



中华人民共和国国家标准

GB/T 38798—2020

综合宽带接入网安全技术要求

Technical requirements for security of integrated broadband access network

2020-04-28 发布

2020-11-01 实施

国家市场监督管理总局
国家标准化管理委员会 发布

目 次

| | |
|----------------------------|----|
| 前言 | I |
| 引言 | II |
| 1 范围 | 1 |
| 2 规范性引用文件 | 1 |
| 3 缩略语 | 1 |
| 4 用户平面安全要求 | 2 |
| 4.1 帧过滤 | 2 |
| 4.2 组播/广播/DLF 报文风暴抑制 | 2 |
| 4.3 协议报文限速 | 2 |
| 4.4 MAC 地址控制功能 | 2 |
| 5 控制平面安全要求 | 2 |
| 5.1 设备认证 | 2 |
| 5.2 可控组播 | 2 |
| 5.3 过滤功能 | 3 |
| 5.4 防 DOS 攻击 | 3 |
| 5.5 ARP 代理功能 | 3 |
| 5.6 心跳机制 | 3 |
| 5.7 SIP 协议的注册认证功能 | 3 |
| 6 管理平面安全要求 | 3 |
| 6.1 管理员口令 | 3 |
| 6.2 设备访问方式 | 3 |
| 6.3 网管系统安全要求 | 4 |
| 7 设备可靠性要求 | 6 |
| 7.1 主控板主备倒换 | 6 |
| 7.2 电源主备倒换 | 6 |
| 7.3 环境监控 | 6 |
| 8 设备电气安全要求 | 6 |
| 8.1 绝缘电阻 | 6 |
| 8.2 接地电阻 | 6 |
| 8.3 过压、过流保护 | 6 |
| 8.4 电磁兼容 | 7 |

前 言

本标准按照 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由中华人民共和国工业和信息化部提出。

本标准由全国通信标准化技术委员会(SAC/TC 485)归口。

本标准起草单位:中国信息通信研究院。

本标准主要起草人:卓安生、刘谦、程强、陈洁。

引 言

为避免非法窃取网络资源、非法使用网络业务、恶意攻击,提高下一代网络设备的安全性可靠性,ITU-T 于 2003 年制定了 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,规定了应用层、业务层和基础设施层三个网络层次,并为每个网络层次定义了用户、控制和管理三个平面。每个层次的每个平面分别从访问控制、鉴别、不可抵赖、数据保密性、通信安全、完整性、可用性和隐私八个方面考虑其安全性。

近几年,随着互联网业务的发展和宽带接入网络向宽带化、综合化和软件化的发展,综合宽带接入网面临比过去单一业务单一网络更为复杂的安全环境,同时技术的升级换代也产生了更多的安全威胁和防御手段。因此制定宽带接入网安全标准势在必行。

参考 ITU-T X.805 的相关准则,并结合综合宽带接入网设备特点,本标准从用户、控制、管理等三个平面进行规定,每个平面分别从访问控制、鉴别、通信安全和可用性等几个方面定义其安全性。

综合宽带接入网安全技术要求

1 范围

本标准规定了综合宽带接入网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的综合宽带接入网设备,专用电信网中的综合宽带接入网设备也可参考使用。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/T 9254 信息技术设备的无线电骚扰限值和测量方法

GB/T 17618 信息技术设备 抗扰度 限值和测量方法

YD/T 1082 接入网设备过电压过电流防护及基本环境适应性技术要求和试验方法

3 缩略语

下列缩略语适用于本文件。

ACK:确认字符(Acknowledgement)

ACL:访问控制列表(Access Control List)

ARP:地址解析协议(Address Resolution Protocol)

DHCP:动态主机配置协议(Dynamic Host Config Protocol)

DLF:目的查找失败(Destination Lookup Failure)

DOS:拒绝服务(Denial of Service)

ICMP:因特网控制消息协议(Internet Control Message Protocol)

IGMP:互联网组管理协议(Internet Group Management Protocol)

IMS:互联网多媒体系统(IP Multimedia Subsystem)

MAC:媒体访问控制(Media Access Control)

NAK:无应答(Negative Acknowledgment)

RMS:远程管理服务器(Remote Management Server)

SIP:会话初始协议(Session Initiation Protocol)

SNMP:简单网络管理协议(Simple Network Management Protocol)

SSL:安全套件层(Secure Sockets Layer)

TCP:传输控制协议(Transmission Control Protocol)

TLS:安全传输层协议(Transport Layer Security)

UDP:用户数据报协议(User Datagram Protocol)

USM:基于用户的安全模型(User-based Security Model)

VLAN:虚拟局域网(Virtual Local Area Network)

VoIP: 互联网上的语音 (Voice over Internet Protocol)

4 用户平面安全要求

4.1 帧过滤

基于不同设备类型, 应支持根据物理端口、以太网封装协议、源/目的 MAC 地址、源/目的 IP 地址、以太网优先级标记和 TCP/UDP 端口号对上、下行以太网数据帧进行过滤。

4.2 组播/广播/DLF 报文风暴抑制

应支持对二层组播/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。

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。

4.3 协议报文限速

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

4.4 MAC 地址控制功能

应支持限制基于端口学习到的 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, 设备应支持忽略新 MAC 地址直到旧 MAC 地址老化。

5 控制平面安全要求

5.1 设备认证

应支持设备的合法性认证的能力, 应拒绝未通过认证的设备接入网络获得服务。

5.2 可控组播

应支持组播权限控制功能, 阻止非法用户获取组播业务。

5.3 过滤功能

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

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。

5.4 防 DOS 攻击

应支持防止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。

5.5 ARP 代理功能

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

5.6 心跳机制

提供 VoIP 业务的设备应支持定期向软交换/IMS 发送心跳消息, 并能正确响应软交换/IMS 发送的心跳消息。

5.7 SIP 协议的注册认证功能

对于采用 SIP 协议提供 VoIP 业务的设备,在向软交换/IMS 注册时,支持认证功能。

6 管理平面安全要求

6.1 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。

无论在设备还是网管系统中,口令不应使用明文保存。

6.2 设备访问方式

6.2.1 SNMP 访问

支持 SNMP 访问的设备应支持 SNMPv1 或 SNMPv2c,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。

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

6.2.2 本地 CONSOLE 访问

支持本地 CONSOLE 访问的设备应支持通过其所带的 CONSOLE 接口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。

6.2.3 Telnet 访问

支持 Telnet 访问的设备应支持以下安全要求:

- a) 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;
- b) 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;
- c) 应限制同时访问的用户数目;
- d) 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;
- e) 可限定用户通过哪些 IP 地址使用 Telnet 服务对设备进行访问;
- f) 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;
- g) 应支持关闭 Telnet 服务。

6.2.4 Web 访问

支持 Web 方式访问的设备应支持以下安全要求:

- a) 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;
- b) 可限定用户通过哪些 IP 地址使用 HTTP 对设备进行访问;
- c) 应支持关闭 HTTP 服务;
- d) 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。

6.2.5 TR-069 访问

支持 TR-069 方式访问的设备应支持以下安全要求：

- a) 终端设备与 RMS 接口应采用 SSL/TLS 加密和 WWW-Authentication 认证组合使用方式实现接口的安全；
- b) 在 SSL/TLS 安全通道建立过程中，RMS 不需要通过证书对终端设备的合法性进行认证。终端设备应支持基于证书和不基于证书的密钥交换认证方式对 RMS 进行合法性认证。

6.3 网管系统安全要求

6.3.1 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：

- a) 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；
- b) 提供管理用户的功能；
- c) 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；
- d) 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。

6.3.2 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：

- a) 增加、删除、修改角色；
- b) 给角色分配管理资源（可管理的对象范围）和操作权限；
- c) 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。

6.3.3 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：

- a) 增加账号；
- b) 删除账号；
- c) 修改账号信息；
- d) 查询账号信息。

管理用户的账号信息包括：

- a) 用户账号；
- b) 用户密码；
- c) 密码有效期；
- d) 用户所属角色；
- e) 附加说明。

支持同一个管理员账号属于多个角色组。

6.3.4 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：

- a) 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,则客户端应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；
- b) 登录的用户只具有已经被授权的指定操作；
- c) 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；
- d) 手工注销登录的用户；
- e) 手工或超时自动锁定客户端或退出。

6.3.5 在线用户管理

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：

- a) 登录用户；
- b) 登录时间；
- c) 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。

6.3.6 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：

- a) 给定时间或时间段进行查询；
- b) 给定用户进行查询；
- c) 给定的日志类型。

可以查询到的信息包括：

- a) 日志类型,包括操作日志、系统日志、安全日志；
- b) 操作时间；
- c) 操作人；
- d) 操作名称；
- e) 操作对象；
- f) 操作内容；
- g) 操作终端；
- h) 操作结果(例如,成功或失败)。



7 设备可靠性要求

7.1 主控板主备倒换

应支持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。

7.2 电源主备倒换

应支持两路电源模块,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。

7.3 环境监控

应支持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 设备电气安全要求

8.1 绝缘电阻

正常情况下,设备的绝缘电阻应不小于 50 M Ω 。

8.2 接地电阻

设备的接地电阻应小于 5 Ω 。

8.3 过压、过流保护

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 对模拟雷电冲击、电力线感应、电力线接触等指标的要求。

8.4 电磁兼容

设备的电磁兼容性指标应符合 GB/T 9254 以及 GB/T 17618 的规定。
