTP	Network Time Protocol	网络时间协议
OAM&P	Operation Administration，Maintenance and Provisioning	运行、管理、维护和预置
OSPF	Open Shortest Path First	最短路径优先
OSPFv3	OSPF version 3	OSPF 协议版本 3
PAE	Physical Address Extentions	物理地址扩展
PAP	Password Authentication Protocol	密码认证协议
PPP	Point-to-Point Protocol	点到点协议
PSTN	Public Switched Telephone Network	公众电话交换网
RADIUS	Remote Authentication Dial In User Service	远程身份验证拨入用户服务
RIP	Route Information Protocol	路由信息协议
RIPng	Routing Information Protocol，next generation	下一代路由信息协议
RSA	Rivest-Shamir-Adleman encryption	RSA 加密算法
RSVP	Resource Reservation Protocol	资源预留协议
RSVP-TE	RSVP-Traffic Engineering	基于流量工程扩展的 RSVP
SA	Security Association	安全联盟
SHA	Secure Hash Algorithm	安全散列算法
SHA1	SHA version 1	SHA 版本 1

SLA	Service Level Agreement	服务水平协议
SNMP	Simple Network Management Protocol	简单网管协议
SNMPv1	SNMP version 1	SNMP 协议版本 1
SNMPv2c	SNMP version 2c	SNMP 协议版本 2c
SNMPv3	SNMP version 3	SNMP 协议版本 3
SSH	Secure Shell	安全外壳程序
SSHv1	SSH version 1	SSH 版本 1
SSHv2	SSH version 2	SSH 版本 2
SSL	Secure Socket Layer	安全套接层
TCP	Transmission Control Protocol	传输控制协议
TFTP	Trivial File Transfer Protocol	简单文件传输协议
TLS	Transport Layer Security	传输层安全
TTL	Time to Live	生命周期
UDP	User Datagram Protocol	用户数据报协议
URPF	Unicast Reverse Path Forwarding	单播反向路径转发
USM	User-based Security Model	基于用户的安全模型
VACM	View-based Access Control Model	基于视图的访问控制模型
VLAN	Virtual Local Area Networks	虚拟局域网
VPDN	Virtual Private Dial Network	虚拟专用拨号网
VPN	Virtual Private Network	虚拟专用网
VRF	VPN Routing and forwarding	VPN 路由和转发

4 安全框架模型

IPv6宽带网络接入服务器是一种能提供端到端宽带连接的IPv6网络设备，通常位于IPv6骨干网的边缘层，作为用户接入网和骨干网之间的网关，终结或中继来自用户接入网的连接，提供接入到IPv6宽带核心业务网的服务。

IPv6宽带网络接入服务器在网络中处于汇接层面，通常面向多种类型的用户接入设备，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。

如图1所示，本标准将IPv6宽带网络接入服务器的功能划分为3个平面：

a）数据平面：主要是指为用户访问和利用网络而提供的功能，如提供用户数据的转发。

b）控制平面：也可称为信令平面，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。

c）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，IPv6宽带网络接入服务器必须提供一定的安全功能。本标准将GB/T 18336.2中定义的安全功能应用到IPv6宽带网络接入服务器中，这些安全功能包括：

a）标识和认证：识别以及确认用户的身份，并确保用户与正确的安全属性相关联。

b）用户数据保护：保护用户数据的完整性、可用性和保密性。

c）系统功能保护：对系统实现的关键功能（如用户接入功能等），以及相关功能所涉及数据（如安全功能所需的用户身份、口令等数据）完整性、可用性和保密性的保护。

d）资源分配：系统容错、资源调度和控制的能力，对系统资源进行有效的控制，限制用户对资源的访问和过度占用，避免造成系统对合法业务拒绝服务。

e）安全审计：识别、记录、存储和分析那些与安全相关活动有关的信息，提供日志等审计记录，以用来分析安全威胁活动和对策。

f）安全管理：系统对安全属性、数据和功能的管理能力。

g）可信信道/路径：通信所使用的通道要求可信，即符合系统安全策略，对于通道两端的身份具有鉴别和抗抵赖的特性。

h）系统访问：管理和控制用户会话的能力。

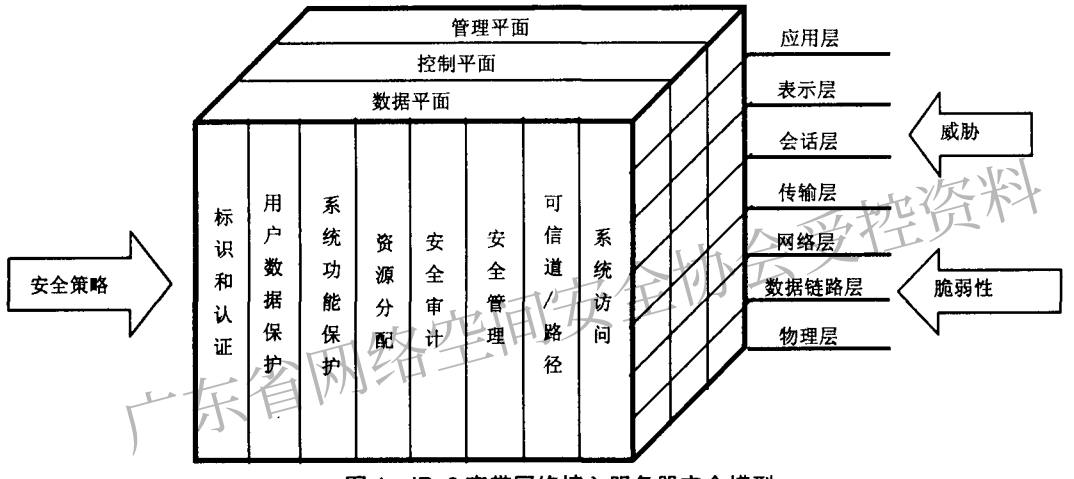

图 1　IPv6 宽带网络接入服务器安全模型

为了确保IPv6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

IPv6宽带网络接入服务器数据平面功能主要是终结或中继来自用户的各种连接，设备面临的安全威胁主要有以下方面，但不局限在这些方面：

a）对数据流进行流量分析，从而获得用户数据的敏感信息；

b）未经授权的观察、修改、插入和删除用户数据；

c）利用用户数据流的拒绝服务攻击。

5.2　安全功能

5.2.1　标识和认证

IPv6宽带网络接入服务器可支持多种不同类型的用户接入方式，设备应能以特定的形式对用户进行标识，并设置访问控制策略来控制用户的接入，同时应可选择有效的认证协议对用户进行身份验证。

设备应支持PPP用户和以太网用户接入的标识和认证功能，相关要求见6.2.1节。

5.2.2 数据保护

5.2.2.1 IPSec 隧道

IPv6宽带网络接入服务器应能够通过建立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。

设备应支持AH和ESP协议，IPSec的相关协议要求见YD/T1466-2006。设备应支持传输模式和隧道模式，应支持SA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验证算法和HMAC-MD5-96验证算法。

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

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

设备宜支持动态密钥管理IKE协议，IKE相关要求参见YD/T1466-2006及YD/T 1897-2009《互联网密钥交换协议（IKEv2）技术要求》。

5.2.2.2 L2TP 隧道

IPv6宽带网络接入服务器可选支持L2TP。

当设备支持L2TP时，应能通过建立L2TP隧道为用户数据提供保护，应实现LAC和LNS功能特性，应支持CHAP鉴别协议。

5.2.3 系统功能保护

IPv6宽带网络接入服务器对数据平面的相关功能（如数据转发功能），及相应功能的安全数据应提供妥善的手段（如通过基于用户的安全策略来实现相关数据的分级访问控制机制）以进行保护，相关功能要求见5.2.1节、5.2.4节、5.2.8节。

5.2.4 资源分配

5.2.4.1 攻击防护

IPv6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、接入带宽控制等）保障设备资源和网络带宽的合理利用，特别是要能够限制和抵御来自网络的各种侵占资源类的攻击，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服务。

IPv6宽带网络接入服务器应能够抵御以下的常见攻击类型，但并不局限于这些方面：

a）大流量攻击：大流量可以分成两种类型，一种是流经流量，即需要设备转发的流量，对于这类攻击，IPv6宽带网络接入服务器数据端口宜具有线速转发的能力，对于超过端口处理能力的流量可以采用按策略对数据包进行丢弃；另一种流量的目的地就是设备本身（如DoS/DDoS），这类攻击可能会占用大量CPU处理时间和内存，严重的甚至会造成设备崩溃，导致服务中断从而无法为用户提供正常服务，对这类攻击流量，IPv6宽带网络接入服务器应采取过滤和丢弃等保护策略拒绝数据接口接收的目的地为设备本身的数据包，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。

b）畸形包处理：IPv6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，设备的正常功能不应受到影响。此外，也应保证IPv6宽带网络接入服务器自身不会产生上述类型的畸形包。

c）IP地址哄骗：设备应能对网络中源地址哄骗报文进行过滤，设备应支持URPF功能（见6.2.4.2节）。

IPv6 宽带网络接入服务器应能够提供相应机制，以便于在必要时对同一用户允许建立 TCP 会话的数量进行控制，来防止用户过渡消耗网络资源。设备应能够根据用户属性（如，接入类型）对允许其建立

的TCP会话数量进行限制和管理。

5.2.4.2 数据包过滤

IPv6宽带网络接入服务器应能够提供控制用户接入和过滤用户数据的能力。通常有两种方式可以采用，一种是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。另一种是指根据不同用户的授权提供特定的前缀信息，以作为用户的IP地址，通过网络的IP包过滤策略，实现不同的用户有不同的接入能力。

IPv6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，依据SLA为用户分配带宽资源。SLA包含承诺速率、峰值速率，承诺突发流量、峰值突发流量等，对于超出协定的流量设备可以采取降级、丢弃等操作。

5.2.5 安全审计

IPv6宽带网络接入服务器应提供对数据平面的相关信息进行日志记录的功能，安全日志至少应包含数据接口状态、出向/入向用户数据流量等。IPv6宽带网络接入服务器应实现对用户数据流量的安全审计的功能。相关要求见7.2.5节。

5.2.6 安全管理

IPv6宽带网络接入服务应能够提供本标准数据平面安全部分要求的安全功能和数据管理能力，要求见7.2.6节。

5.2.7 可信信道/路径

IPv6宽带网络接入服务器与其他设备通信的信道/路径要求可信，设备应能使用专用的通道以保证对数据进行安全鉴别和防抵赖的需求（如对于传送敏感数据、专线用户数据的通信应能同传送其他数据的通信隔离开来）。设备应能够采取物理隔离或逻辑隔离的方式进行通道隔离。IPv6宽带网络接入服务器逻辑通道隔离的方式包括VPN（见5.2.8.2节）、隧道（见5.2.2节）等。

5.2.8 系统访问

5.2.8.1 ACL 功能

IPv6宽带网络接入服务器应实现访问控制列表功能，以此作为一种安全手段，按照相应的安全规则来对进出的数据报文进行匹配，保护系统和资源免受未经授权的访问。

IPv6宽带网络接入服务器应能够提供基于源IP地址、目的IP地址、源端口、目的端口和协议类型等元素的ACL功能。设备应支持对报文匹配情况进行统计计数和记入日志等。IPv6宽带网络接入服务器可选支持基于IPv6包头流量类别和流标签的访问控制列表，可选支持指定有效时间的访问控制列表的功能。

5.2.8.2 VPN 功能

IPv6 宽带网络接入服务器应实现 VPN 功能，通过 VPN 来实现不同用户数据的隔离，避免 VPN 外部数据对 VPN 内部的数据造成影响。设备在功能实现上应确保不同 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 表的容量空间不会溢出。

设备应支持通过 IPSec 隧道或通过 L2TP 隧道实现 VPN，相应隧道的要求参见 5.2.2.2 节。

设备应支持通过 MPLS LSP 实现 VPN。对于数据平面，IPv6 宽带网络接入服务器实现的 MPLS VPN 应满足如下要求：

a）不管是L2VPN还是L3VPN，数据应严格基于标签沿着LSP转发，除非需要，一个VPN的数据不应被发送到该VPN之外；

b）当同时支持VPN服务和其他服务时，特别是在一个物理接口上通过不同的逻辑接口支持多个服务时，应能基于逻辑接口对包括VPN服务在内的不同服务的接入速率进行限制。

相关 MPLS VPN 功能要求见 6.2.8.2 节，MPLS 协议要求见 YD/T 1162.1-2005。

5.2.8.3 防火墙功能

IPv6 宽带网络接入服务器可选支持防火墙功能。设备支持防火墙功能时，除提供基本数据包过滤、ACL 功能外，宜支持和提供应用代理的功能，只允许被保护的用户访问允许的网络应用，对应用层协议信息进行检查，并实时维护相应的 TCP 和 UDP 状态信息，实现基于状态的访问控制。

6 控制平面安全

6.1 安全威胁

IPv6宽带网络接入服务器的控制平面主要负责路由信息的学习和与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，但不局限在这些方面：

a）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；

b）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；

c）利用协议的拒绝服务攻击，如利用路由协议、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；

d）非法设备进行身份哄骗，如建立路由协议、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等；

e）针对路由协议、MPLS标签分配协议等的转发路径信息的欺骗。

6.2 安全功能

6.2.1 标识和认证

6.2.1.1 PPP 用户接入

对于PPP接入方式，IPv6宽带网络接入服务器应可以工作在PPP终结和PPP中继两种模式下。

设备应可以通过对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PPP_Session_Id来标识用户会话。

PPP连接建立和配置应基于IPv6CP，协议封装和网络控制应符合IETF RFC 2472的要求。

同时，IPv6CP应当与其他PPP认证和加密机制共同使用，根据不同的安全性要求对接入的连接进行验证。对于PPP用户的接入，设备应采用CHAP协议，或者是EAP协议进行认证。对于PPP中继模式，设备应按照上行链路的封装格式封装后交由后继设备进行认证。为保证认证信息在传输过程中的安全，可以通过建立L2TP隧道或IPSec隧道提供保护。

6.2.1.2 以太网用户接入

对于以太网用户接入方式，IPv6宽带网络接入服务器应可通过使用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。

IPv6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，同时应可以选择有效的认证协议对用户进行身份验证。设备应支持802.1x认证协议，具体内容参见附录B。为增强安全性，设备

应支持EAP协议和RADIUS扩展协议，从而实现通过不同安全等级的认证协议来对不同用户的连接进行接入安全验证。

当用户通过ND协议自动配置地址时，IPv6宽带网络接入服务器应能对该类用户进行有效标识和认证，认证方式可包括本地认证、RADIUS服务器认证等。

IPv6宽带网络接入服务器可选实现Web Portal认证方式。

6.2.1.3 路由协议

IPv6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，以免造成由于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。

IPv6宽带网络接入服务器应实现基于以下算法的路由协议认证，具体要求如下：

a）RIPng协议应支持HMAC-MD5和HMAC-SHA-1算法；

b）OSPFv3协议应支持HMAC-MD5和HMAC-SHA-1算法；

c）IS-ISv6协议应支持接口Level 1/Level 2、区域内、区域间HMAC-MD5和HMAC-SHA-1算法；

d）BGP4+协议应支持TCP-HMAC-MD5算法（见IETF RFC2385）。

IPv6宽带网络接入服务器对于MPLS中两种用于建立LSP的标签分配协议主要要求如下：

a）LDP/CR-LDP协议：发现交换过程使用的消息由UDP协议承载，对于基本Hello消息，设备应只接收与可信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。

b）RSVP-TE协议：设备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算法和HMAC-SHA1算法。

此外，IPv6宽带网络接入服务器可选实现GTSM安全机制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

IPv6宽带网络接入服务器控制平面的信息主要包括用户认证信息、路由信息、邻居及链路地址前缀信息等，对于这些信息应提供完整性、保密性和可用性保护。在实现上设备可通过建立L2TP、IPSec逻辑安全隧道（见5.2.2节）、以及加密验证算法等方式对数据进行保护。

6.2.3 系统功能保护

IPv6宽带网络接入服务器对控制平面的相关功能（如路由功能）、以及用于相应功能的安全数据（如路由协议的认证密钥）应提供妥善的方式（如，启用路由控制策略和路由过滤功能）实现保护，相关功能要求见6.2.1节、6.2.4节、6.2.8节。

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，IPv6宽带网络接入服务器在控制平面应支持路由控制策略和路由过滤功能，抑制可能的利用路由协议安全缺陷进行的资源耗尽型攻击。

IPv6宽带网络接入服务器可选实现基于VPN使用的CPU、内存等资源的隔离，以防止因独占资源对其他VPN造成的拒绝服务型攻击。

6.2.4.2 URPF

IPv6宽带网络接入服务器应支持URPF功能，只转发IP地址和接口在转发表中存在的分组，以缓解IP地址哄骗等类型的攻击造成的影响。

6.2.4.3 IP 扩展头和选项

IPv6扩展头和选项（如逐跳头、路由头、目的地选项等）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。IPv6宽带网络接入服务器应提供IPv6扩展头和选项安全处理的保护功能，并提供必要时限制或关闭处理特定扩展头和选项的能力。

6.2.4.4 ICMPv6 协议

ICMPv6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，IPv6宽带网络接入服务器应实现ICMPv6协议的功能，并提供必要时限制或关闭ICMPv6相关功能的能力。上述ICMPv6消息类型包括但不限于：

a）Type=1：目的地不可达；

b）Type=3：超时；

c）Type=128：回显请求；

d）Type=129：回显应答。

6.2.4.5 ND 协议

ND被用来解决相同物理链路上的节点之间的交互操作，包括路由器发现、前缀发现、地址自动配置、重复地址检测、邻居不可达检测、链路层地址解析、下一跳确定和重定向。对于开放式网络环境，网络节点可不经链路层验证即加入到设备所处的本地链路上，因此IPv6宽带网络接入服务器在本地链路存在DoS、重定向等类型攻击的威胁。

IPv6宽带网络接入服务器宜提供相关地址宿主验证的措施，对本地链路节点安全性进行验证，可选支持采用CGA、ABK等协议提高ND协议消息交互的安全性。

6.2.4.6 服务

IPv6宽带网络接入服务器应缺省关闭TCP和UDP特定端口的服务，或者不提供相应的服务模型。

设备应缺省关闭或不提供的服务应包括但不限于Echo、Chargen、Finger、NTP等。

6.2.5 安全审计

IPv6宽带网络接入服务器应提供对控制平面的控制数据和信息进行安全日志记录的功能，并应实现对设备相关数据信息进行安全审计的功能，特别是对设备的路由表、邻居缓存、目的地缓存、前缀列表等重要数据有影响的控制数据。相关要求见7.2.5节。

6.2.6 安全管理

IPv6宽带网络接入服务应能够提供本标准控制平面安全部分要求的安全功能和数据管理能力，要求参见7.2.6节。

6.2.7 可信信道/路径

IPv6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/路径要求可信。IPv6宽带网络接入服务器应可以通过物理隔离或是建立安全的逻辑隧道来实现，如建立IPSec安全隧道（见5.2.2节）等。

6.2.8 系统访问

6.2.8.1 路由策略和路由过滤

IPv6宽带网络接入服务器应支持路由控制策略和路由过滤，能够只发布特定条件的路由，也能够只接受特定条件的路由，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设备内存溢出，或设备瘫痪。

IPv6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。

IPv6宽带网络接入服务器应支持如下的路由策略和过滤机制：

a）设备应能按照 IP 网段、自治系统路径、团体属性等特性进行过滤；

b）设备应能够配置成 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；

c）设备在路由协议重发布过程中应能够按照 IP 网段、自治系统号等信息过滤。

6.2.8.2 MPLS VPN

IPv6宽带网络接入服务器应实现MPLS VPN功能。设备应能保证VPN内部的控制信息在VPN之间和VPN与MPLS骨干之间实现相互隔离，互不干扰。

IPv6宽带网络接入服务器实现的L2VPN或L3VPN均应满足如下的基本要求：

a）设备在不同的 VPN 之间，应能够重用地址空间；

b）设备对不同的 VPN 之间交互的控制信息应相互隔离；

c）设备应可实现 VPN 下所使用资源（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；

d）设备应能够提供 VPN 下相关表项的保护和过滤策略，防止 VPN 路由表、MAC 表的溢出。

IPv6宽带网络接入服务器实现L3VPN还应满足如下的要求：

a）设备应支持静态路由算法和动态路由算法。对于动态路由算法，建议具有在接口上过滤路由更新的能力，应支持路由协议 MD5 加密认证；

b）设备应能基于 VRF 实例限制路由更新的速度。

7 管理平面安全

7.1 安全威胁

IPv6宽带网络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：

a）对信息流进行探测、分析，从而获得有关的系统管理、配置信息；

b）未经授权地观察、修改、删除系统的配置信息；

c）未经授权地访问管理接口，控制整个设备；

d）利用管理信息流实施拒绝服务攻击。

7.2 安全功能

7.2.1 标识和认证

IPv6宽带网络接入服务器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，要确保用户标识的唯一性，不应允许多个用户使用同一个标识，不建议一个用户使用多个标识。

7.2.1.1 串口访问

IPv6宽带网络接入服务器应支持串口访问功能，管理员可直接通过相连串口进行访问。设备串口访问应提供如下安全保护能力：

a）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；

b）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；

c）提供对用户密码试探攻击的保护，可对同一个连接使用延时响应机制，也可以限定同一个连接的登录尝试次数；当用户连续登录系统失败次数超过系统设定值时，系统可以将该用户账号锁定；

d）在设定的时间周期内不进行交互应注销该用户。

7.2.1.2 Telnet 访问

IPv6宽带网络接入服务器应提供远程登录Telnet访问模式。对用户的登录和访问，设备应提供下述安全保护能力：

a）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；

b）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；

c）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，系统可以将该用户账号锁定；

d）应能够限制同时登录的 Telnet 用户数量；

e）在设定的时间周期内不进行交互应注销该用户；

f）应可设定允许进行 Telnet 访问和管理的用户 IP 地址范围；

g）应支持必要时可关闭 Telnet 服务的功能。

7.2.1.3 SSH 访问

IPv6宽带网络接入服务器应支持SSH，以便于在不安全的网络上为远程登录会话和其他网络服务提供一定的保护。对SSH服务，设备应提供下述安全保护能力：

a）应支持 SSHv1 和 SSHv2 两种版本；

b）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，设备应支持口令认证，建议支持公钥认证，可实现基于主机认证；

c）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，

d）应限制客户端在一个会话上认证尝试的次数；

e）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；

f）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；

g）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；

h）对于非对称加密算法，应支持 SSH-DSS，建议实现 SSH-RSA；

i）应可设定允许进行 SSH 访问和管理的用户 IP 地址范围；

j）在设定的时间周期内不进行交互应注销该用户；

k）应支持必要时可关闭 SSH 服务。

7.2.1.4 Web 管理

IPv6宽带网络接入服务器可选提供基于Web的管理功能。当IPv6宽带网络接入服务器提供该管理模式时，系统管理员应可通过Web方式实现系统参数配置、统计信息查询等操作，设备应提供下列安全保护能力：

a）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；

b）应可设定允许进行 Web 访问和管理的用户 IP 地址范围；

c）应能够支持 SSL/TLS 协议，确保数据的完整性和机密性；

d）在设定的时间周期内不进行交互应注销该用户；

e）应支持必要时可关闭 Web 服务。

7.2.1.5 SNMP 安全

IPv6宽带网络接入服务器应支持通过安全协议来保护SNMP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，管理员能够将配置参数装载到被管设备，查看被管设备的运行状况和运行参数。

IPv6宽带网络接入服务器的SNMP协议应当支持摘要认证协议和对称私有协议（见IETF RFC1352），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，同时验证消息源；对称私有协议用来保护网管信息，防止泄密。

对于SNMP，设备应提供下列安全保护能力：

a）应支持 SNMPv3 的网络管理接口；

b）可选支持 SNMPv1 和 SNMPv2c 网络管理接口；

c）设备应提供必要时禁用 SNMP 的功能；

d）设备 SNMP 缺省设置应为禁用；

e）应可设定允许进行 SNMP 访问和管理的用户 IP 地址范围。

对于SNMPv3，设备应能够提供支持基于视图的VACM模型和基于用户的USM模型等安全机制，能够提供完善的安全保护。

对于SNMPv1和SNMPv2c，当设备支持时，应提供可以和访问控制列表相结合的方式，限制网管接入设备，同时不应使用public/private作为缺省团体名，缺省只读团体名和读写团体名称应不相同。

7.2.2 数据保护

IPv6宽带网络接入服务器管理平面的数据主要是一些用户和设备的配置及管理信息，对于这些数据应保证其相应的完整性、保密性和可用性，以防止数据出现错误或遭到破坏，同时也要防止敏感数据被窃取或非法使用。

设备管理平面的数据可采用带内和带外两种传送模式，带外模式应通过物理隔离实现数据保护，带内模式则可以通过采用SSHv2（见7.2.1.3节）或者是SNMPv3（见7.2.1.5节）的安全扩展来实现。

7.2.3 系统功能保护

IPv6宽带网络接入服务器管理平面相关功能、以及管理平面相应功能的相关数据（如配置信息）应得到妥善的保护。相关功能要求见7.2.1节、7.2.4节、7.2.8节。

7.2.4 资源分配

IPv6宽带网络接入服务器应提供一种保障机制，以实现对系统资源分配进行安全管理。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应确保不影响控制平面对路由信息的处理和数据平面对用户数据的转发。此外，设备通过管理平面提供的设备补丁下载功能应该得到严格的控制和管理，防止被用来对设备资源的恶意占用。

7.2.5 安全审计

7.2.5.1 端口镜像

IPv6宽带网络接入服务器应支持端口镜像功能。

设备应能通过必要的配置，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。

IPv6宽带网络接入服务器可选支持向远端安全中心进行数据镜像的功能。

IPv6宽带网络接入服务器实现端口镜像时，不应对帧进行修改，采用的镜像方式包括：一对一端口镜像和多对一端口镜像。

7.2.5.2 日志和告警

IPv6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。

设备的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。

IPv6宽带网络接入服务器对日志的要求：

a）安全日志条目应包含事件主体、发生事件、事件描述等，对于基本访问信息应包含用户地址、用户名、操作类型、访问时间、操作结果等信息；

b）设备应支持 NTP，以保证对安全日志记录时间的审计；

c）安全日志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；

d）安全日志应可以实时打印在专用打印机或显示在连接 IPv6 宽带网络接入服务器的显示终端上；

e）安全日志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；

f）设备应支持和专用日志主机之间的通信接口。

IPv6 宽带网络接入服务器对告警的要求：

a）设备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；

b）设备应支持将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；

c）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

IPv6宽带网络接入服务器应能够提供本标准管理平面安全部分要求的安全功能和数据管理能力。设备提供的管理方式应包括但不限于控制台、远程登录或网络管理接口/系统等方式，相关管理方式的安全要求见7.2.1节、7.2.8节。

7.2.6.1 口令管理

IPv6宽带网络接入服务器应提供对口令进行安全管理的功能，设备至少应实现下列安全保护功能：

a）支持长度不短于 8 个字节的口令；

b）支持由数字、字母和符号组成的口令；

c）支持对简单口令、弱口令的检查功能；

d）在系统配置文件中以密文的形式存储口令；

e）登录用户在查看系统配置时，口令以密文形式回显。

7.2.7 可信信道/路径

IPv6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。

IPv6宽带网络接入服务器应能通过专用的逻辑信道（如MPLS VPN，见6.2.8.2节）或者是加密信道（如：IPsec隧道，见5.2.2节），来支持对设备的管理，将管理通信数据和其他通信数据隔离，保证网管数据的传送安全。

设备应支持在必要时关闭或禁用带内接口的功能。

7.2.8 系统访问

7.2.8.1 安全访问控制

IPv6宽带网络接入服务器的配置应通过设备提供的管理功能来实现。设备应能够对登录到设备上进行维护和管理的管理员和用户的访问实现控制，ACL功能要求见5.2.8.1节。

设备至少应实现下列安全保护功能：

a）设备应能验证登录用户的身份，核实用户的操作权限；

b）设备不应允许使用不安全的口令登录设备；

c）用户所有的写操作、执行操作都应记录到安全日志文件中。

7.2.8.2 版本管理

IPv6宽带网络接入服务器应提供完善的补丁和软件版本的管理功能。具有权限的用户可以对设备的软件进行升级，包括软件版本和设备配置等，版本管理可通过本地和远程两种方式。

软件升级可通过FTP/TFTP来实现。对于通过FTP/TFTP的软件升级，设备应支持FTP/TFTP协议的口令认证功能。远程软件升级宜通过SSHv2来实现文件数据的安全传送。

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，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 IEEE 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。

IEEE 802.1x的系统结构如图B.1所示。

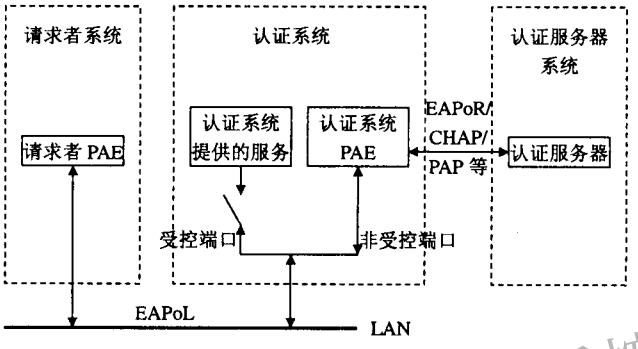

图 B.1 IEEE 802.1x 的系统结构

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IEEE 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。

参 考 文 献

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 1190-2002	基于网络的虚拟IP专用网(IP-VPN)框架
YD/T 1295-2003	支持IPv6的路由协议技术要求——开放最短路径优先协议（OSPF）
YD/T 1341-2005	IPv6基本协议——IPv6协议（IETF RFC2460，MOD）
YD/T 1342-2005	IPv6路由协议——支持IPv6的边界网关协议（BGP4+）
YD/T 1343-2005	IPv6邻居发现协议——基于IPv6的邻居发现协议（IETF RFC2461，MOD）
YD/T 1344-2005	IPv6地址结构协议——IPv6无状态地址自动配置（neq IETF RFC2462）
YD/T 1452-2006	支持IPv6的路由器设备技术要求——低端路由器
YD/T 1466-2006	IP安全协议（IPSec）技术要求
YD/T 1658-2007	宽带网络接入服务器安全技术要求

中华人民共和国

通信行业标准

IPv6网络设备安全技术要求

——宽带网络接入服务器

YD/T 1905-2009

*

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　　2009年8月第1版

印张：1.75　　2009年8月北京第1次印刷

字数：43千字

ISBN 978-7-115-1906/09-148

定价：15元

本书如有印装质量问题，请与本社联系　电话：(010)67114922