ICS 33.040.99
M 19

YD

中华人民共和国通信行业标准

YD/T 2095-2010

基于公用电信网的宽带客户网络安全技术要求

Security technical requirements for broadband customer network based on telecommunication network

2010-12-29 发布　　2011-01-01 实施

中华人民共和国工业和信息化部　发布

目　次

前　言

本标准是“基于公用电信网的宽带客户网络”系列标准之一。该系列标准的结构和名称预计如下。

1. 基于公用电信网的宽带客户网络总体技术要求。
2. 基于公用电信网的宽带客户网络服务质量（QoS）技术要求。
3. 基于公用电信网的宽带客户网络安全技术要求。
4. 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；
   第2部分：协议；
   第3部分：协议互通技术要求；
   第4部分：协议互通测试方法；
   第5部分：网关配置参数；
   第6部分：IP电话适配设备配置参数；
   第7部分：IPTV业务适配设备配置参数。
5. 基于公用电信网的宽带客户网络联网技术要求：
   第1部分：电力线（PLC）联网；
   第2部分：同轴电缆联网。
6. 基于公用电信网的宽带客户网络编址技术要求。
7. 基于公用电信网的宽带客户网络环境保护要求。
8. 基于公用电信网的宽带客户网络设备技术要求：
   第1部分：网关；
   第21部分：适配设备 IP电话业务；
   第22部分：适配设备 IPTV业务；
   第31部分：用户终端设备 无线IP电话；
   第32部分：用户终端设备 有线IP电话。
9. 基于公用电信网的宽带客户网络电磁兼容要求。
10. 基于公用电信网的宽带客户网络数字版权技术要求。
11. 基于公用电信网的宽带客户网络业务媒体格式技术要求。

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、武汉邮电科学研究院、中国电信集团公司、中兴通讯股份有限公司、上海贝尔股份有限公司、华为技术有限公司。

本标准主要起草人：程　强、敖　立、桑梓勤、王　波、阳彦字、鲁林丽、张钦亮。

基于公用电信网的宽带客户网络安全技术要求

1 范围

本标准规定了基于公用电信网的宽带客户网络的安全威胁、安全需求、安全机制和安全算法、设备认证证书轮廓以及安全功能。

本标准适用于电信网络提供的业务和应用通过网关在宽带客户网络内部实现的情况，对仅在宽带客户网络内部设备之间信息流通的情况也可参考使用。

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。

YD/T 1448-2006	基于公用电信网的宽带客户网络总体技术要求
ITU-T X.509	信息技术——开放系统互连——号码簿：公钥和属性鉴别框架
ITU-T X.805	提供端到端通信的系统的安全体系
ITU-T X.1121	移动端到端数据通信的安全技术框架
Broadband FORUM TR-069 Amendment 1（2006）	CPE WAN管理协议

3 术语与定义

下列术语和定义适用于本标准。

3.1

授权证书 Authorization Certificate

用于为对象授权的一个签名物。它至少包括一个发放者和一个对象。它可以包括有效性条件、授权和委托信息。通常，证书可以分为3类：身份证书、属性证书和授权证书。身份证书用于映射对象的名字和公钥，属性证书用于映射对象的名字和授权，授权证书用于映射对象的授权和公钥。获得一个授权证书或属性证书可以代表对象从发放者获得所有或部分权限。

3.2

身份证书 ID Certificate

一段信息，其中至少声明了授权发放者名称、证书对象身份、该对象公钥、证书有效期、序号和认证中心的数字签名。

3.3

设备证书 Device Certificate

身份证书的一种，在宽带客户网络中，它是一个符合ITU-T X.509版本3的证书，用于认证宽带客户网络设备。它可以由宽带客户网络内部CA发放，也可由外部CA发放。

3.4

加盐 Salt

在已执行哈希运算的密码中插入一个随机数字。这一策略有助于阻止潜在的攻击者利用预先计算的字典进行攻击。

3.5

Smurf攻击 Smurf Attack

一种拒绝服务攻击的方法，通过伪装成受害主机的源IP地址发送目的地址为广播地址的Ping包，利用大量的Ping响应攻击受害者。

3.6

LAND攻击 LAND Attack

一种拒绝服务攻击的方法，通过向受害主机发送源和目的地址相同设为受害主机地址的IP报文，导致受害主机连续地向自身发送响应报文。

4 缩略语

下列缩略语适用于本标准。

ACL	Access Control List	访问控制列表
AP	Access Point	接入点
ARP	Address Resolution Protocol	地址解析协议
CA	Certificate Authority	证书机构
CHAP	Challenge Handshake Authentication Protocol	质询握手认证协议
DoS	Denial of Service	拒绝服务
DMZ	DeMilitarized Zone	隔离区
EUTE	End User Terminal Entity	用户终端功能实体
FPE	Functional Processing Entity	功能处理实体
FTP	File Transfer Protocol	文件传输协议
HTTP	Hypertext Transfer Protocol	超文本传送协议
HTTPS	Hypertext Transfer Protocol Secure	超文本安全传送协议
ICMP	Internet Control Message Protocol	互联网控制消息协议
IGMP	Internet Group Management Protocol	互联网组管理协议
IP	Internet Protocol	互联网协议
IPoE	IP over Ethernet	以太网承载IP
IPTV	IP Television	IP电视
LAN	Local Area Network	局域网
MAC	Media Access Control	媒质访问控制
MGCP	Media Gateway Control Protocol	媒体网关控制协议
NAE	Network Access Entity	网络接入实体
NCE	Network Core Entity	网络核心功能实体
SIP	Session Initiation Protocol	会话初始化协议

SNMP	Simple Network Management Protocol	简单网络管理协议
PAP	Password Authentication Protocol	密码认证协议
PPP	Point to Point Protocal	点到点协议
PPPoE	PPP over Ethernet	以太网承载 PPP
PPPoA	PPP over ATM	ATM 承载 PPP
QoS	Quality of Service	服务质量
RBAC	Role-based Access Control	基于角色的访问控制
SIP	Session Initiation Protocol	会话初始协议
SSH	Secure Shell Protocol	安全壳协议
SSID	Service Set identifier	服务集标识
SSL	Secure Socket Layer	安全套接字层
TCP	Transmission Control Protocol	传输控制协议
TLS	Transport Level Security	传送层安全
UDP	User Datagram Protocol	用户数据报协议
WAN	Wide Area Network	广域网
WLAN	Wireless Local Area Network	无线局域网

5 宽带客户网络的安全概述

5.1 宽带客户网络的参考模型

YD/T 1448-2006给出了基于公用电信网的宽带客户网络的参考模型，如图1所示。

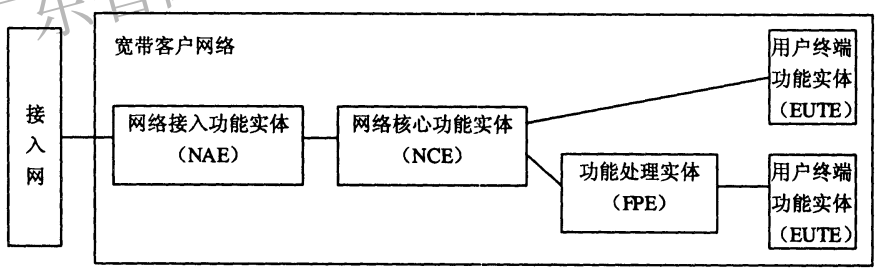

图 1 宽带客户网络参考模型

在图1中，NAE为宽带客户网络提供接入功能；NCE负责完成宽带客户网络的核心功能，包括：宽带客户网络内部设备的联网、远程管理、QoS、安全等；FPE负责IP/非IP的转换，以及信令、媒体格式的转换；EUTE由用户直接使用，提供UI界面。

5.2 宽带客户网络安全的特点

宽带客户网络位于网络的末端，混合了有线和无线联网技术，并且直接给用户提供使用界面，具有独特的安全特点：

— 使用各种不同的传输媒质；

— 混合有线和无线的联网技术；

— 不同的客户有不同的应用场景和安全要求；

— 用户可能随身携带终端；

— 宽带客户网络设备多种多样，安全能力各不相同。

6 宽带客户网络面临的安全威胁

6.1 概述

宽带客户网络可以由有线联网和无线联网或其混合组成，因此宽带客户网络面临的安全威胁包括了有线网络和无线网络，宽带客户网络的安全威胁可以分为两类：通用的安全威胁和移动环境的安全威胁。

6.2 通用安全威胁

6.2.1 窃听/泄露

在开放的网络环境下最易遭遇的安全问题是通过窃听进行匿名攻击。窃听攻击者可以主动地截获传输的数据，从而导致信息的泄露。

6.2.2 通信阻断/通信拥塞

当一个通信链路上的需要收发的数据量通过有意或无意的方式超过了链路容量，可以有效地使该链路失效。例如DoS攻击可以产生该威胁。

6.2.3 数据修改/注入

当未授权的通信实体为了劫持数据连接或恶意发送数据而对传输的数据进行插入、修改或删除时产生该威胁。其中未授权的实体可以是人员、程序或计算机等设备。例如DoS攻击或中间人（man-in-the-middle）攻击可以产生该威胁。

6.2.4 未授权访问

访问控制是限制和控制通过通信链路对业务/服务的访问的能力。当非法的实体通过仿冒合法用户获得对业务/服务的访问权时产生该威胁。试图进行未授权访问的实体应被鉴别或认证。例如，暴露的WAN口的网关管理接口容易受到非授权访问威胁。

6.2.5 抵赖

当发送者或接收者否认曾经发送或接收某消息的事实时产生该威胁。

6.2.6 数据包错误转发

该威胁是数据流中的数据包并未向预定的端点转发或被预定端点收取。例如在家庭网关中的路由表的配置错误可导致该威胁。

6.3 移动环境的安全威胁

6.3.1 窃听/泄露

在移动通信环境中，由于无线信号传输的开放性，截获发送的信号并解码其中的数据更加容易。例如，宽带客户网络内未经加密传输的WLAN数据有可能被窃听。

6.3.2 通信阻断/通信拥塞

对于使用无线传输技术的网络，该威胁更易实施。该威胁有两种不同的方式：拥塞终端设备和拥塞网元设备。通过前者可以仿冒和干扰合法的无线终端，通过后者可以仿冒和干扰带有无线接口的网元设备，阻断正常的通信。例如WLAN的AP会受到此种威胁。

6.3.3 移动终端丢失

由于移动终端被用户四处携带，丢失终端将导致存储其中的信息的泄露或损失。

6.3.4 通信意外中断

由于移动终端有限的电源供应或通信环境不稳定，该威胁可能造成数据丢失。

7 宽带客户网络的安全需求

7.1 概述

考虑到宽带客户网络混合了有线和无线网络技术，宽带客户网络中的安全需求与ITU-T X.1121中描述的安全需求类似。另外，加入了ITU-T X.805中对通信流安全的要求。

7.2 宽带客户网络安全需求

7.2.1 数据保密性

数据保密性是保护数据防范未经授权的泄露。数据保密性应确保数据内容无法被未授权的实体读取。加密、访问控制和文件权限都是用来提供数据保密性的常用方法。

7.2.2 数据完整性

数据完整性应确保数据的正确性和精确性。数据应可以防范未授权的修改、删除、创建和复制，并可以提供这些未授权活动的指示。

7.2.3 认证

认证过程是指鉴别用户身份与其所声称的是否一致或是确保消息的来源与其宣称的发送者是否一致。有两种不同的认证：

— 实体认证

— 消息认证

实体认证确保实体身份的有效性，消息认证确保消息来源的有效性。实体认证用于证实参与通信的实体的身份，消息认证证实参与通信的实体所声明的身份（例如，个人、设备、服务或应用）并且提供手段防止实体试图假冒或非法重放过去的通信过程。认证可以通过使用ID证书和宽带客户网络设备证书实现。

7.2.4 访问控制或授权

访问控制防止未授权的使用网络资源。访问控制应保证只有获授权的个人或设备才可访问网络、存储的信息、信息流、业务或应用。另外，基于角色的访问控制可提供不同的访问级别来精细化个人或设备被授权可以访问的内容和执行的操作。

有3种不同的授权方式：

— 使用 ACL 授权；

— 使用认证服务器授权；

— 使用授权证书或属性证书和身份证书。

访问控制或授权可以通过使用授权证书和ACL完成。在宽带客户网络的入口点的访问控制和授权可以通过宽带客户网络网关中的防火墙实现。防火墙的主要目的是阻止来自公众网络的未授权的访问。防火墙常用于阻止未授权的互联网用户访问连接到互联网的私有网络，例如，内联网（Intranet）。所有进出内联网的消息都要经过防火墙，阻止那些不符合特定的安全准则或安全策略的消息。

7.2.5 不可抵赖性

不可抵赖性通过各种网络相关的活动的证据，用于防止个人或实体否认曾经对数据进行过特定的操作。这些证据包括委托或许诺的证据、数据来源的证据、拥有权的证据、资源使用的证据等。不可抵赖性提供的证据可以提供给第三方用于证明某个事件或行为曾经发生过。

7.2.6 通信流安全

通信流安全确保信息流仅在授权的通信端点间流动。在宽带客户网络环境下通信流安全应通过宽带客户网络网关实现。

7.2.7 隐私安全

隐私安全保护有利于防止通过观察网络活动或通信推测用户信息。这些隐私信息包括：用户访问的Web站点信息、用户的地理位置、业务提供商网络设备的源和目的IP地址以及域名。另外，隐私还包括宽带客户网络中的ID隐私。

7.2.8 可用性

可用性确保不可通过网络活动试图阻碍对网络、存储的信息、信息流、业务和应用的授权的访问。有多种攻击可以导致可用性的丧失或下降。有些攻击手段可以通过认证和加密来应对，然而防范其他类型的攻击需要通过某些物理的方式防止可用性的丧失。

7.3 安全需求与安全威胁的关系

本标准描述的每个安全需求是为了应对宽带客户网络中的某些特定的安全威胁。安全需求和安全威胁的关系见表1和表2。

表1 安全需求与通用安全威胁的关系

安全需求 \ 威胁		窃听		通信阻断/通信拥塞		数据修改/注入		未授权访问		抵赖	数据包错误转发
		存储数据	通信数据	存储数据	通信数据	存储数据	通信数据	存储数据	通信数据		
保密性	通信数据		Y						Y		
	存储数据	Y						Y			
完整性	通信数据						Y				
	存储数据					Y					Y
认证	实体	Y		Y		Y		Y		Y	
	消息	Y		Y			Y	Y		Y	
不可抵赖										Y	
访问控制	通信数据						Y		Y		
	存储数据	Y		Y		Y		Y			
可用性	通信数据				Y						
	存储数据			Y							
隐私	通信数据		Y								
	存储数据										
通信流安全											Y
注：表中的“Y”表示为了抵御特定的威胁所需的安全需求											

表2 安全需求与移动环境安全威胁的关系

安全需求 \ 威胁		窃听		通信阻断		终端丢失	意外中断
		存储数据	通信数据	存储数据	通信数据		
保密性	通信数据		Y				
	存储数据	Y				Y	
完整性	通信数据						
	存储数据						
认证	实体	Y		Y		Y	
	消息	Y		Y			
不可抵赖							

表2（续）

安全需求 \ 威胁		窃听		通信阻断		终端丢失	意外中断
		存储数据	通信数据	存储数据	通信数据		
访问控制	通信数据						
	存储数据	Y		Y		Y	
可用性	通信数据				Y		Y
	存储数据			Y			
隐私	通信数据		Y				
	存储数据	Y				Y	
通信流安全					Y		
注：表中的“Y”表示为了抵御特定的威胁所需的安全需求							

8 宽带客户网络的安全机制概述

8.1 加密

对数据加密可保证通信的保密性，也可保证存储数据的保密性。在宽带客户网络中，加密功能可以在网关上实现。

8.2 数字签名

数字签名包括两个方面：第一是对数据加签名，即采用私钥产生签名；第二是对已加签名的数据进行验证，即采用公钥验证签名的有效性。

8.3 访问控制

为了确定和实现实体的访问能力，要使用实体的已认证身份进行访问控制。如果实体企图使用未授权的资源、或对已授权的资源进行超权限的访问，那么访问控制机制应拒绝此类企图，或在安全审计记录上留下一条记录。访问控制功能可以在宽带客户网络的网关上实现。

8.4 数据完整性

数据完整性要保证数据的正确性和准确性，即接收方收到的数据与发送方发出的数据完全相同。数据完整性要保证数据在传送过程中未被修改、删除、生成、复制。数据完整性函数一般使用哈希函数或数字签名算法。在宽带客户网络中，数据完整性功能一般在宽带客户网络的网关上实现。

8.5 认证

8.5.1 概述

认证包括对用户的认证和对设备的认证。

对宽带客户网络的用户进行认证，规定认证方法，如口令、数字证书和生物特征识别等。根据业务的不同，规定安全级别和相应的用户认证模型。

对宽带客户网络的设备进行认证以及客户宽带网络设备对公网设备进行的互认证，用于标识设备的身份和归属。

8.5.2 用户认证机制

宽带客户网络的用户认证采用客户/服务器模型如图2所示。根据访问方式的不同，用户认证有以下3种情形：

1）用户通过公网远程访问宽带客户网络。

2）在宽带客户网络内部。

3）宽带客户网络的用户访问公网。认证方式由客户与服务器进行约定，如口令、数字证书和生物特征识别等。

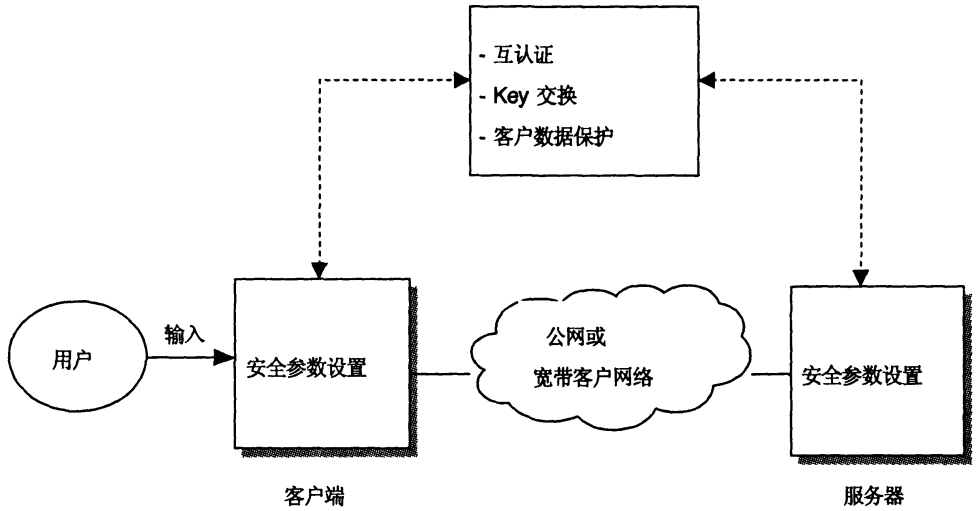

图2 用户认证机制的范畴

用户通过公网远程访问宽带客户网络：用户需要通过宽带客户的安全网关的认证。

在宽带客户网络内部：用户要通过认证服务器的认证，认证服务器可以位于安全网关上，也可是宽带网络内部的一台单独的服务器。

宽带客户网络的用户访问公网：宽带客户网络的安全网关起认证中继作用。

8.5.3 设备认证机制

与用户认证类似，宽带客户网络的设备认证采用客户/服务器模型。设备认证有以下两种情形：

1）宽带客户网关与远程管理服务器关联获得管理配置信息；

2）终端设备与宽带客户网关关联并产生交互，认证方式由客户与服务器进行约定，如口令、数字证书等。

8.5.4 安全级别

为了规范宽带客户网络的用户认证，可以根据业务的不同，规定安全级别和认证机制，如表3所示。

表3 安全级别与认证机制

安全级别	第一级	第二级	第三级
最低安全需求	- 无身份证明 - 客户认证 - 单要素认证 - 对所存储的用户秘密进行读保护和写保护	- 提供身份证明 - 相互认证 - 单要素认证 - 对所存储的用户秘密进行单向哈希、加密或加盐（Salt）	- 提供身份证明 - 相互认证 - 密钥交换 - 对所存储的用户秘密进行单向哈希、加密或加盐（Salt） - 双要素认证 - 在认证协议中通过共享密钥保护敏感数据或结果数据

8.6 密钥管理

密钥管理功能是用来生成、发放、传输、删除和销毁密码密钥，密钥管理功能可以在宽带客户网络的网关上实现。

9 宽带客户网络的安全算法

宽带客户网络的安全算法包括用于认证、签名、加密等过程的密码算法。

10 设备证书轮廓

10.1 概述

本章规定了宽带客户网络中的设备认证，提出认证证书轮廓并规定证书的管理方法。

10.2 设备认证框架

宽带客户网络的设备证书框架分为两种：一种是内部发放证书的模型，另一种是外部发放证书的模型。前者在宽带客户网络中包含一个内部证书机构CA，它通常在安全网关上实现，内部CA产生密钥对，并向宽带客户网络中的设备发放数字证书。后者的情形是：所有宽带客户网络中的设备都使用外部证书机构CA发放的数字证书。

10.3 证书轮廓

宽带客户网络的设备证书轮廓遵从ITU-T X.509的规定。基本证书域包括：版本号、序列号、签名、发放者、有效性、对象、对象公开密钥信息等。由于宽带客户网络的设备计算能力有限，因此证书轮廓只包含基本证书域，不包含扩展证书域。

10.4 证书管理

宽带客户网络的证书机构CA可以是安全网关。证书的管理涉及到设备证书的发放、查询、更新、归档、废除和有效期限管理等。

11 宽带客户网络安全功能要求

11.1 内部联网安全

11.1.1 有线联网技术

对于家庭内部和外部网络共享媒质的有线联网技术（例如电力线、同轴电缆等），应在宽带客户网络与公众网络线路的边界处进行滤波，防止家庭内部通信信号泄露到公众网络中。

11.1.2 无线联网技术

对于WLAN、蓝牙等使用无线媒质的联网技术，应支持通信双方链路层的互认证和数据加密功能。对于支持WLAN的宽带客户网关，还应支持对其WLAN无线信号的发送功率和工作信道的设定以及SSID隐藏的功能。

11.2 IP 访问安全

11.2.1 防火墙功能

11.2.1.1 概述

作为宽带客户网络与公众网络的IP边界设备，宽带客户网关应支持IP防火墙，对内部IP网络进行隔离和保护。

11.2.1.2 安全等级设定

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。

11.2.1.3 报文过滤

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IP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IPoE/PPPoE/ARP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。

11.2.1.4 防攻击功能

设备应支持防DoS攻击功能，对收到的数据包进行解析，并判断是否是DoS攻击，对于DoS攻击的报文进行防DoS攻击处理。该保护适用于所有终结在本设备的IP和桥接的IP的情况。DoS攻击的类型包括以下7种：

— Ping of Death（Ping 攻击）；

— SYN Flooding（SYN 泛洪）；

— ARP Flooding（ARP 泛洪）；

— Spoofing 攻击（哄骗）；

— LAND 攻击；

— Smurf 攻击；

— 其他。

停止攻击后，设备能恢复正常工作，攻击过程中，设备不能死机。

11.2.1.5 防端口扫描功能

宽带客户网关应支持防端口扫描功能，防止攻击者通过端口扫描试探设备上打开的端口和服务。

11.2.1.6 支持端口映射功能

应支持端口映射的设置，包括设置以下4项：

— 目的 IP 地址采用私网地址；

— 可以组合源/目的 IP 地址、协议类型（TCP、UDP）、端口或者端口范围，映射到指定的 LAN 设备的某个端口；

— 支持默认应用列表，支持通用的应用协议的配置，如 FTP、HTTP 等；

— 默认应用列表端口映射规则可查看、可修改。

端口映射可选支持Port Trigger（端口触发）功能，当NAT网关设备收到内部网络的数据包满足触发条件时，这个触发条件一般是协议端口符合预设的端口范围，就会根据预设的开放端口进行端口映射，以提供外部网络访问这些端口的能力。

11.2.1.7 DMZ 功能

支持DMZ主机。

11.2.2 访问控制功能

11.2.2.1 WAN 侧隔离

缺省情况下不允许通过WAN侧以TELNET/HTTP/FTP方式（TR-069协议除外）访问网关设备本身进行设备数据配置。

11.2.2.2 服务访问控制

支持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WEB/FTP/TELNET/SNMP/SSH，默认情况下不允许通过WAN侧访问设备。

11.2.2.3 黑白名单

访问控制规则可以以黑名单或者白名单方式生效。

11.2.3 网络防护功能

11.2.3.1 MAC 地址限制功能

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。

11.2.3.2 组播源禁止功能

宽带客户网关应能防止用户做源的组播。可以禁止用户端口向网络侧发送的IGMP Query和组播数据报文。

11.2.3.3 协议报文抑制速率功能

宽带客户网关应能对发往网络侧的特定协议的广播/组播包（例如DHCP、ARP、IGMP等）的速率进行抑制，并能对其他二层广播报文进行速率限制。

11.3 用户认证和业务安全

11.3.1 用户认证

应支持PAP方式的用户接入认证。在通过PPPoE或PPPoA等PPP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或PPPoA等PPP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的用户接入认证。在拨号过程中，家庭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。

应支持基于PPPoE或PPPoA用户账号的用户接入认证的代理，即家庭网关收到用户终端的包含用户名和密码的PPPoE或PPPoA上网请求后，家庭网关终结PPPoE或PPPoA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，由家庭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。如果家庭网关收到新的用户终端使用该用户名密码拨号，那么家庭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或PPPoA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。

11.3.2 IPTV 业务认证

为了保证IPTV业务的安全，在访问IPTV业务时需要对IPTV用户进行认证。

应支持基于HTTP的基本认证。

应支持基于HTTP的摘要认证。

密码在网络上传输时应进行加密处理。

应支持业务账号和用户标识信息的绑定认证。

11.3.3 VoIP 业务认证

基于SIP协议的VoIP客户端在注册时应支持摘要认证。

基于MGCP协议的VoIP客户端在注册时应支持用户认证。

11.3.4 绿色上网

宽带客户网络需要对网络上的不良信息（如淫秽、色情、暴力等对青少年健康成长不利的信息）、垃圾信息（如垃圾邮件、垃圾短信、垃圾多媒体信息）进行有效过滤。

信息过滤功能可选择安装在安全网关上，也可以选择安装在其他网元上。

宽带客户网络设备初始化并获取安全网关或其他网元IP地址后，下载访问网络的安全配置，并根据这些配置来允许和禁止访问相关网络。

宽带客户网关应具有网址过滤（以黑白名单形式提供）的功能。文本过滤或/和图像过滤等可以在第三方设备实现，可选在宽带客户网关中提供。

宽带客户网络还可具备应用程序管理、时间管理、移动介质管理等辅助过滤功能以及权限管理、日志管理、过滤等级设定、远程告知、远程控制、软件升级和帮助等功能。

11.4 设备管理安全

11.4.1 设备认证

远程管理服务器对宽带客户网络进行远程管理之前，宽带客户网络设备应对远程管理服务器执行设备认证，认证的方式包括以下3种：

— 基于 HTTP 的基本认证；

— 基于 HTTP 的摘要认证；

— 基于 SSL/TLS 的证书认证（可选）。

11.4.2 安全日志

宽带客户网络设备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，每条记录应该打上时间戳。防火墙日志应至少能包含100条记录。

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。

11.4.3 安全管理

宽带客户网关设备应具有两种权限进行不同的本地维护管理功能：普通用户管理权限和管理员本地管理权限。用户进行网络管理所使用的登录口令的长度应不少于8个字符。

普通用户管理权限可对宽带客户网络设备的一些非重要参数进行配置和查询。

管理员本地维护管理权限可对宽带客户网络设备的重要参数进行配置和查询。

12 安全性能要求

对于启用安全功能的宽带客户网络设备（例如，家庭网关），其转发性能与未启用安全功能相比不应有显著下降。具体指标待定。

参 考 文 献

[1] ITU-T X.1111 Framework of security technologies for home network.

[2] ITU-T X.1112 Device certificate profile for the home network.

[3] ITU-T X.1113 Guideline on user authentication mechanism for home network services.

[4] ITU-T X.1114 Authorization Framework for Home Network.

[5] ITU-T X.1121 Framework of security technologies for mobile end-to-end data communications.

[6] YDN 138-2006 基于PC终端的互联网内容过滤软件技术要求。

中 华 人 民 共 和 国

通 信 行 业 标 准

基于公用电信网的宽带客户网络安全技术要求

YD/T 2095-2010

*

人民邮电出版社出版发行

北京市崇文区夕照寺街 14 号 A 座

邮政编码：100061

北京新瑞铭印刷有限公司印刷

*

开本：880×1230 1/16 2011 年 2 月第 1 版

印张：1.25 2011 年 2 月北京第 1 次印刷

字数：30 千字

ISBN 978-7-115-2116/11-67

定价：15 元