



# 中华人民共和国国家标准

GB/T 38799—2020

---

## 基于公用电信网的宽带客户网络设备 安全技术要求 宽带客户网关

Technical requirement for security of broadband customer network equipment  
based on public telecommunication network—Broadband customer gateway

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
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 安全管理功能 .....	2
4.2 访问控制列表 .....	2
4.3 VPN 功能 .....	3
4.4 NAT 功能 .....	3
4.5 防火墙功能 .....	3
4.6 防攻击功能 .....	4
4.7 网络访问的安全性 .....	4
4.8 WLAN 安全性 .....	4
5 控制平面安全要求 .....	4
5.1 PPP 用户认证 .....	4
5.2 日志功能 .....	5
6 管理平面安全要求 .....	5
6.1 Telnet 访问 .....	5
6.2 Web 管理 .....	5
6.3 连接认证功能 .....	5
7 可靠性要求 .....	6
8 电气安全要求 .....	6

## 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:沈天珺、程强。



# 基于公用电信网的宽带客户网络设备 安全技术要求 宽带客户网关

## 1 范围

本标准规定了基于公用电信网的宽带客户网络中宽带客户网关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。

本标准适用于基于公用电信网的宽带客户网络中的网关。

## 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。

YD/T 965 电信终端设备的安全要求和试验方法

IETF RFC 1918 互联网私有地址分配(Address allocation for private internets)

## 3 缩略语

下列缩略语适用于本文件。

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

BGP: 边界路由协议(Border Gateway Protocol)

CHAP: 质询握手认证协议(Challenge-Handshake Authentication Protocol)

DHCP: 动态主机控制协议(Dynamic Host Configuration Protocol)

DMZ: 隔离区(Demilitarized Zone)

DNS: 域名系统(Domain Name System)

DoS: 拒绝服务(Denial of Service)

EGP: 外部网关协议(External Gateway Protocol)

FTP: 文件传输协议(File Transfer Protocol)

HTTP: 超文本传输协议(Hypertext Transfer Protocol)

ICMP: 因特网控制报文协议(Internet Control Messages Protocol)

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

IGP: 内部路由协议(Interior Gateway Protocol)

IP: 互联网协议(Internet Protocol)

IPSec: IP 安全协议(IP Security Protocol)

L2TP: 二层隧道协议(Layer 2 Tunneling Protocol)

LAC: 链路接入控制(Link Access Control)

LAN: 局域网(Local Area Network)

LNS: L2TP 网络服务器(L2TP Network Server)

LSP: 标记交换路径(Label Switch Path)

MAC: 媒质接入控制层(Medium Access Control)

MD5:MD5 消息摘要算法(Message Digest 5 Algorithm)  
MPLS:多协议标签交换(Multiprotocol Label Switching)  
NAPT:网络地址端口转换(Network Address Port Translation)  
NAT:网址变换(Network Address Transform)  
PAP:密码认证协议>Password Authentication Protocol)  
PPP:点对点通信协议(Point to Point Protocol)  
PPPoE:以太网上点到点协议(Point-to-Point Protocol over Ethernet)  
RMS:远程管理服务器(Remote Management Server)  
SIP:会话初始协议(Session Initiation Protocol)  
SSID:服务集标识(service set identifier)  
SSL:安全套接层(Secure Sockets Layer Protocol)  
TCP:传输控制协议(Transmission Control Protocol)  
Telnet:终端网络(Terminal Network)  
TLS:传输层安全性(Transport Layer Security)  
TOS:服务类型(Type of Service)  
UDP:用户数据报协议(User Datagram Protocol)  
URL:统一资源定位器(Uniform Resource Locator)  
VLAN:虚拟局域网(Virtual Local Area Network)  
VPN:虚拟专用网(Virtual Private Network)  
VRF:VPN 路由转发表(VPN Routing and Forwarding)  
WLAN:无线局域网(Wireless Local Area Network)

## 4 用户平面安全要求

### 4.1 安全管理功能

#### 4.1.1 口令管理

宽带客户网关涉及的口令长度应不少于 8 个字符,并且应由数字、字母或特殊符号组成,宽带客户网关可提供检查机制,保证每个口令至少是由前述 3 类符号中的两类组成。

#### 4.1.2 用户管理

网关应具有普通用户及管理员用户。

普通用户管理权限可以对网关的一些非重要参数进行配置和查询,不能对网关的重要参数进行配置。

管理员本地维护管理权限可以对网关的重要参数进行配置和查询。

### 4.2 访问控制列表

应实现的访问控制列表。

应支持基于源 MAC 地址、源 IP 地址、目的 IP 地址、以太网协议类型、TCP/UDP 源端口号、TCP/UDP 目的端口号、TOS 域、IP 协议类型的访问控制列表。

### 4.3 VPN 功能

#### 4.3.1 L2TP 隧道

应支持通过 L2TP 隧道技术实现 VPN, 应支持 LAC 和 LNS 功能, 支持 CHAP 鉴别协议。

#### 4.3.2 IPSec 隧道(可选)

可选支持通过 IPSec 隧道技术实现 VPN。

#### 4.3.3 MPLS VPN(可选)

##### 4.3.3.1 通用要求

不管是 L2 VPN 还是 L3 VPN, 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, 一个 VPN 的数据不应进入到另一个 VPN。

当同时支持 VPN 服务和因特网服务时, 特别是在同一个物理接口上通过不同的逻辑接口支持 VPN 服务和因特网服务时, 可以基于逻辑接口对接入速率进行限制。

##### 4.3.3.2 L2 VPN

VPN 之间的 MAC 地址和 VLAN 信息应相互隔离, VPN 之间或 VPN 和 MPLS 骨干之间应可以复用 MAC 地址空间和 VLAN 空间。除非需要, VPN 之间或 VPN 和 MPLS 骨干之间的交换信息应相互隔离。

##### 4.3.3.3 L3 VPN

常用的 L3 VPN 技术是 BGP/MPLS VPN。BGP/MPLS VPN 实质上是通过 BGP 协议约束路由信息分配的 MPLS, 对 L3 VPN 的要求如下:

- 应支持静态路由算法和动态路由算法。对于动态路由算法, 应具有接口上过滤路由更新的能力, IGP 和 EGP 路由协议都应支持 MD5 加密认证, 并可基于 VRF 实例限制路由更新速度。
- VPN 之间的拓扑和编址信息应相互隔离, 一个 VPN 应可以使用所有因特网地址范围, 包括 IETF RFC 1918 定义的私有地址范围, VPN 之间或 VPN 和 MPLS 骨干之间应可以复用 IP 地址空间。
- 应为每个 VPN 维持一个独立的 VRF 实例, 除非需要, VPN 之间或 VPN 和 MPLS 骨干之间的路由信息及其分发和处理应相互独立, 互不干扰。

### 4.4 NAT 功能

宽带客户网关应支持 NAT 功能, 对 NAT 的功能特性要求如下:

- 应支持 NATPT;
- 应支持 HTTP、FTP、DNS、H.323、SIP 等应用协议;
- 应支持输出 NAT 日志记录。

### 4.5 防火墙功能

宽带客户网关应支持防火墙功能, 除包过滤、访问控制列表、NAT 外, 应支持应用代理功能, 只允许被保护的网路访问允许的网络应用。

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。

可选支持在本地 Web 界面配置防火墙的等级, 分为高、中、低三级。

状态检测不仅检查网络层和传输层的信息,还检查应用层协议的信息,实时维护这些 TCP 或 UDP 的状态信息。使用这些状态信息确定访问控制,应支持基于状态检测的包过滤功能。

## 4.6 防攻击功能

### 4.6.1 防 DoS 攻击功能

宽带客户网关应支持防止 Ping of Death、SYN Flood 等 DoS 攻击,并建议网关能够防止对自身代理的应用协议(例如,DNS)进行攻击。

### 4.6.2 防端口扫描能力

宽带客户网关应能够提供防端口扫描功能,支持防止其他设备或者应用的恶意端口扫描。

### 4.6.3 限制每端口 MAC 地址学习数量功能

宽带客户网关应能配置限制从每个用户 LAN 端口学习到的源 MAC 地址的数量。

### 4.6.4 非法组播源控制功能

宽带客户网关应支持防止用户做源的组播,可以配置禁止用户端口发出的 IGMP Query 和组播数据报文。

### 4.6.5 报文抑制

宽带客户网关应能够对特定协议的广播/组播包(例如,DHCP、ARP、ICMP、IGMP 等)进行速率抑制,并能对其他二层广播报文进行速率限制。

## 4.7 网络访问的安全性

宽带客户网关应支持 DMZ 功能。

宽带客户网关应支持基于 MAC 地址和 IP 地址进行接入控制(包括 LAN 和 WLAN)。

宽带客户网关应支持设置黑白名单实现 URL 访问控制功能。黑白名单应支持与网关发起的 PPPoE 账号绑定。

宽带客户网关应支持基于网关发起的 PPPoE 账号的上网时间管理。

## 4.8 WLAN 安全性

宽带客户网关应支持配置不同 SSID 以区分网络,支持启用或者关闭 SSID 广播功能,以及 SSID 隐藏的功能。还应支持对其 WLAN 无线信号的发送功率和工作信道的设定。应支持对 WLAN 客户端的认证和 WLAN 收发数据的加密。

## 5 控制平面安全要求

### 5.1 PPP 用户认证

PPP 作为数据链路层协议,本身不具备完善的安全能力。应支持 PAP 方式的用户接入认证。在通过 PPPoE 方式接入时,可以通过 PAP 方法进行用户认证。

应支持 CHAP 方式的用户接入认证。在通过 PPPoE 方式接入时,可以通过 CHAP 方法进行用户认证。

应支持基于运营商信息用户接入认证。在拨号过程中,网关从认证过程中提取运营商信息并基

于该信息确定是否进行后续的拨号流程。

可选支持基于 PPPoE 用户账号的用户接入认证的代理。即宽带客户网关收到用户终端的包含用户名和密码的 PPPoE 上网请求后,网关终结 PPPoE 请求,然后使用截获的用户名和密码向网络侧发起链接请求。由宽带客户网关给用户终端分配内部网络地址允许用户终端进行网络接入。如果宽带客户网关收到新的用户终端使用该用户名密码拨号,那么网关直接为用户终端分配内部网络地址,不再向网络侧发起新的连接,直接使用已有的连接上网。当存在多条不同账号的网络侧 PPPoE 连接时,对应的用户侧账号的连接应仅绑定在相应账号的网络侧连接上。

## 5.2 日志功能

对控制平面的信息要提供日志记录功能,网关应具有独立的防火墙日志,该防火墙日志记录该网络设备检测到的宽带客户网络中违背该防火墙规则的网络行为,每条记录应打上时间戳。防火墙日志应至少能够包含 100 条记录。如果产生的日志数量超过容量,宜采取保留最新的记录,覆盖时间最早的记录的方式。

防火墙日志应不能被修改。日志也不应被删除,除非被复位至出厂/默认配置。

日志应记录过滤规则、拒绝访问、配置修改等相关安全事件。对日志的要求包括:

- 每个安全日志条目应包含事件主体、发生时间和事件描述等;
- 应可以保存在本地系统的缓存区内,也可以发送到专用的日志主机上作进一步处理;
- 可选实时打印在专用打印机或连接设备的显示终端上;
- 应定义日志的严重级别,并能够根据严重程度级别过滤输出;
- 应支持和日志主机之间的接口。

## 6 管理平面安全要求

### 6.1 Telnet 访问

Telnet 协议用于通过网络设备进行远程登录。如果对用户提供 Telnet 服务,则建议满足下列规定:

- 用户应提供用户名/口令才能进行后续操作,用户地址和操作应计入日志;
- 应限制同时访问的用户数;
- 在设定的时间内不进行交互,用户应自动被注销;
- 可限定用户通过哪些 IP 地址使用 Telnet 服务对设备进行访问;
- 必要时可关闭 Telnet 服务。

### 6.2 Web 管理

Web 管理基于 HTTP 协议,宽带客户网关应支持 Web 管理,应满足下列约定:

- 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;
- 可限定用户通过哪些 IP 地址使用 HTTP 对设备进行访问;
- 必要时可关闭 HTTP 服务;
- 应支持 SSL/TLS。

### 6.3 连接认证功能

网关应具有一定的安全措施,保证 RMS 对网关远程管理和控制的安全性,避免对网关的非法配置。同时网关应具有一定的安全机制,如远程网管应都支持连接认证、支持修改管理认证账号、系统日志和安全日志、管理信息传输的安全机制等,保证远程管理的安全性。

## 7 可靠性要求

宽带客户网关应实现软件升级失败后可以自动回滚,关键配置不丢失,具有远程诊断及远程重启等功能。

## 8 电气安全要求

宽带客户网关应符合 YD/T 965 中关于电气安全的要求。

