

ICS 33.040.50
M 19



中华人民共和国通信行业标准

YD/T 2046-2009

接入网安全技术要求 ——xDSL 用户端设备

Technical requirements for security of xDSL CPE

2009-12-11 发布

2010-01-01 实施

中华人民共和国工业和信息化部 发布

目 次

前 言.....II

1 范围.....1

2 规范性引用文件.....1

3 缩略语.....1

4 xDSL 用户端设备分类.....2

5 概述.....3

6 用户平面安全.....3

 6.1 类型 1 的 xDSL 用户端设备用户平面安全.....3

 6.2 类型 2 的 xDSL 用户端设备用户平面安全.....3

 6.3 类型 3 的 xDSL 用户端设备用户平面安全.....4

 6.4 类型 4 的 xDSL 用户端设备用户平面安全.....6

7 控制平面安全.....6

 7.1 IGMP Snooping 和 IGMP Snooping 代理功能.....6

 7.2 防火墙 TCP 连接控制.....6

 7.3 VoIP 业务的用户接入安全.....6

8 管理平面安全.....6

 8.1 远程管理安全.....6

 8.2 本地管理安全.....7

 8.3 防火墙日志管理.....7

9 可靠性要求.....7

 9.1 设备一般要求.....7

 9.2 设备电气安全.....7

前 言

本标准是接入网安全系列标准之一，该系列标准预计结构及名称如下：

1. YD/T 2046-2009 接入网安全技术要求——xDSL用户端设备
2. YD/T 2047-2009 接入网设备安全测试方法——xDSL用户端设备
3. YD/T 2048-2009 接入网安全技术要求——DSL接入复用器（DSLAM设备）
4. YD/T 2049-2009 接入网设备安全测试方法——DSL接入复用器（DSLAM）设备
5. TD/T 2050-2009 接入网安全技术要求——无源光网络（PDN）设备
6. TD/T 2051-2009 接入网设备安全测试方法——无源光网络（PDN）设备
7. TD/T 1910-2009 接入网安全技术要求——综合接入系统
8. 接入网设备安全测试方法——综合接入系统

在本标准的制定过程中注意了与以下标准的协调统一：

1. YD/T 1323-2004 接入网技术要求——不对称数字用户线（ADSL）
2. YD/T 1239-2002 接入网技术要求——甚高速数字用户线（VDSL）
3. YD/T 1530-2006 接入网技术要求——频谱扩展的第二代不对称数字用户线(ADSL2+)
4. YD/T 1188-2008 接入网技术要求——不对称数字用户线(ADSL/ADSL2+)用户端设备
5. YD/T 1996-2009 接入网技术要求——第二代甚高速数字用户线（VDSL2）

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、中兴通讯股份有限公司、华为技术有限公司、上海贝尔股份有限公司、国家计算机网络应急技术处理协调中心。

本标准主要起草人：赵 苹、程 强、刘 谦、陈 洁、敖 立、党梅梅、葛 坚、李云洁、袁立权、牛乐宏、姚亦峰。

接入网安全技术要求——xDSL 用户端设备

1 范围

本标准规定了xDSL用户端设备的用户平面、控制平面、管理平面的安全性要求，以及设备可靠性要求。

本标准适用于公众电信网的xDSL用户端设备。专用电信网的xDSL用户端设备也可参考使用。

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。

YD/T 1082-2000	接入网设备过电压过电流防护及基本环境适应性技术条件
YD/T 1132-2001	防火墙设备技术要求
YD/T 1244-2002	数字用户线（xDSL）设备电磁兼容性要求和测量方法
YD/T 1706-2007	接入网技术要求——数字用户线（DSL）承载宽带业务
ITU-T X.805	端到端通信系统安全框架
IEEE 802.1ag	链接故障管理
IEEE 802.1D	媒体访问控制网桥
IEEE 802.1Q	虚拟桥接局域网
IEEE 802.1X	基于端口的网络接入控制
IEEE 802.3	局域网和城域网 第三部分：CSMA/CD接入方法和物理层规范
IETF RFC3947	在IKE中协商NAT穿透
IETF RFC3948	UDP封装IPsec ESP报文
TR-069	CPE WAN 管理协议

3 缩略语

下列缩略语适用于本标准。

ADSL	Asymmetric Digital Subscriber Line	不对称数字用户线
ADSL2+	Asymmetric Digital Subscriber Line Transceivers 2 plus	频谱扩展的第二代不对称数字用户线
ALG	Application Layer Gateway	应用层网关
ARP	Address Resolution Protocol	地址解析协议
ATM	Asynchronous Transfer Mode	异步传输模式
CPE	Customer Premises Equipment	客户驻地设备
DHCP	Dynamic Host Configuration Protocol	动态主机配置协议

DoS	Denial of Service	拒绝服务
DSL	Digital Subscriber Line	数字用户线
ICMP	Internet Control Message Protocol	因特网控制消息协议
HTTP	Hypertext Transfer Protocol	超文本传输协议
IGMP	Internet Group Management Protocol	因特网组管理协议
IKE	Internet Key Exchange	因特网密钥交换
IP	Internet Protocol	互连网协议
L2TP	Layer 2 Tunneling Protocol	二层隧道协议
MAC	Medium Access Control	媒质访问控制
MTBF	Meaning Time Between Failure	无故障平均工作时间
NAPT	Network Address Port Translation	网络地址端口转换
NAT	Network Address Translation	网络地址转换
PPPoE	PPP over Ethernet	以太网承载 PPP
PPTP	Point-to-Point Tunneling Protocol	点对点通道协议
QoS	Quality of Service	服务质量
RSTP	Rapid Spanning Tree Protocol	快速生成树协议
SSL	Secure Sockets Layer	安全套接字层
STP	Spanning Tree Protocol	生成树协议
SYN	Synchronize Sequence Number	同步序列号
TCP	Transmission Control Protocol	传输控制协议
TLS	Transport Layer Security	传输层安全
UDP	User Datagram Protocol	用户数据报协议
URL	Universal Resource Locator	通用资源定位
VDSL	Very High Speed Digital Subscriber Line	甚高速数字用户线
VDSL2	Very High Speed Digital Subscriber Line 2	第二代甚高速数字用户线
VoIP	Voice over IP	IP 语音
VLAN	Virtual LAN	虚拟局域网
VPN	Virtual Private Network	虚拟专网
WAN	Wide Area Network	广域网
WLAN	Wireless Local Area Network	无线局域网

4 xDSL 用户端设备分类

xDSL用户端设备是指线路侧接口可以是ADSL、ADSL2+、VDSL、VDSL2的DSL用户端设备。

按照所支持的功能，xDSL用户端设备可分为4类。

- 类型1：仅具有桥接功能的xDSL用户端设备，支持Internet 接入业务。
- 类型2：具有路由功能的xDSL用户端设备，仅支持IP层以及IP层以下各层的相关功能，不支持IP层以上和业务/应用相关的功能，支持Internet接入业务。

- 类型3：即为支持多业务而具有QoS、安全等功能的xDSL用户端设备，但是不支持实现业务相关的功能（例如VoIP编解码等）。
- 类型4：支持业务实现功能的xDSL用户端设备，即除了具有类型3 xDSL用户端设备支持的各项功能和业务承载之外，还具有与业务实现相关的各项功能（如为实现VoIP而支持的相关功能等）。

5 概述

ITU-T X.805 定义了一个完整的端到端通信系统的安全框架，定义了应用层、业务层和基础设施层3个网络层次，并为每个网络层次定义了用户、控制和管理3个平面。对每个层次的每个平面都分别从访问控制、鉴别、不可抵赖、数据保密性、通信安全、完整性、可用性和隐私8个方面考虑其安全性。

xDSL用户端设备作为基础设施层的网元设备，其安全要求包括：用户平面安全要求、控制平面安全要求、管理平面安全要求和设备可靠性要求。用户平面安全要求使xDSL用户端设备在面临一些安全威胁时仍能安全地转发业务流。控制平面安全要求能够保证xDSL用户端设备与网络之间、xDSL用户端设备与用户终端之间控制消息和信令的安全传递，防止用户通过协议报文进行攻击。管理平面安全要求能够保证xDSL用户端设备远程和本地管理系统在面临管理方面的安全威胁时的安全性。

6 用户平面安全

6.1 类型 1 的 xDSL 用户端设备用户平面安全

6.1.1 帧过滤功能

xDSL用户端设备应支持对NETBEUI、BPDU、GVRP、GMRP等MAC帧（见表1）进行过滤，可选支持针对MAC源地址和/或目的地址设置过滤条目。

表 1 预定义和保留地址的 MAC 帧处理

目的 MAC 地址	作 用	缺省行为	可选配置	引用标准
01-80-C2-00-00-00	桥组地址 (BPDUs)	Block	None	IEEE 802.1D, Table 7-9
01-80-C2-00-00-01	PAUSE	Block	None	IEEE 802.3
01-80-C2-00-00-02	慢速协议 (LACP, EFM OAM PDUs)	Block	Peer	IEEE 802.3, Table 43B-1
01-80-C2-00-00-03	EAP over LANs	Block	Peer	IEEE 802.1X, Table 7-2
01-80-C2-00-00-04 - 01-80-C2-00-00-0F	保留	Block	None	IEEE 802.1D, Table 7-9
01-80-C2-00-00-10	所有 LAN 的桥管理地址	Block	None	IEEE 802.1D, Table 7-10
01-80-C2-00-00-20	GMRP	Block	None	IEEE 802.1D, Table 12-1
01-80-C2-00-00-21	GVRP	Block	None	IEEE 802.1Q, Table 11-1
01-80-C2-00-00-22 - 01-80-C2-00-00-2F	保留 GARP 应用地址	Block	Forward	IEEE 802.1D, Table 12-1
01-80-C2-xx-xx-xy	CFM	Forward	Block	IEEE 802.1ag-D6, Table 8-9

6.1.2 MAC 地址表深度控制功能

为了防止MAC泛洪攻击，xDSL用户端设备应当可以配置并限制从每个用户端口学习到的源MAC地址的数量。

6.2 类型 2 的 xDSL 用户端设备用户平面安全

6.2.1 概述

除应支持6.1的功能要求之外，还应支持6.2.2、6.2.3、6.2.4、6.2.5和6.2.6所述功能。

6.2.2 广播帧速率抑制功能

为了防止形成广播风暴，xDSL用户端设备应对协议特定的广播/多播包（例如DHCP、ARP、IGMP等）进行抑制。应具备对其它二层广播报文进行速率限制的功能。

6.2.3 NAT 穿越

当xDSL用户端设备支持并且实现NAT/NAPT功能时，应支持对IPSec、L2TP和PPTP等VPN协议的透传，可选提供基于IPSec的VPN Client功能；应支持与xDSL用户端设备相连的VPN客户设备发起IPSec会话；应支持与xDSL用户端设备相连的多个用户同时发起独立的IPSec会话；应支持与xDSL用户端设备相连的VPN客户设备采用UDP封装IPSec报文，详见IETF RFC3948；应支持与xDSL用户端设备相连的VPN客户设备协商IKE的NAT穿越，详见IETF RFC3947。

6.2.4 RSTP、STP 协议

为了防止形成以太网环网，多端口的xDSL用户端设备应支持RSTP协议，RSTP协议要求见IEEE 802.1D《媒体访问控制网桥》。可选支持STP协议。

6.3 类型 3 的 xDSL 用户端设备用户平面安全

6.3.1 概述

除应支持6.1和6.2的功能要求之外，还应支持6.3.2、6.3.3所述功能。

6.3.2 防火墙功能

6.3.2.1 概述

应支持防火墙功能，包括接入控制能力、报文过滤能力、防端口扫描能力、防止非法报文攻击能力，保证业务流能正常通过防火墙。

建议防火墙功能支持对7层协议栈中的有状态包检测和包过滤功能。

建议防火墙功能符合YD/T 1132-2001《防火墙设备技术要求》的要求。

6.3.2.2 防火墙等级设定

支持防火墙高、中、低等级设置，每个安全等级的内容可以修改。

可选在本地Web界面配置防火墙的等级，分为高、中、低三级。

6.3.2.3 报文丢弃

应支持丢弃以下类型的报文：

- 源与目的地址相同的报文；
- 源地址为广播的报文；
- 非法碎片IP报文。

6.3.2.4 防火墙过滤功能

应支持基于以下防火墙过滤规则：

- 源、目的IP地址及子网掩码；
- 源、目的MAC地址；
- IP源端口及范围段、目的端口及范围段；
- Ethertype；
- 以太网包的传输层协议类型进行报文过滤，要求有IPoE/PPPoE/ARP的选项；
- IP包的传输层协议类型进行报文过滤，要求有TCP/UDP/ICMP/TCP+UDP/ANY的选项；

- 对匹配规则的报文进行处理模式的选择，对匹配规则的报文的处理模式有允许和禁止两种，默认为禁止模式。

6.3.2.5 防非法报文攻击功能

设备应支持防DoS攻击功能，对收到的数据包进行解析，并判断是否是DoS攻击，对于DoS攻击的报文进行防DoS攻击处理。该保护适用于所有终结在本设备的IP和桥接的IP的情况。DoS攻击的类型包括：

- Ping of Death;
- SYN Flooding;
- ARP Flooding;
- Spoofing;
- LAND;
- Smurf;
- 其他。

停止攻击后，设备能恢复正常工作，攻击过程中，设备不能死机。

SYN Flood是指攻击设备不断地成倍发送只有SYN标志的TCP连接请求，以消耗尽被攻击设备的资源。

Ping of Death是指利用一些超大字节的ICMP报文对设备进行攻击，使得设备系统崩溃死机或者重启。

6.3.2.6 防端口扫描功能

宽带客户网关应支持防端口扫描功能，防止攻击者通过端口扫描试探设备上打开的端口和服务。

6.3.2.7 支持端口映射功能

应支持端口映射的设置，支持的端口映射功能包括：

- 前转的目的IP地址采用私网地址；
- 可以组合源/目的IP地址、协议类型（TCP、UDP）、端口或者端口范围，映射到指定的LAN设备的某个端口；
- 支持默认应用列表，支持通用的应用协议的配置，如FTP、HTTP等；
- 默认应用列表端口映射规则可查看、可修改。

端口映射（可选）支持Port Trigger功能，当NAT网关设备收到内部网络的数据包满足触发条件时，这个触发条件一般是协议端口符合预设的端口范围，就会根据预设的开放端口进行端口映射，以提供外部网络访问这些端口的能力。

6.3.2.8 基于用户账号的防火墙配置（可选）

用户账号与防火墙策略的绑定。不同用户账号可以自动启用对应的防火墙策略。

6.3.3 MAC地址可控功能

为了防止MAC泛洪攻击，xDSL用户端设备应当可以配置并限制从每个用户端口学习到的源MAC地址的数量。地址表深度不小于256。

6.3.4 DMZ功能

xDSL用户端设备应支持DMZ功能。

6.3.5 URL访问控制功能

xDSL用户端设备应支持设置黑白名单，实现URL访问控制功能。黑白名单应支持与账号绑定。

6.4 类型4的xDSL用户端设备用户平面安全

6.4.1 概述

除应支持6.1、6.2和6.3的功能要求之外，还应支持6.4.2所述功能。

6.4.2 逃生功能（可选）

xDSL用户端设备可选支持VoIP业务的IP网络故障逃生、断电逃生功能，即当IP网络故障或CPE断电时，能够切换到PSTN线路。

7 控制平面安全

7.1 IGMP Snooping 和 IGMP Snooping 代理功能

类型3和类型4的xDSL用户端设备应支持本节规定的功能。

7.1.1 IGMP Snooping 代理功能

xDSL用户端设备应支持IGMP Snooping代理功能，该功能定义见YD/T 1706-2007《接入网技术要求——数字用户线（DSL）承载宽带业务》的3.8。

多端口的xDSL用户端设备应支持IGMP Snooping功能。

7.1.2 非法组播源控制功能

xDSL用户端设备应防止用户做源的组播。可以禁止用户端口发出的IGMP Query和组播数据报文。

7.2 防火墙 TCP 连接控制

类型3和类型4的xDSL用户端设备应支持本节规定的功能。

防火墙应能丢弃超出设备所能接受的会话连接。

防火墙应支持能够丢弃或者拒绝来自WAN侧到LAN侧设备的TCP连接请求和访问。

7.3 VoIP 业务的用户接入安全

对于类型4的xDSL用户端设备可以通过惟一的标识码向软交换注册并且认证，认证功能可选。当xDSL用户端设备向软交换传送数据时，应保证用户信息的安全性、保密性和完整性。

8 管理平面安全

8.1 远程管理安全

类型1和类型2的xDSL用户端设备可选支持远程管理安全功能，类型3和类型4的xDSL用户端设备应支持远程管理安全功能。

8.1.1 远程管理访问控制功能

8.1.1.1 WAN侧隔离

缺省情况下不允许通过WAN侧以Telnet/HTTP/FTP方式（TR-069协议除外）访问网关设备本身进行设备数据配置。

8.1.1.2 服务访问控制

支持ACL规则的配置，可以配置授权的地址范围（默认为任何IP地址），可以配置访问的接口（WAN/LAN），可以配置接入方式Web/FTP/Telnet/SNMP/SSH，默认情况下不允许通过WAN侧访问设备。

8.1.1.3 黑白名单

访问控制规则可以以黑名单或者白名单方式生效。

8.1.2 设备认证

当采用TR-069方式对xDSL用户端设备进行远程管理时，远程管理服务器对xDSL用户端设备进行远程管理之前应能与其进行设备认证，认证方式包括：

- 基于 HTTP 的基本认证；
- 基于 HTTP 的摘要认证；
- 基于 SSL/TLS 的证书认证。

8.1.3 恢复出厂配置

如系统需要，设备应能远程控制恢复出厂配置。

8.1.4 版本升级的安全要求

升级时本地应备份旧版本，当升级不成功或异常中断时恢复到前一版本。

8.2 本地管理安全

xDSL用户端设备应具有两种权限进行不同的本地维护管理功能：普通用户管理权限和管理员本地维护管理权限。用户进行网络管理时所使用的登录口令的长度应不少于8个字符，并且应由数字、字符或特殊符号组成，xDSL用户端设备可选提供检查机制，保证每个口令至少是由前述的三类符号中的两类组成。

普通用户管理权限可以对xDSL用户端设备的一些非重要参数进行配置与查询，包括设备基本信息、普通用户管理密码、WLAN相关参数、MAC地址过滤、VoIP相关信息等。

管理员本地维护管理权限可以对xDSL用户端设备的重要参数进行配置与查询，包括用户管理权限可配置的参数、远程管理服务器URL、网络侧相关参数（DSL、ATM、PPPoE、IP、桥接或路由工作模式等相关参数）和用户侧参数（根据不同类型的xDSL用户端设备，不同的参数，例如DHCP、路由、ALG、NAT、IGMP、QoS、防火墙等相关参数）。

8.3 防火墙日志管理

类型3和类型4的xDSL用户端设备应支持此功能。

应提供独立的防火墙日志，记录所有违背防火墙规则操作，每个条目都应打上时间戳。日志应至少包括100条条目或者大小为10kbyte的文本。日志不应该被清除，除非是设备复位到默认或者出厂配置。

9 可靠性要求

9.1 设备一般要求

xDSL用户端设备应能在一天24h，连续7d工作的情况下，不需要重启而能正常工作。

xDSL用户端设备的MTBF应至少为1年。

设备的生命周期至少能达到7年。

9.2 设备电气安全

9.2.1 过压、过流保护

xDSL用户端设备应安装过压、过流保护器。过压、过流保护器在外接电源异常时保护设备的核心部分。

xDSL用户端设备应满足YD/T 1082-2000《接入网设备过电压过电流防护及基本环境适应性技术条件》的要求，其中对于要求性能不劣化的过压、过流测试项目，经过压、过流测试后的设备应能达到相关的DSL传输性能要求。

9.2.2 电磁兼容

应满足YD/T1244-2002《数字用户线（xDSL）设备电磁兼容性要求和测量方法》的要求。