



中华人民共和国通信行业标准

YD/T 2048-2009

接入网安全技术要求 ——DSL 接入复用器 (DSLAM) 设备

Technical requirements for security of Digital Subscriber Line
Access Multiplexer (DSLAM)

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 概述.....2

5 用户平面安全要求.....2

6 控制平面安全要求.....3

7 管理平面安全要求.....4

8 可靠性要求.....7

9 设备电气安全.....8

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. YD/T 2050-2009 接入网安全技术要求——无源光网络（PON）设备
6. YD/T 2051-2009 接入网设备安全测试方法——无源光网络（PON）设备
7. YD/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 1055-2005 接入网设备测试方法——带话音分离器的不对称数字用户线（ADSL）
4. 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+)
5. YD/T 1706-2007 接入网技术要求——数字用户线（DSL）承载宽带业务
6. 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、大唐电信科技产业集团、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：程 强、刘 谦、赵 苹、陈 洁、敖 立、牛乐宏、袁立权、姚亦峰、党梅梅、葛 坚、李云洁。

接入网安全技术要求
——DSL 接入复用器（DSLAM）设备

1 范围

本标准规定了数字用户线接入复用设备（DSLAM）的用户平面、控制平面和管理平面的安全性要求，以及对设备可靠性和电气安全方面的要求。

本标准适用于公众电信网的局端xDSL接入复用器设备，对于放置在远端的DSL接入复用设备可以参考使用。专用电信网也可参考使用。

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 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 |
| IETF RFC1157 | 简单网络管理协议 |
| IETF RFC1901 | 基于团体的SNMPv2简介 |
| IEEE 802.1ad | 虚拟桥接的局域网 附件4：运营商桥 |
| 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 |

3 缩略语

下列缩略语适用于本标准。

| | | |
|--------|--|------------------|
| AAA | Authentication, Authorization and Accounting | 认证、鉴权和计费 |
| ADSL | Asymmetric Digital Subscriber Line | 不对称数字用户线 |
| ADSL2+ | Asymmetric Digital Subscriber Line 2 plus | 频谱扩展的第二代不对称数字用户线 |
| ARP | Address Resolution Protocol | 地址解析协议 |
| BNG | Broadband Network Gateway | 宽带网络网关 |
| C-VID | Custom VLAN IDentifier | 客户 VID |
| DELT | Double-Ended Line Test | 双端线路测试 |
| DHCP | Dynamic Host Config Protocol | 动态主机配置协议 |
| DLF | Destination Lookup Failure | 目的查找失败 |
| DSL | Digital Subscriber Line | 数字用户线 |

| | | |
|-------|--|-------------|
| DSLAM | Digital Subscriber Line Access Multiplexer | 数字用户线接入复用器 |
| HTTP | HyperText Transfer Protocol | 超文本传输协议 |
| IGMP | Internet Group Management Protocol | 因特网组管理协议 |
| IP | Internet Protocol | 互联网协议 |
| MAC | Media Access Control | 媒质访问控制 |
| PPP | Point to Point Protocol | 点到点协议 |
| PPPoE | PPP over Ethernet | 以太网承载 PPP |
| RSTP | Rapid Spanning Tree Protocol | 快速生成树协议 |
| SELT | Single-Ended Line Test | 单端线路测试 |
| SNMP | Simple Network Management Protocol | 简单网络管理协议 |
| SSH | Secure Shell | 安全 Shell |
| SSL | Secure Socket Layer | 安全套接字层 |
| S-VID | Service VLAN IDentifier | 业务 VID |
| TLS | Transport Layer Security | 传送层安全 |
| USM | User-based Security Model | 用户安全模型 |
| 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 |
| VID | VLAN ID | VLAN 标识 |
| VLAN | Virtual Local Area Network | 虚拟局域网 |

4 概述

ITU-T X.805《端到端通信系统安全框架》定义了一个完整的端到端通信系统的安全框架，应用层、业务层和基础设施层定义了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。

DSLAM设备作为基础设施层的网元设备，在用户、控制和管理3个平面上的安全功能主要用于保障自身及网络安全、业务提供的安全和信息传递的安全。

用户平面安全要求能够使设备在面临一些安全威胁时仍能安全可靠地转发用户业务流。

控制平面安全要求能够保证设备自身信令功能正常运行与其他业务节点（如BNG、软交换等）之间的信令安全传送，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设备和网管系统在面临管理方面的安全威胁时仍能正常运转。

5 用户平面安全要求

5.1 二层隔离功能

DSLAM设备应对用户侧的所有DSL端口之间提供二层隔离的功能，即同一DSLAM设备下的不同DSL端口上的用户不应通过DSLAM设备上的二层桥接功能直接互通。

5.2 VLAN 功能

DSLAM中的VLAN功能可用来标记不同的广播域，用于业务区分、用户区分等目的。VLAN功能的

具体规定见YD/T 1706-2007的《接入网技术要求——数字用户线（DSL）承载宽带业务》的7.1。

5.3 帧过滤功能

DSLAM应能根据MAC源地址和/或目的地址设置过滤条目。对于预定义和保留地址的MAC 帧（见YD/T 1706-2007《接入网技术要求——数字用户线（DSL）承载宽带业务》表1），DSLAM缺省应过滤掉，不进行转发，但设备可以提供改变缺省行为的配置选项。

DSLAM宜支持基于MAC目的地址、MAC源地址、MAC协议类型、IP目的地址、IP源地址的五元组过滤规则功能。

DSLAM应可配置为过滤从用户端口发出目的地址为组播的UDP流。

5.4 MAC 地址控制功能

DSLAM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。

DSLAM应能防止用户盗用BNG（例如接入服务器或业务路由器）端口的MAC地址。

DSLAM应可以拒绝向存在MAC地址重复的用户提供业务。

5.5 广播/组播/DLF 帧速率抑制

DSLAM应具备对MAC目的地址为广播或组播地址的报文以及DLF报文进行速率限制的功能，在上行方向应默认开启此功能。

DSLAM应支持基于全局的抑制方式，宜支持基于VLAN和端口的抑制方式。

5.6 绑定功能

DSLAM设备应支持对MAC地址、IP地址与端口或VLAN等的绑定。

DSLAM应支持基于静态配置用户IP地址与DSL端口或VLAN的绑定功能。

DSLAM可选支持跟踪DHCP中的IP地址分配过程进行端口、MAC地址和IP地址的动态绑定功能。

5.7 上联口相关功能

DSLAM设备应具备提供至少2个上联以太网接口的能力。

DSLAM设备上联口应支持IEEE 802.3链路聚集功能。

DSLAM设备应支持上联端口通过链路聚合进行链路冗余保护功能。

DSLAM设备应支持多个上联接口通过链路聚合进行链路负载均衡功能。

DSLAM设备上联口应支持快速生成树(RSTP)功能。

5.8 端口镜像功能

DSLAM设备宜支持对特定的物理端口或逻辑端口的流镜像功能。

5.9 协议报文限速

DSLAM设备应支持对特定协议报文（例如，DHCP、IGMP、ICMP等）进行限速处理。

5.10 用户环网检测

DSLAM设备应支持对用户侧端口是否成环的检测，防止环网形成。

6 控制平面安全要求

6.1 IGMP Snooping 代理功能及可控组播功能

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

DSLAM设备应支持基于用户和组播组的访问控制功能，防止非法用户获得无权限收看的内容。

可控组播功能规定见YD/T 1706-2007《接入网技术要求——数字用户线（DSL）承载宽带业务》的7.6.2。

6.2 非法组播源过滤

DSLAM应可配置为过滤从用户端口发出的IGMP查询包。

DSLAM应支持对网络侧合法组播源的配置和对非法组播源进行过滤的配置。

6.3 ARP 代理功能

DSLAM宜支持对ARP协议的代理功能。

对于支持三层转发功能的DSLAM，该功能为必选。

6.4 DHCP 下行处理要求

针对特定用户的下行DHCP响应报文不应被转发到其他用户端口，防止其他用户通过嗅探该报文获得该用户的IP地址。

6.5 端口定位功能

端口定位功能用于标识DSLAM设备的用户业务流通道，并对每个通道按照端口编号计划进行惟一编号，该编号可用于：

- (1) AAA 服务器对用户账号的防盗用；
- (2) 通过 AAA 服务器日志中的用户名、IP 地址、端口号等对故障进行追踪和判断；
- (3) 业务网关和策略服务器等可以根据端口编号关联用户特定的业务配置文件；
- (4) 用户的位置可溯；
- (5) 其他应用等。

DSLAM应支持二层DHCP中继代理、PPPoE中继代理和VLAN堆叠功能。

二层DHCP中继代理功能见YD/T 1706-2007《接入网技术要求——数字用户线（DSL）承载宽带业务》的7.4.2。

PPPoE中继代理功能见YD/T 1706-2007《接入网技术要求——数字用户线（DSL）承载宽带业务》的7.4.3。

VLAN堆叠功能参见IEEE 802.1ad，DSLAM设备应支持采用S-VID、C-VID的惟一组合标识惟一的用户。

6.6 防 DoS 攻击

应具备对攻击目标为本设备的DoS攻击抵御能力，例如Ping of Death、SYN Flood、LAND等攻击。

7 管理平面安全要求

7.1 管理员口令

不论在何种管理方式下，对设备的管理用户都需要鉴别和认证，鉴别和认证是系统访问的基础。与管理权限相关的安全数据应得到妥善的保护。

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、字母或特殊符号组成，DSLAM网管系统应提供检查机制，保证每个口令至少是由前述的三类符号中的两类组成。

无论在设备还是网管系统中，口令不应使用明文保存。

7.2 设备访问方式

7.2.1 SNMP 访问

DSLAM应支持SNMP协议。应支持SNMP v1（见IETF RFC1157）或SNMPv2c（见IETF RFC1901），宜支持SNMPv3。

当采用SNMPv1和SNMPv2c时，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，并且具有提示管理员修改团体名的功能。

支持SNMPv3时，支持USM等安全机制。

DSLAM宜实现对网管站的访问控制，限定用户通过哪些IP地址使用SNMP对设备进行访问。

7.2.2 Telnet 访问（可选）

DSLAM可选支持Telnet。若支持Telnet，则应支持以下安全要求：

- （1）用户应提供用户名/口令才能进行后续的操作，用户地址和操作应记入日志；
- （2）Telnet 访问时应提供对用户的账号的分级管理机制，提供对 Telnet 用户权限的控制功能；
- （3）应限制同时访问的用户数目；
- （4）在设定的时间内不进行交互，用户应自动被注销，提供终端超时锁定功能；
- （5）可限定用户通过哪些 IP 地址使用 Telnet 服务对设备进行访问；
- （6）能够针对 Telnet 的密码试探攻击进行防范；
- （7）必要时可关闭 Telnet 服务。

7.2.3 本地 CONSOLE 访问

DSLAM应能通过其所带的CONSOLE口对其进行带外方式的操作维护，在维护终端与设备进行交互的过程中应提供与Telnet访问方式相同的安全保护能力。

7.2.4 Web 管理（可选）

DSLAM可选支持Web管理方式。若支持Web管理方式，则应支持以下安全要求：

- （1）用户应提供用户名/口令才能进行后续的操作，用户地址和操作应记入日志；
- （2）可限定用户通过哪些 IP 地址使用 HTTP 对设备进行访问；
- （3）可关闭 HTTP 服务；
- （4）支持 SSL/TLS 安全协议或提供其他安全措施，实现对管理用户数据的完整性保护。

7.2.5 SSH 支持（可选）

DSLAM设备可选提供SSH协议支持，提供到设备的TCP连接的安全性保护。在SSH方式下可以承载Telnet、FTP、HTTP等管理协议。

7.3 网管系统安全要求

7.3.1 安全策略管理

网管系统应能提供统一的安全策略控制，包括以下几项。

- （1）登录策略管理：提供设置非法登录系统的次数及锁定时间，设置管理用户的账号有效期，设置登录超时退出时间、账号登录时间段、限制同一账号最大连接数等功能。
- （2）提供管理用户的功能。
- （3）管理用户密码设置策略：限制管理用户设置的密码长度、密码组成，提供密码重置功能，设置用户密码有效天数等。
- （4）支持管理用户登录的 IP 管理策略，将登录的管理用户与 IP 地址绑定。

7.3.2 角色管理

角色表示一类特定的权限的集合，包括管理用户可以登录的客户端IP地址范围，管理用户可以进行的操作，管理用户可以管理的资源等。

通过安全管理可以动态地创建、删除和修改角色，形成新的权限集合，以便分配给管理用户，达到控制管理用户权限的目的。

角色管理功能应包含以下几项。

(1) 增加、删除、修改角色；

(2) 给角色分配管理资源（可管理的对象范围）和操作权限。

(3) 从操作权限来说，网管系统应可以提供三类缺省的角色：

- 系统管理员：可以执行网管系统提供的所有功能项，包括权限分配功能。
- 配置管理员：可以执行网管系统提供的对设备和系统自身有数据修改权限的功能（不包括权限分配功能），如资源维护、设备配置、版本升级、系统维护等。
- 监控管理员：可以执行网管系统提供的对设备的监控和网管系统自身的查询和审计等功能，如资源查询、告警监控、性能统计、日志查询等。

网管系统应提供灵活的角色创建功能，如可以根据管理用户的需要再单独创建版本管理员、统计管理员等角色。

从管理资源来说，这些操作权限都应可以指定管理的范围。

7.3.3 账号管理

对使用网管系统的管理用户账号进行管理维护，包括：

(1) 增加账号；

(2) 删除账号；

(3) 修改账号信息；

(4) 查询账号信息。

管理用户的账号信息包括：

(1) 用户账号；

(2) 用户密码；

(3) 密码有效期；

(4) 用户所属角色；

(5) 附加说明。

支持同一个管理员账号属于多个角色组。

7.3.4 管理用户登录管理

网管系统应能提供完善的用户登录管理功能，包括：

(1) 只有在服务器中已经注册的用户才能登录到网管系统，如果启动了访问控制列表功能，则客户端必须同时满足存在于网管系统 ACL 表中的用户才能登录到网管系统；

(2) 登录的用户只具有已经被授权的指定操作；

(3) 登录失败告警，使用同一管理账号连续多次登录失败时，网管系统应产生非法登录告警，并对该管理账号进行锁定；

- (4) 手工注销登录的用户;
- (5) 手工或超时自动锁定客户端或退出。

7.3.5 在线管理用户管理

网管系统应能对在线用户进行监视, 能够实时监视在线用户的登录情况, 包括:

- (1) 登录用户;
- (2) 登录时间;
- (3) 操作终端信息。

网管系统应能对在线用户进行管理, 超级用户能够查看一般用户所做的操作, 并强制其退出。

7.3.6 日志管理

管理用户可以根据给定条件对日志进行查询, 并可对查询到的日志进行排序。

查询的条件为:

- (1) 给定时间或时间段进行查询;
- (2) 给定用户进行查询;
- (3) 给定的日志类型。

可以查询到的信息包括:

- (1) 日志类型, 包括操作日志、系统日志、安全日志;
- (2) 操作时间;
- (3) 操作人;
- (4) 操作名称;
- (5) 操作对象;
- (6) 操作内容;
- (7) 操作终端;
- (8) 操作结果(例如成功或失败)。

8 可靠性要求

8.1 线路故障诊断

DSLAM应提供对ADSL2/ADSL2+和VDSL2线路的内置的DELT和SELT测试功能, 以帮助判断线路故障。

8.2 设备故障

大容量的DSLAM应支持主控板的1+1备份功能, 在主控板倒换过程中不应丢失配置数据, 用户业务不发生中断。

8.3 环境监控

DSLAM设备应能提供对设备风扇工作情况、内部温度等环境信息的收集和上报功能。

8.4 电源安全性

对于采用单独电源模块集中供电设备, 应支持双电源模块热备份功能。

对于分散单板供电设备, 应提供两个互为备份的电源接口。

9 设备电气安全

9.1 绝缘电阻

正常情况下，设备的绝缘电阻不应小于 $50\text{M}\Omega$ 。

9.2 设备接地要求

设备的接地电阻应小于 5Ω 。

9.3 过压、过流保护

ADSL局端和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。

ADSL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》对模拟雷电冲击、电力线感应、电力线接触等指标的要求。

9.4 电磁兼容

设备的电磁兼容性指标应满足YD/T 1244-2002《数字用户线（xDSL）设备电磁兼容性要求和测量方法》的要求。
