

ICS 33.040.50

M 19



中华人民共和国通信行业标准

YD/T 2050-2009

接入网安全技术要求 ——无源光网络（PON）设备

Technical requirements for security of passive optical network
(PON) equipment

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	4
7 管理平面安全要求	5
8 设备可靠性要求	8
9 设备电气安全	9

前 言

本标准是接入网设备安全系列标准之一，该标准系列的名称和结构预计如下：

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

本标准在制定过程中注意了和下列标准的协调统一：

1. YD/T 1475-2006 接入网技术要求——基于以太网方式的无源光网络（EPON）
2. YD/T 1771-2008 接入网技术要求——EPON 系统互通性
3. YD/T 1949-2009 接入网技术要求——吉比特的无源光网络
4. YD/T 1953-2009 接入网技术要求——EPON/GPON 系统承载多业务

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：陈 洁、程 强、刘 谦、赵 苹、敖 立、党梅梅、葛 坚、李云洁、张博山、牛乐宏、姚亦峰。

接入网安全技术要求——无源光网络(PON)设备

1 范围

本标准规定了PON设备（包括EPON设备和GPON设备）的用户平面安全要求、控制平面安全要求、管理平面安全要求、设备可靠性和电气安全要求。

本标准适用于公众电信网环境下的PON设备，专用电信网也可参照使用。

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。

GB 9254-1998	信息技术设备的无线电骚扰限值和测量方法
GB/T 17618-1998	信息技术设备抗扰度限值和测量方法
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 1475-2006	接入网技术要求——基于以太网方式的无源光网络（EPON）
YD/T 1771-2008	接入网技术要求——EPON 系统互通性要求
YD/T 1949.1-2009	接入网技术要求——吉比特的无源光网络（GPON） 第1部分 总体要求
YD/T 1949.3-2009	接入网技术要求——吉比特的无源光网络（GPON） 第3部分 传输汇聚（TC）层要求
IEEE 802.1ag	局域网和城域网——虚拟桥接局域网增补件5：连接故障管理
IEEE 802.1D	局域网和城域网——MAC桥
IEEE 802.1Q	局域网和城域网——虚拟桥接局域网
IEEE 802.1X	局域网和城域网——基于端口的网络接入控制
IEEE 802.3	信息技术——系统间通信和信息交换——局域网和城域网特定要求——第3部分：CSMA/CD接入方式和物理层规范
IETF RFC1901	基于团体名的 SNMPv2

3 缩略语

下列缩略语适用于本标准。

BRAS	Broadband Remote Access Server	宽带远程接入服务器
DHCP	Dynamic Host Config Protocol	动态主机配置协议
DLF	Destination Lookup Failure	目的查找失败
DoS	Denial of Service	拒绝服务
EPON	Ethernet Passive Optical Network	基于以太网方式的无源光网络
GPON	Gigabit-Capable Passive Optical Network	吉比特无源光网络

IGMP	Internet Group Management Protocol	互联网组管理协议
MDU	Multi-Dwelling Unit	多住户单元
OLT	Optical Line Terminal	光线路终端
OMCI	ONT Management and Control Interface	ONT 管理控制接口
ONU	Optical Network Unit	光网络单元
PON	Passive Optical Network	无源光网络
PPP	Point to Point Protocol	点到点协议
PPPoE	PPP over Ethernet	以太网承载 PPP
SCB	Single Copy Broadcast	单拷贝广播
SSL	Secure Sockets Layer	安全套件层
TC	Transmission Convergence	传输汇聚
TCP	Transmission Control Protocol	传输控制协议
TLS	Transport Layer Security	传输层安全
UDP	User Datagram Protocol	用户数据协议
USM	User-based Security Model	基于用户的安全模型
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，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。

PON设备（包括EPON设备和GPON设备）用户平面安全要求在面临信息安全威胁时仍然能够保证用户数据信息在OLT上联接口和ONU下联接口之间的安全传递。

PON设备控制平面安全要求能够保障OLT和ONU之间、OLT和网络节点设备之间、ONU和用户设备之间控制消息和信令的安全传递，防止非法用户通过协议报文攻击网络。

PON设备管理平面安全要求在面临安全威胁时仍能够保证管理用户、网管系统和PON设备三者之间的安全接入和管理信息的安全传递。

5 用户平面安全要求

5.1 数据加密功能

PON设备在下行方向应支持对用户单播数据进行加密，以保证用户数据的安全性。下行组播业务和上行用户数据无需进行加密处理。

EPON设备应采用三重搅动方法对用户数据进行保护，具体应符合YD/T 1771-2008《接入网技术要求——EPON系统互通性要求》的规定。

GPON设备采用的加密算法应符合YD/T 1949.3-2009《接入网技术要求——吉比特的无源光网络（GPON）第3部分 传输汇聚（TC）层要求》的规定。

5.2 二层隔离

OLT应支持各ONU之间的二层隔离，即同一OLT设备上同一和不同PON接口下的各ONU之间均不应通过OLT设备上的二层桥接功能直接互通。

MDU类型的ONU应支持各用户物理端口之间的二层隔离，即各用户物理端口之间不应通过ONU上的二层桥接功能直接互通。

5.3 帧过滤

5.3.1 OLT 的帧过滤功能

OLT应支持根据以太网封装协议、源/目的MAC地址、源/目的IP地址和TCP/UDP端口号对上、下行以太网数据帧进行过滤。

OLT应能过滤来自用户的组播流。

缺省状态下，OLT应支持过滤表 1规定的预定义和保留地址的MAC帧，但OLT可以提供改变缺省行为的配置选项。

表1 预定义和保留MAC地址

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

5.3.2 ONU 的帧过滤功能

ONU应支持根据物理端口、以太网帧封装协议、源/目的MAC地址、以太网优先级标记 (P-bit) 对上、下行以太网数据帧进行过滤。

缺省状态下，ONU应支持过滤表 1规定的预定义和保留地址的MAC帧，但ONU可以提供改变缺省行为的配置选项。

建议ONU支持基于源/目的IP地址和TCP/UDP端口号对数据帧进行过滤。

建议ONU过滤来自用户的组播流。

5.4 组播/广播/DLF 报文风暴抑制

OLT应对二层组播/广播/DLF报文的速率进行抑制，在上行方向应默认开启此功能。

OLT应支持基于全局的抑制方式，建议支持基于VLAN和端口的抑制方式。

5.5 协议报文限速

OLT和MDU类型ONU应支持对特定协议报文（例如，DHCP、IGMP、ICMP等）进行限速处理。

5.6 MAC 地址控制功能

5.6.1 OLT 的 MAC 地址控制功能

OLT应能配置并限制从每个ONU学习到的MAC地址的数量，限制的数量应可以灵活配置。

当达到MAC地址表深度时，OLT应支持忽略新MAC地址直到旧MAC地址老化等不同策略。

5.6.2 ONU 的 MAC 地址控制功能

ONU应支持限制从每个用户物理端口学习到的MAC地址的数量，且限制的数量应可以灵活配置。

当达到MAC地址表深度时，ONU应支持忽略新MAC地址直到旧MAC地址老化等不同策略。

5.7 防止 MAC 地址欺骗

OLT应能够防止用户MAC地址欺骗，应支持丢弃重复的MAC地址的帧。

OLT应能够防止用户仿冒宽带网络网关（如BRAS）的MAC地址。

5.8 IP 地址绑定功能

OLT和MDU类型的ONU应支持IP地址与端口或VLAN等的绑定，地址绑定功能应包含下面两个子功能：

- （1）端口a被限制仅能使用地址A，不能使用除地址A外的其他地址；
- （2）端口b不能盗用端口a使用的地址A。

OLT和MDU类型的ONU应支持基于静态配置用户IP地址与用户端口或VLAN的绑定功能。

OLT和MDU类型的ONU可选支持跟踪DHCP中的IP地址分配过程进行端口和IP地址的动态绑定功能。

5.9 VLAN 和 VLAN Stacking

OLT和ONU应支持通过VLAN实现用户隔离和业务隔离，并应支持对不信任用户的VLAN ID进行丢弃或切换处理。

OLT和ONU应支持的VLAN和VLAN Stacking具体功能要求见YD/T 1949.1-2009《接入网技术要求——吉比特的无源光网络（GPON）第1部分 总体要求》的规定。

5.10 RTP 报文过滤功能

对于内置VoIP语音功能的ONU，当遭到未建立呼叫的、目的为本设备的RTP报文攻击时，ONU应丢弃所有的非法RTP报文，并且语音业务质量应不受影响。

5.11 上联端口安全相关功能

PON设备的OLT应具备提供至少2个上联以太网接口的能力。

PON设备的OLT上联端口应支持IEEE 802.3规定的链路聚集功能，应实现链路负载分担和链路冗余保护功能。

PON设备的OLT上联端口应支持快速生成树（RSTP）功能。

PON设备的OLT上联端口应支持对特定的物理端口或逻辑端口的流镜像功能。

5.12 用户环网检测

ONU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 ONU 认证

EPON设备的OLT应支持根据ONU的MAC地址对其合法性进行认证的能力，应拒绝非法ONU接入网络获得服务。

GPON设备的OLT应支持根据ONU序列号对其合法性进行认证的能力，可选支持同时采用序列号和

password对ONU进行合法性认证，应拒绝非法ONU接入网络获得服务。

非法ONU事件应记入系统日志，并应产生相应警告信息。

6.2 用户端口识别与定位功能

OLT设备和MDU类型的ONU应支持用户物理端口的识别和标记功能，并按照端口编号计划进行惟一编号。

OLT和MDU类型的ONU应支持通过二层DHCP中继代理、PPPoE中继代理和VLAN Stacking功能传递用户端口信息，端口信息可包括OLT设备标识、槽位号、PON端口号、ONU标识、用户物理端口号、VLAN ID和VPI/VCI等信息。

6.3 可控组播

PON设备应支持组播权限控制功能阻止非法用户获取组播业务，具体要求见YD/T 1949.1-2009《接入网技术要求——吉比特的无源光网络（GPON）第1部分 总体要求》的规定。

6.4 过滤功能

OLT应能够过滤来自用户端口的IGMP查询帧和DHCP OFFER/ACK/NAK帧。

OLT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。

建议ONU支持过滤来自用户端口的IGMP查询帧和DHCP OFFER/ACK/NAK帧。

6.5 防DoS攻击

OLT、HGU类型ONU和MDU类型的ONU均应支持防止攻击目标为本设备的Ping of Death、SYN Flood、LAND攻击和IP欺骗等DoS攻击，当遭遇DoS攻击时，应能保证用户正常数据流的正常转发。

6.6 ARP代理功能

为了防止形成广播风暴，建议OLT支持ARP协议代理功能。对支持三层功能的OLT设备，应支持ARP代理功能。

6.7 心跳机制

提供VoIP业务的ONU应定期向软交换发送心跳消息，并应能正确响应软交换发送的心跳消息。

6.8 SIP协议的注册认证功能

对于采用SIP协议提供VoIP业务的ONU，在向软交换注册时，可选支持认证功能。

7 管理平面安全要求

7.1 管理员口令

(1) 应对PON设备的管理用户进行鉴别和认证，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。

(2) 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，PON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。

(3) 无论在设备还是网管系统中，管理员口令不应使用明文保存。

7.2 设备访问方式

7.2.1 基本要求

OLT设备应支持带内和带外访问的管理方式。建议使用带外方式进行管理。在保证通信安全的前提下，PON设备也可采用带内方式管理。

OLT设备应支持SNMP管理控制方式和CONSOLE管理控制方式，可选支持Telnet（SSH）和Web管理控制方式。

7.2.2 SNMP 访问

OLT设备应支持SNMPv2c（见IETF RFC1901），宜支持SNMPv3。

支持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，并且在适当的时机提示管理员修改团体名。

支持SNMPv3时，支持USM等安全机制。

建议OLT实现对网管站的访问控制，限定通过哪些IP地址使用SNMP对设备进行访问。

7.2.3 本地 CONSOLE 访问

OLT设备应能通过其所带的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 Telnet 访问（可选）

OLT设备可选支持Telnet访问方式。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，可对同一个IP地址使用延时响应机制，也可利用限定来自同一个IP地址的登录尝试次数；
- （7）应支持关闭Telnet服务。

7.2.5 Web 访问（可选）

OLT设备可选支持Web访问方式。若支持Web访问方式，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）应支持关闭HTTP服务；
- （4）应支持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。

7.3 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 设备可靠性要求

8.1 光纤保护倒换

PON设备可选支持光纤保护倒换功能，光纤保护倒换主要包括主干光纤保护倒换和全光纤保护倒换两种方式。

EPON设备应符合YD/T 1475-2006《接入网技术要求——基于以太网的无源光网络（EPON）》对光纤保护倒换功能的具体规定。

GPON设备应符合YD/T 1949.1-2009《接入网技术要求——吉比特的无源光网络（GPON）第1部分 总体要求》对光纤保护倒换功能的具体规定。

8.2 主控板主备倒换

OLT应提供主控板的热备份功能，在主控板倒换过程中，所有业务配置和业务连接不应发生差错或丢失，业务质量不应受到影响。

主控板倒换应支持人工倒换和自动倒换两种模式。

8.3 电源主备倒换

OLT应提供两路电源模块，在任何一路电源供电失效的情况下，设备应正常工作，业务质量不应受到影响。

8.4 环境监控

OLT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。

9 设备电气安全

9.1 绝缘电阻

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

9.2 设备接地要求

OLT和ONU设备的接地电阻应小于 5Ω 。

9.3 过压、过流保护

OLT和ONU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。

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

OLT和ONU设备的电磁兼容性指标应符合GB 9254-1998《信息技术设备的无线电骚扰限值和测量方法》以及GB/T 17618-1998《信息技术设备抗扰度限值和测量方法》的规定。