



中华人民共和国国家标准

GB/T 38797—2020

基于公用电信网的宽带客户网络设备 安全测试方法 宽带客户网关

Test method 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 发布
国家标准化管理委员会

目 次

前言 III

1 范围 1

2 规范性引用文件 1

3 缩略语 1

4 用户平面安全测试 2

 4.1 安全管理 2

 4.2 访问控制列表 3

 4.3 VPN 功能 4

 4.4 NAT 功能 4

 4.5 防火墙功能 4

 4.6 防攻击功能 5

 4.7 网络访问的安全性 7

 4.8 WLAN 安全性 9

5 控制平面安全测试 11

 5.1 鉴别和认证 11

 5.2 日志功能 11

6 管理平面安全测试 11

 6.1 测试目的 11

 6.2 测试配置 11

 6.3 测试步骤 11

 6.4 预期结果 12

7 可靠性测试 12

 7.1 升级功能 12

 7.2 远程重启功能 12

 7.3 远程诊断功能 13

8 电气安全测试 13

 8.1 电源测试 13

 8.2 过压、过流保护测试 13

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 安全测试方法 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的用户平面安全、控制平面安全、管理平面安全、设备可靠性和电气安全的测试方法。

本标准适用于基于公用电信网的宽带客户网络中的宽带客户网关。

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。

YD/T 1055—2005 接入网设备测试方法——不对称数字用户线(ADSL)

YD/T 1082—2011 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

YD/T 1440—2006 路由器设备安全测试方法——中低端路由器(基于 IPv4)

3 缩略语

下列缩略语适用于本文件。

AP:无线接入节点(Access Point)

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

BRAS:宽带接入服务器(Broadband Remote Access Server)

DMZ:隔离区(Demilitarized Zone)

DoS:拒绝服务(Denial of Service)

FTP:文件传输协议(File Transfer Protocol)

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

HTTPS:安全超文本传输协议(Hypertext Transfer Protocol Security)

INTERNET:因特网(Interconnected Network)

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

IP:互联网协议(Internet Protocol)

MAC:媒质接入控制层(Medium Access Control)

NAT:网址变换(Network Address Transform)

PC:个人计算机(Personal Computer)

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)

SSID:服务集标识(Service Set Identifier)

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

TFTP:简单文件传输协议(Trivial File Transfer Protocol)

UDP:用户数据报协议(User Datagram Protocol)

URL:统一资源定位器(Uniform Resource Locator)

VPN:虚拟专用网(Virtual Private Network)

WEP:有线等效加密(Wired Equivalent Privacy)

WLAN:无线局域网(Wireless Local Area Network)

WPA-PSK:Wi-Fi 保护接入-预共享密钥(Wi-Fi Protected Access-Pre-Shared Key)

4 用户平面安全测试

4.1 安全管理

4.1.1 设备登录安全性测试

4.1.1.1 测试目的

用户进行网络管理时需要使用登陆口令,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,设备可选提供检查机制,保证每个口令至少是由前述的三类符号中的两类组成。

应支持空闲超时自动退出,连续输入错误密码应能锁定。

4.1.1.2 测试配置

测试配置见图 1。



图 1 设备配置安全性测试配置

4.1.1.3 测试步骤

测试步骤如下:

- 按照图 1 进行连接;
- 在 PC 上登录设备;
- 修改本地设备的配置账号的密码;
- 等待一段空闲时间后在设备配置界面上进行操作;
- 注销登录后再次访问网关配置界面,并连续输入错误密码。

4.1.1.4 预期结果

步骤 b)中,需要输入密码才能登陆设备,所输入的密码符合安全性要求。

步骤 c)中,设置新密码时,能够对密码的安全性进行检查并提示。

步骤 d)中,空闲超时后,试图再次对网关配置界面进行操作时会提示超时,此时无法进行配置,需要重新登录。

步骤 e)中,连续输入错误密码后,登录界面会锁定。

4.1.2 普通用户账号测试

4.1.2.1 测试目的

普通用户账号具备联网的基本配置和设备查询能力,可配置的参数待定,并且能够修改本账号的密码。

4.1.2.2 测试配置

测试配置见图 1。

4.1.2.3 测试步骤

测试步骤如下：

- a) 按照图 1 进行连接；
- b) 在 PC 上以普通用户账号登录设备,查看可以查询和配置的内容；
- c) 修改密码后退出登录；
- d) 用新密码登录网关,再次查看本地配置界面。

4.1.2.4 预期结果

步骤 b)中,普通用户账号登录后可以查看到当前设备运行的基本状态,可以进行部分参数的配置,无法配置不在权限范围内的参数。

步骤 c)中,可以对普通用户账号的密码进行修改,修改时需校验当前密码。

步骤 d)中,新的密码可正常登录。

4.1.3 管理员用户账号测试

4.1.3.1 测试目的

管理员用户账号可对网关全部参数进行配置,并可修改普通用户账号的用户名和密码。

4.1.3.2 测试配置

测试配置见图 1。

4.1.3.3 测试步骤

测试步骤如下：

- a) 按照图 1 进行连接；
- b) 在 PC 上以管理员用户账号登录设备,查看可以查询和配置的内容；
- c) 修改密码后退出登录；
- d) 用新密码登录网关,再次查看本地配置界面；
- e) 查看当前普通用户账号的密码,并对其进行修改；
- f) 退出登陆后,用旧的普通用户账号重新登陆；
- g) 用新的普通用户账号进行登录。

4.1.3.4 预期结果

步骤 b)中,管理员用户账号登录后可以对设备参数进行完整的查询和配置。

步骤 d)中,新的密码可正常登录。

步骤 e)中,管理员用户账号可对普通用户账号进行修改。

步骤 f)中,旧的普通用户账号无法登录。

步骤 g)中,新的普通用户账号能够正常登录。

4.2 访问控制列表

访问控制列表功能的测试内容见 YD/T 1440—2006 中 5.4 的规定。

4.3 VPN 功能

VPN 功能的测试内容见 YD/T 1440—2006 中 6.3 的规定。

4.4 NAT 功能

NAT 功能的测试内容见 YD/T 1440—2006 中 5.5 的规定。

4.5 防火墙功能

4.5.1 测试目的

网关应支持防火墙功能,支持对防火墙等级的设置,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协议类型进行报文过滤；
- 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 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 2 种,默认为禁止模式。

4.5.2 测试配置

测试配置见图 2。

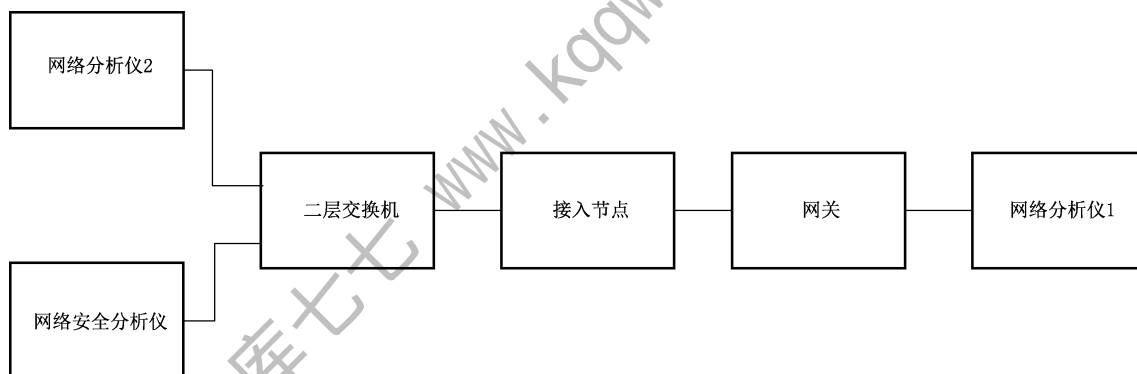


图 2 防火墙功能测试配置

4.5.3 测试步骤

测试步骤如下:

- 按照图 2 进行连接,在 Web 界面上配置网关防火墙等级;
- 配置网关根据目的端口进行报文过滤,并从网络分析仪端口 2 发送目的端口为指定端口的报文,观察网络分析仪端口 1 收到的报文;
- 分别配置网关根据源/目的 MAC 地址、源/目的 IP 地址、源/目的 TCP/UDP 端口、以太网协议类型、以太网包的传输层协议类型进行报文过滤,并从网络分析仪端口 2 发送特定报文,观察协议分析仪端口 1 收到的报文。

4.5.4 预期结果

步骤 a) Web 界面上可配置防火牆的等級,分为高、中、低三级。

步骤 c) 网络分析仪端口 1 收到的报文应符合所配置的防火墙规则。

4.6 防攻击功能

4.6.1 防 DoS 攻击功能

4.6.1.1 测试目的

设备应能够提供防 DoS 攻击功能。

4.6.1.2 测试配置

测试配置见图 2。

4.6.1.3 测试步骤

测试步骤如下：

- a) 按照图 2 进行连接；
- b) 配置网络分析仪 1 和网络分析仪 2 互发广播和以一定速率的单播以太网帧；
- c) 配置网络安全分析仪以网关网络侧地址为目标进行 DoS 攻击测试，如发送大流量 ping 报文；
- d) 停止 DoS 攻击。

4.6.1.4 预期结果

步骤 c) 中，网络分析仪 1 和网络分析仪 2 之间的正常单播以太网数据流不应中断。

步骤 d) 中，网络分析仪 1 和网络分析仪 2 之间的正常单播以太网数据流正常转发，无丢包。

4.6.2 防端口扫描能力

4.6.2.1 测试目的

网关应能够提供防端口扫描功能，支持防其他设备或者应用的恶意端口扫描。

4.6.2.2 测试配置

测试配置见图 3。



图 3 防端口扫描测试配置

4.6.2.3 测试步骤

测试步骤如下：

- a) 按照图 3 进行连接，开启网关的防端口扫描功能，网关上关闭除常用服务端口外的其他端口；
- b) 在测试 PC 上使用端口扫描软件对网关的 WAN 侧 IP 进行扫描；
- c) 在测试 PC 上进行抓包，分析收到的报文。

4.6.2.4 预期结果

未开启的端口应无响应，已开启的端口应能识别非法报文，并在识别后不进行响应。

4.6.3 限制每端口 MAC 地址学习数量功能

4.6.3.1 测试目的

网关应能限制从每个用户端口学习到的源 MAC 地址数量。

4.6.3.2 测试配置

测试配置见图 4。

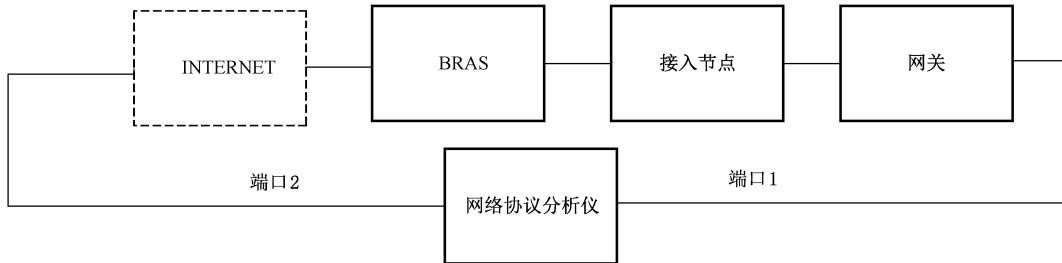


图 4 MAC 地址学习数量限制测试配置

4.6.3.3 测试步骤

测试步骤如下：

- 按照图 4 进行连接,限制网关端口学习到的源 MAC 数量为 n ;
- 网络协议分析仪端口 1 发送源 MAC 地址不同的 $n+1$ 条数据流;
- 分析网络协议分析仪端口 2 收到的数据流。

4.6.3.4 预期结果

步骤 c) 中,协议分析仪 2 收到的数据流应为 n 条。

4.6.4 非法组播源控制功能

4.6.4.1 测试目的

网关应防止用户做源的组播。可以禁止用户端口发出的 IGMP Query 和组播数据报文。

4.6.4.2 测试配置

测试配置见图 4。

4.6.4.3 测试步骤

测试步骤如下：

- 按照图 4 进行连接,在网络协议分析仪端口 2 配置组播客户端 IP 地址及组播上行端口,增加节目 P1 和网络协议分析仪端口 1;
- 在网络协议分析仪端口 2 抓包,用网络协议分析仪端口 1 点播节目 P1;
- 在网络协议分析仪端口 2 抓包,网络协议分析仪端口 1 停止点播;
- 在网络协议分析仪端口 2 抓包,网络协议分析仪端口 1 发送 IGMP Query 报文;

- e) 在网络协议分析仪端口 2 抓包,网络协议分析仪端口 1 发送组地址与 P1 组地址相同的组播数据报文。

4.6.4.4 预期结果

步骤 b)中网络协议分析仪端口 1 可正常收到节目 P1 的流,网络协议分析仪端口 2 可抓到组播加入报文。

步骤 c)中网络协议分析仪端口 1 不再正常收到节目 P1 的流,网络协议分析仪端口 2 可抓到组播离开报文。

步骤 d)中网络协议分析仪端口 2 没有抓到网络协议分析仪 1 发出的报文。

步骤 e)中网络协议分析仪端口 2 没有抓到网络协议分析仪 1 发出的报文。

4.6.5 报文抑制

4.6.5.1 测试目的



网关应能对特定协议的广播/多播包(例如,DHCP、ARP、IGMP 等)进行抑制,并能对其他二层广播报文进行速率限制。

4.6.5.2 测试配置

测试配置见图 4。

4.6.5.3 测试步骤

测试步骤如下:

- a) 按照图 4 进行连接,配置网关对用户端口的 DHCP、ARP、IGMP 报文的抑制功能,关闭接入节点上的抑制功能;
- b) 网络协议分析仪端口 1 上发送一定速率的 DHCP、ARP、IGMP 报文;
- c) 分析网络协议分析仪端口 2 收到的报文。

4.6.5.4 预期结果

步骤 c)中,网络协议分析仪 2 收到一定量的 DHCP、ARP、IGMP 报文,速率应符合抑制后的报文速率。

4.7 网络访问的安全性

4.7.1 DMZ 功能

4.7.1.1 测试目的

网关应支持 DMZ 功能。

4.7.1.2 测试配置

测试配置见图 5。

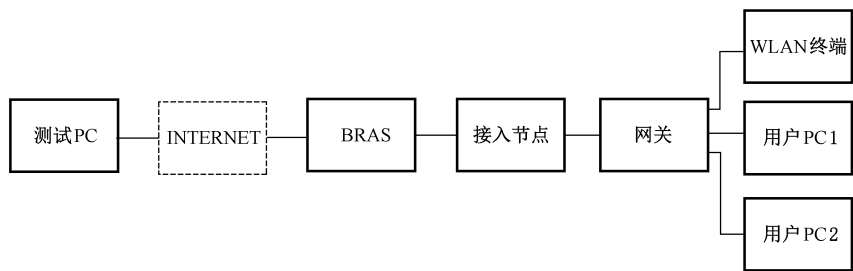


图 5 DMZ 功能测试配置

4.7.1.3 测试步骤

测试步骤如下：

- a) 按照图 5 进行连接,开启网关的 DMZ 功能,并指定为 PC1；
- b) 在 PC1 上开启 HTTP 和 FTP 服务；
- c) 在测试 PC 上用网关 IP 地址连接 HTTP 和 FTP 服务。

4.7.1.4 预期结果

步骤 c)中,测试 PC 连接网关 IP 地址,能够访问到 PC1 上的 HTTP 和 FTP 服务。



4.7.2 基于 MAC 地址的接入控制功能

4.7.2.1 测试目的

网关应支持基于 MAC 地址的接入控制,可以配置接入控制的 MAC 地址。

4.7.2.2 测试配置

测试配置见图 5。

4.7.2.3 测试步骤

测试步骤如下：

- a) 按照图 5 进行连接,开启网关的 MAC 地址接入控制功能；
- b) 配置禁止接入的 WLAN 终端和用户 PC 的 MAC 地址；
- c) WLAN 终端和用户 PC 访问网络。

4.7.2.4 预期结果

步骤 c)中,被禁止的终端无法连接网络。

4.7.3 基于 IP 地址的接入控制功能

4.7.3.1 测试目的

网关应支持 IP 地址接入控制功能,可以配置接入控制的 IP 地址。

4.7.3.2 测试配置

测试配置见图 5。

4.7.3.3 测试步骤

测试步骤如下：

- a) 按照图 5 进行连接,开启网关的 IP 地址接入控制功能；
- b) 禁止 PC1 的 IP 地址,允许 PC2 的 IP 地址；
- c) PC1 和 PC2 访问网络。

4.7.3.4 预期结果

步骤 c)中,PC1 无法访问,PC2 可以访问。

4.7.4 URL 访问控制功能

4.7.4.1 测试目的

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。

4.7.4.2 测试配置

测试配置见图 5。

4.7.4.3 测试步骤

测试步骤如下：

- a) 按照图 5 进行连接；
- b) 配置网关的 URL 控制功能,设定黑白名单功能,并根据名单内的 URL 进行访问。

4.7.4.4 预期结果

步骤 b)中,访问结果应符合对 URL 访问控制功能的配置。

4.8 WLAN 安全性

4.8.1 SSID 广播/隐藏功能测试

4.8.1.1 测试目的

网关应支持配置不同的 SSID 以区分网络,支持启用或者关闭 SSID 广播功能,SSID 可以隐藏。

4.8.1.2 测试配置

测试配置见图 6。

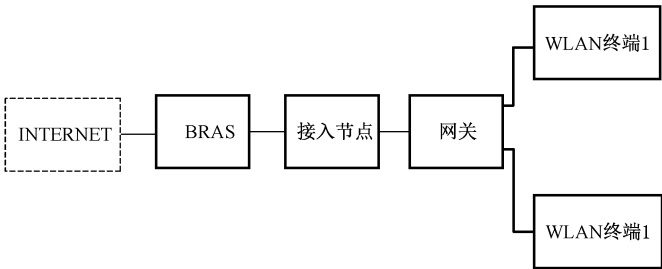


图 6 WLAN 安全性测试配置

4.8.1.3 测试步骤

测试步骤如下：

- a) 按照图 6 进行连接,开启网关的 WLAN 功能；
- b) 网关上配置 2 个不同的 SSID,WLAN 终端 1 和终端 2 分别连接每个 SSID；
- c) 关闭 SSID 广播功能,查看 SSID 是否隐藏。

4.8.1.4 预期结果

步骤 b)中,WLAN 终端 1 和终端 2 可正常接入网络。

步骤 c)中,WLAN 终端的无线网络列表中看不到 SSID,但通过手动配置可连接到网关。

4.8.2 MAC 层认证功能测试

4.8.2.1 测试目的

网关应支持 Open System 和 Shared Key 两种认证方式。

4.8.2.2 测试配置

测试配置见图 6。

4.8.2.3 测试步骤

测试步骤如下：

- a) 按照图 6 进行连接,开启网关的 WLAN 功能,配置 WEP 加密功能；
- b) 分别启用 Open System 和 Shared Key 两种认证方式；
- c) 设置 WLAN 接入终端的各参数,分别采用 Open System 和 Shared Key 两种认证方式；
- d) WLAN 终端接入公网。

4.8.2.4 预期结果

步骤 d)中,WLAN 终端可正常接入网络。

4.8.3 WPA-PSK、WPA2-PSK 加密功能测试

4.8.3.1 测试目的

验证网关 WLAN 加密功能。

4.8.3.2 测试配置

测试配置见图 6。

4.8.3.3 测试步骤

测试步骤如下：

- a) 按照图 6 进行连接,开启网关的 WLAN 功能,正确配置加密参数；
- b) WLAN 终端正确配置相应的加密方式和密钥,观察与 AP 连接情况。

4.8.3.4 预期结果

步骤 b)中,WLAN 终端可以连接到 AP,能够访问公网。

5 控制平面安全测试

5.1 鉴别和认证

鉴别和认证的测试内容见 YD/T 1440—2006 中 6.1 的规定。

5.2 日志功能

5.2.1 测试目的

日志应记录过滤规则、拒绝访问、配置修改等相关安全事件。网关应提供防火墙日志,记录所有违背防火墙规则的操作,每个条目应打上时间戳,日志应至少包括 100 条以上条目。

5.2.2 测试配置

测试配置见图 1。

5.2.3 测试步骤

测试步骤如下:

- a) 按照图 1 进行连接;
- b) 在 PC 上以 Web 方式登录网关配置界面,对网关进行一些配置,多次配置,使日志条目大于 100 条;
- c) 查看网关日志记录。

5.2.4 预期结果

步骤 c) 中,日志应至少包含最新 100 条记录,记录中包含用户账户登录和配置的记录,且能看到防火墙日志。

6 管理平面安全测试

6.1 测试目的

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,如远程网管都应支持连接认证、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。

6.2 测试配置

测试配置见图 7。

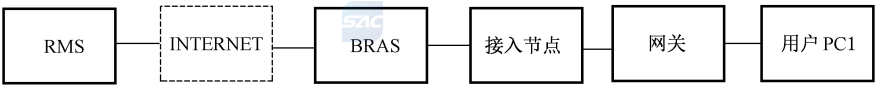


图 7 连接认证功能测试配置

6.3 测试步骤

测试步骤如下:

- a) 按图 7 进行连接；
- b) 在网关上配置错误的连接认证信息，重启网关后观察网关与 RMS 的连接情况；
- c) 在网关上配置正确的连接认证信息，重启网关后观察网关与 RMS 的连接情况。

6.4 预期结果

步骤 b) 中，网关无法与 RMS 建立连接。

步骤 c) 中，网关应能成功与 RMS 建立连接。

7 可靠性测试

7.1 升级功能

7.1.1 测试目的

网关应将当前的软件和固件版本上报给 RMS，并在需要时可以由 RMS 启动对网关软件和固件远程升级。升级后将升级是否成功的结果反馈给运营商。

传输协议应支持 HTTP 或 HTTPS 或 FTP 或 TFTP。

升级应支持安全校验。

7.1.2 测试配置

测试配置见图 7。

7.1.3 测试步骤

测试步骤如下：

- a) 按照图 7 进行连接，网关与 RMS 的连接正常；
- b) 通过 RMS 查看网关当前软件版本；
- c) 在 RMS 上对网关的软件进行远程升级，等待升级过程完成；
- d) 通过 RMS 查看网关当前软件版本。

7.1.4 预期结果

步骤 c) 中，网关应能正确响应远程升级指令，并在升级后上报是否成功。

步骤 d) 中，网关的软件版本应为升级后的版本。

7.2 远程重启功能

7.2.1 测试目的

网关应支持 RMS 对其进行远程重启。

7.2.2 测试配置

测试配置见图 7。

7.2.3 测试步骤

测试步骤如下：

- a) 按照图 7 进行连接，网关与 RMS 的连接正常；
- b) 在 RMS 上对网关下发重启命令。

7.2.4 预期结果

步骤 b)中,网关应在正确响应远程重启命令后重新启动。

7.3 远程诊断功能

7.3.1 测试目的

网关应支持 RMS 远程进行链路连接诊断。

7.3.2 测试配置

测试配置见图 7。

7.3.3 测试步骤

测试步骤如下:

- a) 按照图 7 进行连接,网关与 RMS 的连接正常;
- b) 在 RMS 上发起链路连接诊断;
- c) 查看网关相关参数。

7.3.4 预期结果

步骤 c)中,应能看到链路诊断结果。

8 电气安全测试

8.1 电源测试

电源测试的内容见 YD/T 1055—2005 中第 12 章的规定。

8.2 过压、过流保护测试

过压、过流保护测试的内容见 YD/T 1082—2011 中第 6 章的规定。