ICS 33.040.50
M 19

中华人民共和国国家标准

GB/T 32403.2—2015

基于公用电信网的宽带客户网络设备技术要求 第2部分：企业用宽带客户网关

Technical requirements for equipments in broadband customer network based on telecommunication network—Part 2：Enterprise gateway

2015-12-31 发布　　2016-07-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

GB/T 32403《基于公用电信网的宽带客户网络设备技术要求》由两部分组成：

——第1部分：家庭用宽带客户网关；

——第2部分：企业用宽带客户网关。

本部分为GB/T 32403的第2部分。

本部分按照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。

本部分由工业和信息化部提出。

本部分由全国通信标准化技术委员会(SAC/TC 485)归口。

本部分起草单位：工业和信息化部电信研究院、华为技术有限公司、上海贝尔股份有限公司。

本部分主要起草人：程强、侯聪、葛坚、张钦亮、陈晓。

基于公用电信网的宽带客户网络设备技术要求 第2部分:企业用宽带客户网关

1 范围

GB/T 32403的本部分规定了基于公用电信网的宽带客户网络(以下简称宽带客户网络)中企业用宽带客户网关的设备分类、接口、设备功能、安全功能、操作管理维护要求、性能和环境要求、供电要求等。

本部分适用于基于公用电信网的宽带客户网络中的企业用宽带客户网关。

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。

GB/T 7611 数字网系列比特率电接口特性

GB/T 9951 信息技术 系统间远程通信和信息交换 34插针DTE/DCE接口连接器的配合性尺寸和接触件编号分配

GB 15629.11(所有部分) 信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求 第11部分:无线局域网媒体访问控制和物理层规范

YD/T 993 电信终端设备防雷技术要求及试验方法

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

YD/T 1475 接入网技术要求—基于以太网方式的无源光网络(EPON)

YD/T 1530 接入网技术要求—频谱扩展的第二代不对称数字用户线(ADSL2+)

YD/T 1814 基于公用电信网的宽带客户网络的远程管理 第1部分:总体

YD/T 1814.2 基于公用电信网的宽带客户网络远程管理 第2部分:协议

YD/T 1949.1 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 1965 基于公用电信网的宽带客户网络设备及其辅助设备的电磁兼容性要求和测量方法

YD/T 1996.1 接入网技术要求 第二代甚高速数字用户线(VDSL2) 第1部分:总体要求

YD/T 2278—2011 接入网设备测试方法 第二代甚高速数字用户线(VDSL2)

SJ/T 11363 电子信息产品中有毒有害物质的限量要求

ITU-T V.24 数据终端设备(DTE)和数据电路终接设备(DCE)之间的交换电路定义表[List of definitions for interchange circuits between data terminal equipment (DTE) and data circuit-terminating equipment (DCE)]

ITU-T V.35—1984 使用60-108 kHz群带电路速率为48 kbit/s的数据传输(Data transmission at 48 kbit/s using 60-108 kHz group band circuits)

IEEE 802.3 CSMA/CD访问方法和物理层规范[Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical]

IETF RFC 1157　简单网络管理协议[A Simple Network Management Protocol(SNMP)]

IETF RFC 1901　基于团体的 SNMPv2 的介绍(Introduction to Community-based SNMPv2)

IETF RFC 2663　IP 网络地址转换术语及思考[IP Network Address Translator (NAT) Terminology and Considerations]

IETF RFC 3022　传统 IP 网络地址转换[Traditional IP Network Address Translator (Traditional NAT)]

IETF RFC 3027　IP 网络地址转换的协议兼容性(Protocol Complications with the IP Network Address Translator)

IETF RFC 3489　NAT 的 UDP 简单穿越[STUN—Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)]

Broadband Forum TR-069 Amendment2　CPE WAN 管理协议(CPE WAN Management Protocol)

3　术语和定义

下列术语和定义适用于本文件。

3.1

IGMP/MLD 嗅探　IGMP/MLD snooping

通过在 IEEE 802.1 桥上侦听组播路由器或接收组播的主机发出的 IGMP/MLD 消息,达到优化组播流在二层网络上的分发的功能,包括但不限于:

——侦听通过桥转发的 IGMP/MLD 消息判定 IGMP/MLD 路由器和主机的端口位置;

——建立基于端口和 VLAN 的组播转发表;

——在非路由器端口维护基本 IGMP/MLD 成员关系状态。

3.2

IGMP/MLD 代理　IGMP/MLD proxy

该功能可被分解为 3 个子功能:

——报告抑制:截取和处理来自 IGMP/MLD 主机的 Report 报文,仅在必要的时候才向上行转发,例如当组播组中第一个用户加入时;对于每个组播组的 IGMP/MLD Query 报文仅响应一次。

——离开抑制:截取和处理来自 IGMP/MLD 主机的 Leave 报文,仅在必要的时候才向上行转发,例如当组播组中最后一个用户离开时。

——查询抑制:截取和处理 IGMP/MLD Query 报文。

当实现以上功能时,功能实体可能转发 IGMP/MLD 主机和组播路由器发出的报文,也可能自己产生 IGMP/MLD 报文。

3.3

ping 攻击　ping of death attack

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。

3.4

SYN 洪泛攻击　SYN flood attack

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。

4　缩略语

下列缩略语适用于本文件。

3G:第三代无线通信系统(third generation wireless systems)
ADSL:不对称数字用户线(a symmetric digital subscriber line)
ADSL2+:频谱扩展的第二代不对称数字用户线(a symmetric digital subscriber line 2 plus)
ALG:应用层网关(application layer gateway)
ARP:地址解析协议(address resolution rrotocol)
AP:接入点(access point)
ATM:异步传输模式(asynchronous transfer mode)
BRAS:宽带远程接入服务器(broadband remote access server)
CAR:承诺接入速率(committed access rate)
CBR:恒定比特率(constant bit rate)
DDNS:动态域名系统(dynamic domain name system)
DHCP:动态主机配置协议(dynamic host configure protocol)
DMZ:隔离区(de-militarized zone)
DNS:域名系统(domain name system)
DoS:拒绝服务(denial of service)
DPI:深度包检测(deep packet inspection)
DSCP:差分服务代码点(differentiated services code point)
DSL:数字用户线(digital subscriber line)
DSLAM:DSL 接入复用器(DSL access multiplexer)
EPON:以太网无源光网络(ethernet passive optical networks)
FTP:文件传输协议(file transfer protocol)
GPON:吉比特无源光网络(gigabit-capable passive optical networks)
HTTP:超文本传输协议(hypertext transfer protocol)
HTTPS:安全超文本传输协议(hypertext transfer protocol secure)
IGMP:互联网组管理协议(internet group management protocol)
IP:互联网协议(internet protocol)
IPSec:互联网安全协议(internet protocol security)
L2TP:2 层隧道协议(layer 2 tunneling protocol)
LAN:局域网(local area network)
MAC:媒质访问控制(medium access control)
MCS:调制编码方案(modulation coding scheme)
MDI:媒质相关接口(media dependent interface)
MDIX:交叉的媒质相关接口(media dependent interface with crossover)
MLD: 组播侦听者发现(multicast listener discovery)
NAPT:网络地址端口转换(network address port translation)
NAT:网络地址转换(network address translation)
ND:邻居发现(neighbor discovery)
nrt-VBR:非实时的可变比特率(业务)(non-real-time VBR)
NTP:网络时间协议(network time protocol)
PON:无源光网络(passive optical network)
PPPoE:以太网承载点对点协议(point-to-point protocol over ethernet)
PVC:永久虚连接(permanent virtual connection)
QoS:服务质量(quality of service)

RIP:路由信息协议(routing information protocol)
RMS:远程管理服务器(remote management server)
rt-VBR:实时的可变比特率(业务)(real-time VBR)
SIP:会话初始化协议(session initiation protocol)
SNMP:简单网络管理协议(simple network management protocol)
SSH:安全外壳协议(secure shell)
SSID:服务集标识符(service set identifier)
SSL:安全套接层(secure socket layer)
STB:机顶盒(set-top box)
TCP:传输控制协议(transmission control protocol)
TDM:时分复用(time division multiplexing)
TELNET:终端网络(terminal network)
TFTP:简单文件传输协议(trivial file transfer protocol)
TLS:传输层安全(transport layer security)
UBR:未规定比特率(业务)(unspecified bit rate)
UDP:用户数据报协议(user datagram protocol)
URL:统一资源定位符(uniform resource locator)
USB:通用串行总线(universal serial bus)
USIM:通用用户识别模块(universal subscriber identity module)
VBR:可变比特率(variable bit rate)
VDSL2:第二代甚高速数字用户线(very high speed digital subscriber line 2)
VID:VLAN 标记(VLAN identifier)
VLAN:虚拟局域网(virtual local area network)
VoIP:在 IP 上传送语音(voice over IP)
VPN:虚拟专用网络(virtual private network)
WAN:广域网(wide area network)
WEP:有线等效加密(wired equivalent privacy)
WLAN:无线局域网(wireless local area network)
WMM:Wi-Fi 多媒体(Wi-Fi multimedia)
WRPQ:加权随机早期检测(weighted random parly detection)
WRR:加权循环调度(weighted round robin)

5 企业用宽带客户网关的设备概述

5.1 网关在宽带客户网络中的位置

企业用宽带客户网关在宽带客户网络中的位置如图 1 所示。网关可以通过各种接口直接与接入网相连。网关可以直接与企业用户终端设备或适配设备相连,也可以直接与企业的局域网相连。

如无特别说明,以下出现的网关均指企业用宽带客户网关。

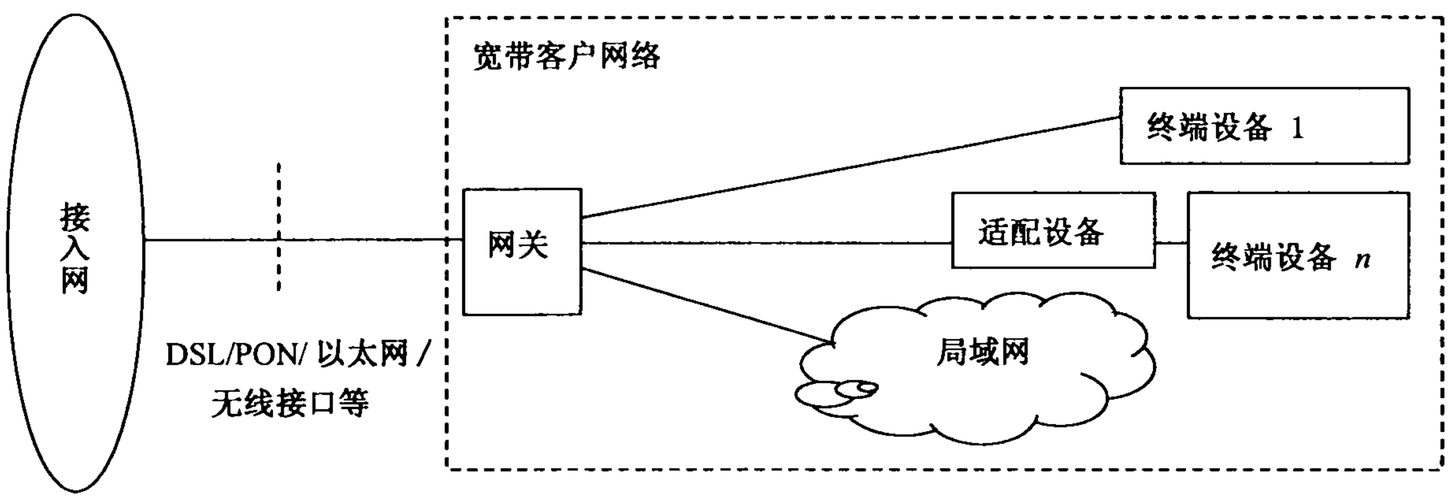

图 1　网关在宽带客户网络中的位置图

5.2　网关的功能参考模型

图 2 为网关功能模块划分示意图，包括 5 个方面的功能模块：

——接入功能；

——联网功能；

——传送功能；

——核心功能；

——业务功能。

其中业务功能模块是可选的，其他功能模块是必选的。

网关的接入功能主要实现宽带客户网络与公用电信网络(以下简称电信网络)的连接。

网关的联网功能主要实现网关与宽带客户网络内部的用户终端设备及宽带客户网络内部的用户终端设备之间的连接。

网关的传送功能主要实现宽带客户网络内部设备与电信网络之间 IP 包等的传送。

网关的核心功能包括：

——地址功能，主要实现网关自身 IP 地址获得以及支持宽带客户网络内部终端获得 IP 地址；

——QoS 功能，主要实现多业务流的分级处理及转发，用于保证服务质量；

——安全功能，主要防止外部网络对宽带客户网络的非法访问以及内部网络的非法接入；

——远程管理功能，主要实现运营商对网关的远程管理与控制；

——本地管理功能，主要实现网关功能的本地管理与控制。

网关的业务功能：主要实现网关上电信业务的适配和终接。

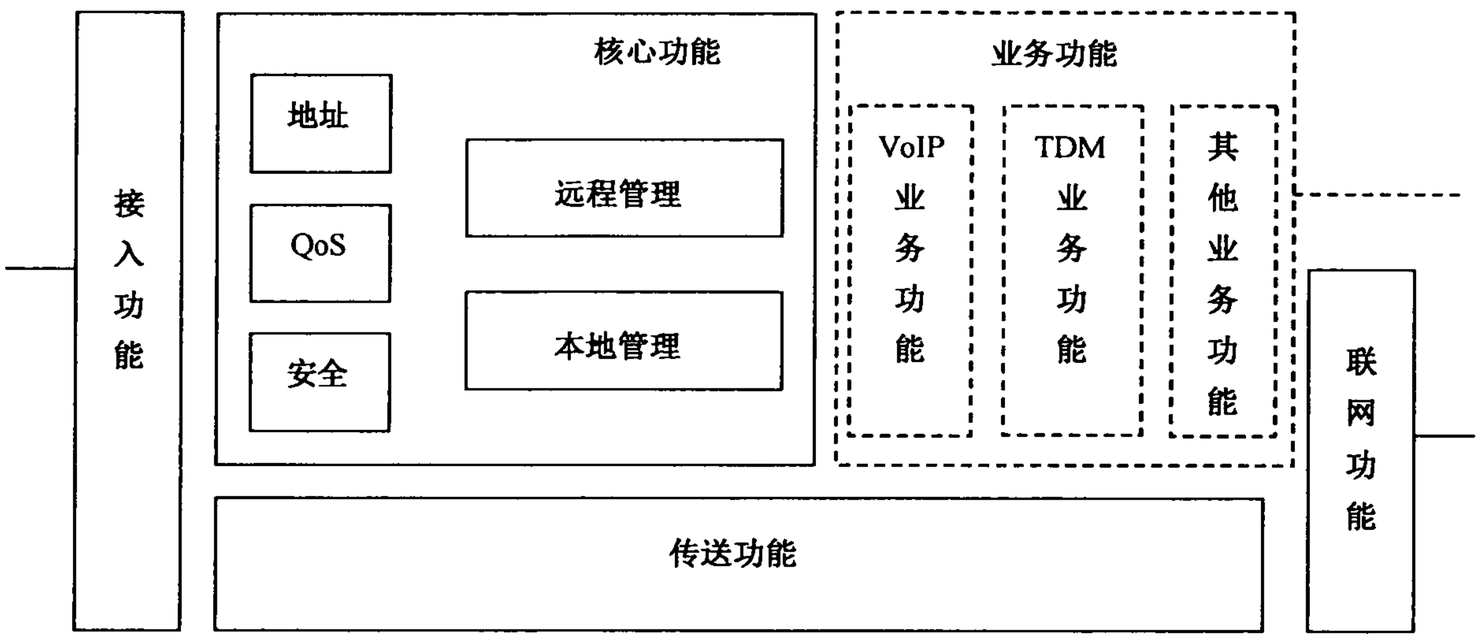

图 2　网关功能框图

6 接口要求

6.1 用户侧接口

6.1.1 100/1000 BASE-T 接口

网关的用户侧接口应至少提供 4 路以太网 100BASE-T 接口，以及至少 1 路 1000BASE-T 接口。100/1000BASE-T 接口应符合 IEEE 802.3 相关要求，建议支持自适应连接网线的功能(Auto MDI/MDIX)。

6.1.2 WLAN AP 接口

网关的用户侧接口可选提供 WLAN AP 接口。

WLAN AP 接口应支持 GB 15629.11 系列标准定义的 2.4 GHz 物理层规范，可选支持 5.8 GHz 物理层。

6.1.3 USB 接口

网关的用户侧接口可选提供 USB 接口。USB 接口应满足 USB 2.0，应支持 USB 主(Master)模式，应支持全速 Full Speed(12 Mbit/s)方式，可选支持高速 Hi-Speed(480 Mbit/s)方式。

6.1.4 Z 接口

网关的用户侧接口可选提供 Z 接口。

6.1.5 2048 kbit/s 电接口(E1 接口)

当提供 TDM 专线业务时，网关应支持 2048 kbit/s 电接口(E1 接口)，接口应符合 GB/T 7611 的规定。

6.1.6 V.24/V.35 接口

网关可选支持 V.24 或 V.35 接口。

V.24 接口应符合 ITU-T V.24 的规定。

V.35 接口物理特性应符合 ITU-T V.35—1984 10.1 和 GB/T 9951 的规定。

6.2 网络侧接口

网关应至少支持下列接口之一作为网络侧接口，接入宽带网络为用户提供服务：

——ADSL2+接口；

——VDSL2 接口；

——以太网(10/100/1000 BASE-T)接口；

——EPON 接口；

——GPON 接口；

——3G 等无线接口。

ADSL2+接口应符合 YD/T 1530 的规定。

VDSL2 接口应符合 YD/T 1996.1 的规定。

10/100/1000 BASE-T 接口应符合 IEEE 802.3 相关要求。

EPON 接口应符合 YD/T 1475 的规定。

GPON 接口应符合 YD/T 1949.1 的规定。

3G 等无线接口根据具体选择的技术应符合相应技术规范的接口要求。

6.3 USIM 卡接口

对于采用 3G 等无线接口作为网络侧接口的网关，应支持 USIM 卡接口。

7 设备功能

7.1 联网功能

7.1.1 用户接口联网功能

网关应支持客户网络内部各个有线和/或无线终端之间相互访问，数据流无需通过 WAN 连接。网关应支持终端对网关的访问。

7.1.2 WLAN AP 功能(可选)

网关应支持通过硬件开关开启或关闭 WLAN AP 功能。

网关的 WLAN AP 功能应支持多 SSID，至少支持 4 个虚拟 AP，每个虚拟 AP 具有独立的配置功能，包括对 SSID、发送队列、加密方式等参数的配置。支持各 SSID 与物理或虚拟 WAN 接口(例如：VLAN、PVC)的绑定关系。

网关的 WLAN AP 功能应支持自动速率调节，IEEE 802.11 中 b 模式下速率调节范围为 11 Mbit/s、5.5 Mbit/s、2 Mbit/s 和 1 Mbit/s，IEEE 802.11 中 g 模式下速率调节范围为 54 Mbit/s、48 Mbit/s、36 Mbit/s、24 Mbit/s、18 Mbit/s、12 Mbit/s、9 Mbit/s 和 6 Mbit/s。IEEE 802.11 中 n 模式下应支持工作在 20 MHz 或 40 MHz 信道带宽下，应支持 IEEE 802.11 中 n 模式中规定的各种 MCS。

网关的 WLAN AP 功能应支持手动或自动信道选择。

网关的 WLAN AP 功能应能支持终端在节电模式下工作，并能识别终端进入节电状态。

网关的 WLAN AP 功能可选支持发射功率可配置。

7.2 接入功能

网关应至少支持 6.2 规定的网络侧接口之一。

网关应支持作为客户端建立 PPPoE、L2TP、IPSec VPN 隧道等连接的功能。

网关应支持 IPv4/IPv6 的双栈接入的能力。在桥接方式下支持 IPv6 报文的透传。在路由方式下支持以太网承载 IPv6 和 PPP 承载 IPv6 两种接入方式。

网关可选支持 DHCP 中继功能，能够将终端的 DHCP 请求转发给位于宽带客户网络外部的 DHCP 服务器，并返回地址分配结果。

7.3 传送功能

7.3.1 设备工作模式

网关应支持工作在桥接、路由或桥接/路由混合模式，在各种模式下，客户网络内的各个终端之间应能相互访问，各个终端应能对网关访问。

7.3.2 VLAN 功能

网关应支持接收无 VLAN 标记、携带优先级标记(VID=0)或 VLAN 标记的报文。

网关应支持对上行无 VLAN 标记报文添加 p-bit 和/或 VID，对优先级标记的报文添加 VID，支持

丢弃携带 VLAN 标记的报文。

网关应支持将下行接收到的 VLAN 标记的报文去掉 VLAN 标记。

网关应支持 1∶1 的 VLAN 转换功能。

网关应支持透明以太网专线业务(TLS)端口,透传用户无 VLAN 标记、携带优先级标记(VID=0)或 VLAN 标记的以太网报文。

网关应支持用户侧以太网端口或不同的 WLAN SSID 划分到不同的 VLAN。

7.3.3 组播支持功能

网关应支持 IGMP/MLD 代理和 IGMP/MLD 嗅探功能,IGMP 协议支持 IGMP v2,可选支持 IGMP v3。MLD 协议应支持 MLD v1,可选支持 MLD v2。

网关应支持跨 VLAN 组播功能,将组播 VLAN 中的下行组播流传送到用户侧单播 VLAN 端口。

7.3.4 路由功能

网关应支持静态路由配置,可选支持 RIP v1/v2 协议。

7.4 地址功能

7.4.1 DNS 功能

网关应支持在 DHCP 会话过程中将 DNS 服务器地址发送给客户网络内部设备,DNS 服务器的地址可以配置,并能对客户网络内部设备的 DNS 请求进行转发并将解析结果送回给客户网络内部设备。

网关应支持 DDNS 功能。

网关应支持 DNSv6。

7.4.2 NAT 功能

网关应支持 NAT/NAPT 功能,符合 IETF RFC 2663、IETF RFC 3022 和 IETF RFC 3027 规范。

网关应支持 IETF RFC 3489 定义的锥形网络地址翻译(cone NAT)。

网关应支持远程或本地配置端口前转(Port Forwarding),支持虚拟服务器(Virtual Server),用户可选择常见协议(如 FTP、HTTP 等)进行虚拟服务器配置,网关应至少同时支持 8 个虚拟服务器的配置。

7.4.3 ALG 功能

支持 ALG 功能,支持 SIP、FTP、RTSP、L2TP、H.323 等协议的私网穿越功能,支持 IPSec 协议;每种协议必须提供单独的开关功能。

7.4.4 DHCP 功能

网关的 WAN 侧应支持静态配置 IP 地址、DHCP 和 PPPoE 3 种方式获取 IP 地址信息。

网关 WAN 侧接口应支持 DHCP 客户端功能,能够从网络侧接口获取 IP 地址信息,包括 IP 地址、DNS 服务器地址、IP 网关地址等。

网关 LAN 侧接口应支持 DHCP 服务器功能,为用户侧设备分配 IP 地址,IP 地址池可配置。网关的 DHCP 服务器应支持查看地址池中已分配的地址情况,包括客户端名称、MAC 地址、IP 地址、剩余租借期等。DHCP 服务器功能应可配置打开或关闭。

网关的 DHCP 服务器应支持根据用户侧设备上报的 Option 60 标识,为不同类型的设备从同一网段不同的 IP 地址区间中分配 IP 地址,不同设备 IP 地址池可配置。

7.4.5 IPv6 地址功能

网关中的 3 层功能应支持 IPv6 协议族。包括支持 SLAAC、DHCP-PD 和 PPP 承载 IPv6 时的各种地址获取方式；支持对 LAN 侧设备的 IPv6 地址的分配。

7.5 QoS 功能

7.5.1 业务流分类和标记功能

流分类技术是指采用一定的规则识别符合某类特征的报文，它是有区别地进行服务的前提和基础。

网关应支持外部网络要求的 QoS 机制，例如：

——ATM 的 QoS 机制；

——以太网的 QoS 机制；

——IP 的 QoS 机制。

网关应支持以下流分类技术：

a) 应支持按源 IP(包括网段和范围)、目的 IP(包括网段和范围)、源端口、目的端口、物理接口(包括 SSID)进行流分类；

b) 应支持按源 MAC 地址、目地 MAC 地址、VLAN ID、IEEE 802.1D 优先级进行流分类；

c) 应支持按 DSCP 进行流分类；

d) 应支持按协议类型(TCP/UDP/ICMP)进行流分类；

e) 可选支持通过识别业务报文，对动态业务进行流分类。例如通过识别 SIP 报文，提取呼叫语音流的 IP 地址/UDP 端口号信息，并施加已经配置的流分类策略；

f) 可选支持按 ToS/traffic class 域进行流分类。

网关应支持根据外部网络采用的 QoS 机制的不同，对流分类的结果进行标记或重标记：

如果外部网络采用 ATM 的 QoS 机制，网关可选支持流分类结果与 PVC 的映射；PVC 支持 UBR、CBR、rt-VBR、nrt-VBR 业务类型，并提供 PVC 业务类型配置查询功能；

如果外部网络采用以太网的 QoS 机制，网关应支持流分类结果与 802.1D 优先级的映射；

如果外部网络采用 IP 的 QoS 机制，网关应支持流分类结果与 IPv4 报文 ToS、DSCP 域的映射，以及与 IPv6 报文的流量类(traffic class)域的映射。

7.5.2 业务流限速功能

网关应支持对业务进行流量控制，包括每种上行业务流的 CAR、LAN-WLAN 的 CAR。应支持 CAR 规则的本地配置和远程配置。

7.5.3 优先级队列调度功能

网关应支持至少 4 个优先级队列，并能根据流分类的结果将业务流映射到不同的队列，应支持绝对优先级队列调度、应至少支持 WRR、WRED 等加权队列调度方式之一，应支持绝对优先级和加权优先级的混合调度。

7.5.4 WLAN QoS 功能

网关具有 WLAN AP 功能时，应支持 WMM。支持数据流与 WMM 队列的映射，支持 WMM 定义的 4 种流类型及其优先级调度规则，支持基于优先级的数据处理和转发。支持为不同的 SSID 分配不同的优先级。

7.6 USB 功能(可选)

USB 接口可以用于提供 USB 共享打印、USB 共享存储、额外的上联接口卡的连接等功能。

7.7 以太网环路检测功能

应支持检测并处理以下两类用户侧以太网成环情况:

a) 检测设备不同 LAN/WLAN 端口之间成环,并断开成环端口中的一个;

b) 检测设备同一个 LAN 口之下的网络成环,并断开成环端口。

应支持通过网管远程配置该功能的开启或关闭。当开启并发生成环事件时,网关应产生相应的告警信息。

8 安全功能

8.1 防攻击功能

8.1.1 防 DoS 攻击能力

网关应支持防止 ping 攻击、SYN 洪泛等 DoS 攻击。建议网关能够防止对自身代理的应用协议(例如,DNS)的攻击。

8.1.2 防端口扫描能力

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。

8.1.3 限制每端口 MAC 地址学习数量功能

网关应能限制从每个用户端口以及 WAN 口学习到的源 MAC 地址的数量。

8.1.4 防火墙功能

网关应支持防火墙功能,支持对防火墙等级的设置,支持对防火墙规则的配置,并支持基于以下规则对报文进行过滤:

——支持根据源 MAC 地址、目的 MAC 地址进行报文过滤;

——支持根据源 IP 地址及范围段、目的 IP 地址及范围段进行报文过滤;

——支持根据 TCP/UDP 源端口及范围段、目的端口及范围段进行报文过滤;

——支持根据以太网包的传输层协议类型进行报文过滤,要求有 IP/PPPoE/ARP/ND 的选项;

——支持根据 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;

——支持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。

8.1.5 病毒扫描功能(可选)

企业网关可选具有对企业用户互联网业务流量的病毒过滤功能,支持 HTTP、SMTP、POP3、FTP 等协议,支持病毒代码库/防病毒引擎定期的自动更新。

8.1.6 入侵检测功能(可选)

网关可选具有入侵检测功能,对流入和流出的流量进行扫描和特征匹配。网关应可以阻止检测到

的入侵行为，并记入日志。

8.1.7 非法组播源控制功能

网关设备建议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 查询和组播数据报文。

8.1.8 报文速率抑制

网关建议能够对特定协议的广播/组播包(例如 DHCP，ARP/ND，IGMP/MLD 等)进行速率抑制，并能对其他两层广播报文进行速率限制。

8.2 网络访问的安全性

网关应支持 DMZ 和 DMZ 主机功能。

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)。

网关应支持设置黑白名单实现 URL 访问控制功能。黑白名单应支持与账号绑定。可选支持基于账号进行上网时间管理。

网关应支持对企业内部用户上网行为的控制策略设置，可以基于 MAC 地址、主机名、时间/日期等策略进行配置。建议支持基于组的权限设置。

网关可选支持 DPI 功能，通过配置对特定的网络应用程序进行阻止或流量限制。

8.3 设备访问安全性

8.3.1 服务访问控制

网关应支持对访问自身的 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 HTTP/FTP/TELNET/SNMP/SSH。缺省情况下不允许通过 WAN 侧访问网关设备本身进行设备数据配置(TR-069 协议除外)。

8.3.2 黑白名单

对网关的访问控制规则可以以黑名单或者白名单方式生效。

8.4 WLAN 安全性

如果支持 WLAN AP 接口，网关设备必须支持配置不同 SSID 以区分网络，支持启用或者关闭 SSID 广播功能。SSID 可以隐藏。

网关应支持开放系统(Open System)和共享密钥(Shared Key)两种认证方式。

网关设备应支持的加密机制按国家有关规定执行。

可选支持 WPS，如果用户使用 WPS Push Button 方式接入，则按照 WPS 规范协商加密算法和密钥。每个 SSID 下都维护一张许可接入的设备列表，为已经过 WPS 验证的接入设备列表。列表内的设备允许随时接入，非列表内的设备经过 WPS 验证成功后加入至列表中；许可接入列表可在网关查询。

9 操作管理维护

9.1 管理方式

9.1.1 概述

企业网关所有参数(各类用户名/密码配置等私密信息除外)的配置和查询都应同时支持本地管理

和远程管理两种方式。

9.1.2 远程管理功能

网关应支持 RMS 通过 TR-069 对其进行远程管理，可选作为代理支持通过 TR-069 协议对宽带客户网络内部设备进行远程管理。网关可选支持 SNMP 方式进行管理。

网关应支持通过 PPPoE 或 DHCP 方式获得独立的管理 IP 地址。

当网络侧接口为 ADSL2＋接口时，管理通道应支持采用独立的 PVC 通道；当网络侧接口为 VDSL2、以太网、GPON 或 EPON 接口时，管理通道应支持采用独立的 VLAN。

TR-069 远程管理功能、协议应符合 YD/T 1814 和 YD/T 1814.2 的规定。

SNMP 协议应支持 SNMPv1 和 SNMPv2c。SNMPv1 见 IETF RFC 1157。SNMPv2c 见 IETF RFC 1901。

网关设备可选支持通过 IPv6 承载要求的管理协议。

9.1.3 本地管理功能

网关应支持通过 HTTPS 方式进行本地管理，可选支持 TELNET 方式。

本地管理方式应支持两级用户账号管理模式，即普通用户账号和管理维护账号。普通用户账号只具备网关联网的基本配置和设备查询能力；管理维护账号具备网关完整的配置和管理能力，并且能够查询普通账号的用户名，修改普通账号信息。

网关应支持登录空闲超时自动退出，连续输入错误密码应能锁定，锁定时间至少 1 min。

网关应支持本地进行恢复出厂配置操作。

9.2 日志功能

网关应提供记录日志，包括系统日志、访问日志、防火墙日志、告警记录等，能够记录网关设备的登录记录、管理配置操作，以及记录宽带客户网络外部和内部间违反预先设定的规则或策略的访问（如非法攻击，对某些互联网站点的访问等），并提供查询、清空日志记录功能。日志文件建议为文本文件格式。

日志文件断电应不丢失。

网关应支持 NTP 协议，并为日志记录带上时间戳。

日志应可通过远程管理或本地管理功能获取和操作。

9.3 故障管理功能

网关应具有实时告警上报功能。上报的告警消息种类和级别等应可配置。告警消息同时应在网关本地进行保存。TR-069 协议中具体的告警上报机制待定。

建议网关至少支持下列告警消息：

a) 严重告警：

——端口不可用；

——文件服务器不可达；

——文件服务器用户名/密码错误；

——下载文件超时；

——服务器上无指定文件；

——软件升级失败；

——闪存空间不足。

b) 主要告警：

——CPU 使用率过高；

——日志空间受限。

c) 次要告警：

——设备重启；

——管理员登录连续错误次数超过最大值。

9.4 软件升级功能

网关中的系统和应用软件应可通过网管系统进行升级。升级软件时应具有容错校验功能，如果升级失败，应能恢复到原来的软件版本。

远程升级操作应允许运营商定义设备的保留参数，这些参数在经历升级操作后不应被清除。

9.5 配置的保存和恢复

网关应允许管理员用户对系统的配置进行保存下载、上传恢复等功能。

9.6 恢复出厂配置操作

在通过远程、本地进行恢复出厂配置操作，应允许运营商定义设备的保留参数，这些参数在经历恢复出厂设置后不应被清除。

10 性能要求

10.1 WAN 侧性能

10.1.1 ADSL2＋传输性能

当网关工作在 ADSL2＋线路模式下时，物理层传输性能应符合 YD/T 1530 的要求。

10.1.2 VDSL2 传输性能

当网关工作在 VDSL2 线路模式下时，物理层传输性能应符合 YD/T 2278—2011 的要求。

10.1.3 EPON 接口性能

应符合 YD/T 1475 的要求。

10.1.4 GPON 接口性能

应符合 YD/T 1949.1 的要求。

10.1.5 以太网业务性能

具体要求待定。

10.1.6 VoIP 业务性能

应符合 YD/T 1188—2008 中 8.5 的要求。

10.1.7 MAC 地址表深度

网关应支持不小于 4 000 个 MAC 地址转发表项。

10.1.8 静态路由条目数

建议网关支持不小于 128 条静态路由表项。

10.1.9 NAPT 并发连接数

建议网关在开启 NAPT 功能时支持的最大并发 TCP 连接数不小于 1 000 条。

10.2 LAN 侧性能

10.2.1 以太网接口

用户侧以太网接口间应达到无阻塞交换。

10.2.2 WLAN 性能

对于 IEEE 802.11 中 b 模式下，理想环境下最大吞吐量不小于 5.5 Mbit/s。

对于 IEEE 802.11 中 g 模式下，理想环境下最大吞吐量不小于 20 Mbit/s。

对于 IEEE 802.11 中 n 模式，在 20 MHz 信道 2 空间流最大吞吐量不小于 70 Mbit/s。

对于 IEEE 802.11 中 n 模式，在 40 MHz 信道 2 空间流最大吞吐量不小于 140 Mbit/s。

10.3 设备吞吐量

对于 ADSL2+、VDSL2 和 3G 等无线方式上行的网关，吞吐量不应小于上联接口的最大连接速率能力。

对于以太网接口和 EPON/GPON 上行的网关，吞吐量待定。

网关在开启 IPSec、L2TP 等 VPN 加密连接时，吞吐量不应低于无加密时的 75%。

11 其他要求

11.1 环境要求

网关在以下室内环境中应能正常工作：

——工作温度：0 ℃～40 ℃；

——工作湿度：5%～95%无凝结；

——大气压力：86 kPa～106 kPa。

11.2 供电要求

网关(或其电源适配器)应支持本地交流供电方式，输入交流电压及其波动范围要求为：单相 100 V～240 V，频率 50 Hz，频率变化范围为 5%，线电压波形畸变率小于 5%。设备在此范围内应正常工作。

建议企业网关提供双路电源接口，支持电源的保护倒换。

11.3 过压、过流保护

网关应内置过压、过流保护器件。过压、过流保护器件在外接电源异常时保护设备的核心部分。

网关应满足 YD/T 993 规定的要求，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传输性能要求。

11.4 电磁兼容

网关应满足 YD/T 1965 中的相关要求。

11.5 环保要求

网关应满足 SJ/T 11363 中的相关要求。

网关应采用低能耗设计方案。

中华人民共和国
国家标准
基于公用电信网的宽带客户网络设备技术要求
第2部分：企业用宽带客户网关
GB/T 32403.2—2015
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室：(010)68533533　发行中心：(010)51780238
读者服务部：(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230　1/16　印张 1.5　字数 34 千字
2016年2月第一版　2016年2月第一次印刷
*
书号：155066·1-53058　定价　24.00 元

GB/T 32403.2-2015