YD

# 中华人民共和国通信行业标准

YD/T 1742-2008

# 接入网安全防护要求

Security Protection Requirements for Access Network

2008-01-14 发布　　2008-01-14 实施

中华人民共和国信息产业部　发布

# 目　次

# 前　言

本标准是“电信网和互联网安全防护体系”系列标准之一。该系列标准的结构及名称如下：

1. YD/T 1728-2008　电信网和互联网安全防护管理指南；
2. YD/T 1729-2008　电信网和互联网安全等级保护实施指南；
3. YD/T 1730-2008　电信网和互联网安全风险评估实施指南；
4. YD/T 1731-2008　电信网和互联网灾难备份及恢复实施指南；
5. YD/T 1732-2008　固定通信网安全防护要求；
6. YD/T 1733-2008　固定通信网安全防护检测要求；
7. YD/T 1734-2008　移动通信网安全防护要求；
8. YD/T 1735-2008　移动通信网安全防护检测要求；
9. YD/T 1736-2008　互联网安全防护要求；
10. YD/T 1737-2008　互联网安全防护检测要求；
11. YD/T 1738-2008　增值业务网——消息网安全防护要求；
12. YD/T 1739-2008　增值业务网——消息网安全防护检测要求；
13. YD/T 1740-2008　增值业务网——智能网安全防护要求；
14. YD/T 1741-2008　增值业务网——智能网安全防护检测要求；
15. YD/T 1742-2008　接入网安全防护要求；
16. YD/T 1743-2008　接入网安全防护检测要求；
17. YD/T 1744-2008　传送网安全防护要求；
18. YD/T 1745-2008　传送网安全防护检测要求；
19. YD/T 1746-2008　IP承载网安全防护要求；
20. YD/T 1747-2008　IP承载网安全防护检测要求；
21. YD/T 1748-2008　信令网安全防护要求；
22. YD/T 1749-2008　信令网安全防护检测要求；
23. YD/T 1750-2008　同步网安全防护要求；
24. YD/T 1751-2008　同步网安全防护检测要求；
25. YD/T 1752-2008　支撑网安全防护要求；
26. YD/T 1753-2008　支撑网安全防护检测要求；
27. YD/T 1754-2008　电信网和互联网物理环境安全等级保护要求；
28. YD/T 1755-2008　电信网和互联网物理环境安全等级保护检测要求；
29. YD/T 1756-2008　电信网和互联网管理安全等级保护要求；
30. YD/T 1757-2008　电信网和互联网管理安全等级保护检测要求；
31. YD/T 1758-2008　非核心生产单元安全防护要求；
32. YD/T 1759-2008　非核心生产单元安全防护检测要求。

本标准与YD/T 1743-2008《接入网安全防护检测要求》配套使用。

随着电信网和互联网的发展，将不断补充和完善电信网和互联网安全防护体系的相关标准。

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：信息产业部电信研究院、中国电信集团公司、中国移动通信集团公司、中国网络通信集团公司、中国联合通信有限公司

本标准主要起草人：刘　谦、唐建军、曹一生、钟　星、贾　川

# 接入网安全防护要求

## 1 范围

本标准规定了接入网在安全等级保护、安全风险评估、灾难备份及恢复等方面的安全防护要求。

本标准适用于公用电信接入网。

## 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 1728-2008 电信网和互联网安全防护管理指南

YD/T 1729-2008 电信网和互联网安全等级保护实施指南

YD/T 1730-2008 电信网和互联网安全风险评估实施指南

YD/T 1731-2008 电信网和互联网灾难备份及恢复实施指南

YD/T 1754-2008 电信网和互联网物理环境安全等级保护要求

YD/T 1756-2008 电信网和互联网管理安全等级保护要求

YD/T 1323-2004 接入网技术要求——不对称数字用户线（ADSL)

YD/T 1530-2006 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 1475-2006 接入网技术要求——基于以太网方式的无源光网络（EPON）

YD/T 1160-2001 接入网技术要求——基于以太网技术的宽带接入网

YD/T 1418-2005 接入网技术要求——综合接入系统

YD/T 1186-2002 接入网技术要求——26GHz LMDS 本地多点分配系统

YD/T 1158-2001 接入网技术要求——3.5GHz固定无线接入

YDB 010-2007 固定宽带无线接入设备技术要求：用户站

YDB 012-2007 固定宽带无线接入设备技术要求：基站

## 3 术语和定义

下列术语和定义适用于本标准。

3.1

**接入网安全等级 Security Classification of Transport Network**

接入网安全重要程度的表征。重要程度可从接入网受到破坏后，对国家安全、社会秩序、经济运行、公共利益、网络和业务运营商造成的损害来衡量。

3.2

**接入网安全等级保护 Classified Security Protection of Transport Network**

对接入网分等级实施安全保护。

3.3

组织 Organization

组织是由不同作用的个体为实施共同的业务目标而建立的结构，组织的特性在于为完成目标而分工、合作。一个单位是一个组织，某个业务部门也可以是一个组织。

3.4

接入网安全风险 Security Risk of Transport Network

人为或自然的威胁可能利用接入网中存在的脆弱性导致安全事件的发生及其对组织造成的影响。

3.5

接入网安全风险评估 Security Risk Assessment of Transport Network

指运用科学的方法和手段，系统地分析接入网所面临的威胁及其存在的脆弱性，评估安全事件一旦发生可能造成的危害。为进一步提出有针对性的防护对策和安全措施，防范和化解接入网安全风险，将风险控制在可接受的水平，为最大限度地保障接入网的安全提供科学依据。

3.6

接入网资产 Asset

接入网中具有价值的资源，是安全防护保护的对象。接入网中的资产可能是以多种形式存在，无形的、有形的、硬件、软件，包括物理布局、通信设备、物理线路、数据、软件、文档、规程、业务、人员、管理等各种类型的资源，如接入网的设备（DSLAM、OLT、ONU、以太网交换机、MSAN、无线接入的基站等）、接入网的光/电缆线路、接入网的网络布局等。

3.7

接入网资产价值 Asset Value

接入网中资产的重要程度或敏感程度。资产价值是资产的属性，也是进行资产识别的主要内容。

3.8

接入网威胁 Threat

可能导致对接入网产生危害的不希望事件的潜在起因。它可能是人为的，也可能是非人为的；可能是无意失误，也可能是恶意攻击。常见的接入网威胁有光纤/缆中断、设备失效、火灾、水灾等。

3.9

接入网脆弱性 Vulnerability

脆弱性是接入网中存在的弱点、缺陷与不足，不直接对资产造成危害，但可能被威胁所利用从而危及资产的安全。

3.10

接入网灾难 Disaster of Transport Network

由于各种原因，造成接入网故障或瘫痪，使接入网支持的业务功能停顿或服务水平不可接受，达到特定的时间的突发性事件。

3.11

接入网灾难备份 Backup for Disaster Recovery of Transport Network

为了接入网灾难恢复而对相关网络要素进行备份的过程。

3.12

接入网灾难恢复 Disaster Recovery of Transport Network

为了将接入网从灾难造成的故障或瘫痪状态恢复到正常运行状态或部分正常运行状态，并将其支持的业务功能从灾难造成的不正常状态恢复到可接受状态，而设计的活动和流程。

## 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 |
| DSL | Digital Subscriber Line | 数字用户线 |
| DSLAM | Digital Subscriber Line Access Multiplexer | 数字用户线接入复用器 |
| IP | Internet Protocol | 互联网协议 |
| LMDS | Local Multi-point Distribution System | 本地多点分配系统 |
| MAC | Media access control | 媒质接入控制 |
| OLT | Optical Line Terminal | 光线路终端 |
| ONU | Optical Network Unit | 光网络单元 |
| PON | Passive Optical Network | 无源光网络 |
| PWLAN | Public Wireless Local Area Network | 公众无线局域网 |
| SNI | Service Node Interface | 业务节点接口 |
| UNI | User Network Interface | 用户网络接口 |

## 5 接入网安全防护概述

### 5.1 接入网安全防护范围

接入网由三个接口所定界，即网络侧经由SNI与业务节点相连，用户侧经由UNI与用户设备或用户驻地网相连，网管方面经由网管接口与电信管理网相连。接入网包括各种有线和无线接入系统以及网元管理系统。

接入网的安全防护的范围特指本地网下不同区域（如：区、县等）的接入网，包括各种有线接入系统（如：DSL系统、PON系统、以太网接入系统、综合接入系统等）和无线接入系统（如：LMDS、3.5GHz固定无线接入系统、5.8GHz固定无线接入系统、PWLAN系统、基于802.16d的WiMAX系统等）。

### 5.2 接入网安全防护内容

根据YD/T 1728-2008《电信网和互联网安全防护管理指南》将接入网安全防护内容分为安全风险评估、安全等级保护、灾难备份及恢复等三个部分。

——接入网安全等级保护

主要包括定级对象和安全等级的确定、网络安全、设备安全、物理环境安全、管理安全等。

——接入网安全风险评估

主要包括资产识别、脆弱性识别、威胁识别、已有安全措施的确认、风险分析、风险评估文件记录等。本标准仅对接入网进行资产分析、脆弱性分析、威胁分析，在接入网安全风险评估过程中确定各个资产、脆弱性、威胁的具体值。资产、脆弱性、威胁的赋值方法及资产价值、风险值的计算方法参见YD/T 1730-2008《电信网和互联网安全风险评估实施指南》。

——接入网灾难备份及恢复

主要包括灾难备份及恢复等级确定、针对灾难备份及恢复各资源要素的具体实施等。

## 6 接入网定级对象和安全等级确定

接入网特指本地网范围内的接入网，包括各种有线接入系统（如：DSL系统、PON系统、以太网接入系统、综合接入系统等）和无线接入系统（如：LMDS、3.5GHz固定无线接入系统、5.8GHz固定无线接入系统、PWLAN系统、WiMAX系统等）。网络和业务运营商应根据YD/T 1728-2007《电信网和互联网安全等级保护实施指南》附录A中确定网络安全等级的方法，按照本地网下不同区域（如：区、县等）对接入网定级，根据社会影响力、所提供服务的重要性、服务用户数的大小分别定级，权重$\alpha$、$\beta$、$\gamma$可根据具体网络情况进行调节。

## 7 接入网资产、脆弱性、威胁分析

### 7.1 资产分析

接入网的资产至少应包括：设备硬件、设备软件、重要数据、提供的服务、文档、人员、网络拓扑等，见表1。

**表1 资产列表**

| 分 类 | 示 例 |
|---|---|
| 设备硬件 | 各接入系统及其相关的软硬件，如DSL系统、PON系统、以太网接入系统、综合接入系统、LMDS、3.5GHz固定无线接入系统、5.8GHz固定无线接入系统、PWLAN系统、WiMAX系统等；<br>物理环境设备包括机房、电力供应系统、电磁防护系统、防火、防水和防潮系统、防静电系统、防雷击系统、温湿度控制系统等；<br>链路；<br>各接入系统的操作维护系统 |
| 设备软件 | 设备的系统软件：操作系统、各种数据库软件等；<br>系统控制软件、协议软件；<br>操作维护系统软件 |
| 重要数据 | 支撑接入网运行的各种重要数据，包括网络配置数据、管理员操作维护记录、用户数据等 |
| 文档 | 纸质以及保存在存储介质中的各种文件，如设计文档、技术要求、管理规定（机构设置、管理制度、人员管理办法）、工作计划、技术或财务报告、用户手册等 |
| 人员 | 掌握重要技术的人员，如网络维护人员、设备维护人员等 |
| 网络拓扑 | 光缆/管道、网络拓扑、频率资源 |

### 7.2 脆弱性分析

接入网的脆弱性可以从技术脆弱性和管理脆弱性两个方面考虑。脆弱性识别对象应以资产为核心。部分脆弱性识别内容见表2。

**表2 脆弱性分析表**

| 类 型 | 对 象 | 存在的脆弱性 |
|---|---|---|
| 技术脆弱性 | 网络 | 绘制网络拓扑与现网不一致，光缆/管道超过设计使用年限，网络访问控制不符合规范等 |
| | 设备（含操作系统和数据库） | 设备重要部件未配置主备用保护，设备业务处理能力和功能结构不满足设计要求，设备不具备电源保护措施，与室外电缆相连的设备无防护措施，超过设计使用年限，网管访问无安全控制等 |
| | 物理环境 | 机房场地选择不合理，防火、供配电、防静电、接地与防雷、电磁防护、温湿度控制不符合规范，通信线路、机房设备的保护不符合规范 |

表2（续）

| 类　型 | 对　象 | 存在的脆弱性 |
| --- | --- | --- |
| 管理脆弱性 | | 安全管理机构方面：岗位设置不合理（如人员配置过少、职责不清），授权和审批程序简化，沟通和合作未执行，审核和检查未执行等；<br>安全管理制度方面：管理制度不完善、制度评审和修订不及时等；<br>人员安全管理方面：人员录用不符合程序、人员离岗未办理安全手续，人员未进行安全培训，对于第三方人员未进行限制访问等；<br>建设管理方面：安全方案不完善，软件开发不符合程序，工程实施未进行安全验收或验收不严格等；<br>运维管理方面：物理环境管理措施简单，存储介质使用不受限，设备没有定期维护，厂家支持力度不够，关键性能指标没有定期监控，无恶意代码防范措施，无数据备份和恢复策略，访问控制不严格，操作管理不规范等，应急保障措施不到位，灾难恢复预案不完善 |

### 7.3 威胁分析

接入网的威胁根据来源可分为技术威胁、环境威胁和人为威胁。环境威胁包括自然界不可抗的威胁和其他物理威胁。根据威胁的动机，人为威胁又可分为恶意和非恶意两种，部分威胁见表3。

**表3 威胁来源列表**

| 来　源 | | 威胁描述 |
| --- | --- | --- |
| 技术威胁 | | 光缆/管道中断、板卡失效、网管瘫痪、网络节点失效、病毒入侵、雷击、电磁辐射等 |
| 环境威胁 | 物理环境 | 断电、静电、灰尘、潮湿、温度、电磁干扰等，意外事故或通信线路方面的故障 |
| | 自然灾害 | 鼠蚁虫害、洪灾、火灾、泥石流、山体滑坡、地震、台风、闪电 |
| 人为威胁 | 恶意人员 | 不满的或有预谋的内部人员滥用权限进行恶意破坏；<br>采用自主或内外勾结的方式盗窃或篡改机密信息；<br>外部人员利用网络进行攻击、入侵、植入病毒；<br>外部人员进行物理破坏、盗窃等 |
| | 无恶意人员 | 内部人员由于缺乏责任心或者无作为，应该执行而没有执行相应的操作，或无意地执行了错误的操作导致安全事件；<br>内部人员没有遵循规章制度和操作流程而导致故障或信息损坏；<br>内部人员由于缺乏培训、专业技能不足、不具备岗位技能要求而导致故障或攻击；<br>安全管理制度不完善、落实不到位造成安全管理不规范或者管理混乱导致安全事件 |

## 8 接入网安全等级保护要求

### 8.1 第1级要求

不作要求。

### 8.2 第2级要求

#### 8.2.1 接入网网络安全要求

##### 8.2.1.1 网络拓扑安全

a）光缆/管道使用年限一般不应超过设计要求，超过设计年限的光缆/管道应加强在线监测，定期记录光缆/管道使用状态；

b）应绘制与当前运行情况相符合的网络拓扑图。

#### 8.2.1.2 网络访问控制安全

本节要求只适用于传送IP包的接入网，不适用于传送TDM业务的接入网。

a） 接入网应保证用户在二层域的隔离；

b） 接入网应能对二层广播风暴进行抑制；

c） 接入网应提供用户 MAC 地址或用户账户或 IP 地址与物理端口（如：DSLAM 线路口、ONU/ONT 物理端口、以太网交换机物理端口、无线接入系统远端站物理端口等）的动态对应列表；

d） 接入网应能具有用户带宽限制、用户端口申请 IP 地址数量的限制、用户端口 MAC 地址数量限制等功能；

e） 接入网应根据访问控制列表对源地址、目的地址、源端口、目的端口、协议等进行检查，能允许/拒绝数据包出入；

f） 接入网应能对接入到共享物理媒质网络（如：无线接入、PON 等）的用户端设备进行认证；

g） 接入网中采用共享物理媒质网络（如：无线接入、PON 等）的设备应具备数据加密功能；

h） 接入网设备远程管理系统应具有一定安全机制，避免对用户端设备的非法远程配置；

i） 对重要用户的接入网应开启双归属功能，当接入网与主用软交换设备之间的连接中断时，接入网应能发起向备用软交换的注册请求，并与备用软交换建立连接。

### 8.2.2 接入网设备安全要求

接入网设备包括各种有线接入系统（如：DSL系统、PON系统、以太网接入系统、综合接入系统等）和无线接入系统（如：LMDS、3.5GHz固定无线接入系统、5.8GHz固定无线接入系统、PWLAN系统、WiMAX系统等）。

ADSL系统的安全应符合YD/T1 323、YD/T 1530中的安全要求。

EPON系统的安全应符合YD/T 1475中的安全要求。

GPON系统的安全应符合该系统的相关企业标准中的安全要求。

以太网接入系统的安全应符合YD/T 1160中的安全要求。

综合接入系统的安全应符合YD/T 1418中的安全要求。

LMDS的安全应符合YD/T 1186中的安全要求。

3.5GHz固定无线接入系统的安全应符合YD/T 1158中的安全要求。

PWLAN系统的安全应符合该系统的相关企业标准中的安全要求。

WiMAX系统的安全应符合YDB 010-2007、YDB 012-2007中的安全要求。

### 8.2.3 接入网物理环境安全要求

#### 8.2.3.1 机房设备的物理环境要求

应满足YD/T 1754-2008《电信网和互联网物理环境安全等级保护要求》中第2级的安全要求。

#### 8.2.3.2 无机房的设备物理环境要求

a）设备放置地点的承重能力应满足设计要求；

b）设备放置场所也应当避开强电场、强磁场、易发生火灾、水灾、泥石流、易遭受雷击等的地区；

c）机箱应具备防雨、雪、风砂、日照、雷击的防护措施，保证设备正常工作；

d）机箱应备锁，钥匙由专门人员管理；

e）机箱应具备告警系统，进行环境、电源的告警监测；

f）重要的无机房设备应提供短期的备用电力供应（如UPS设备或蓄电池等）。

#### 8.2.4 接入网管理安全要求

应满足YD/T 1756-2008《电信网和互联网管理安全等级保护要求》中第2级的安全要求。

### 8.3 第3.1级要求

与8.2的要求相同。

### 8.4 第3.2级要求

与8.2的要求相同。

### 8.5 第4级要求

同第3.2级要求。

### 8.6 第5级要求

待补充。

## 9 接入网灾难备份及恢复要求

### 9.1 灾难备份及恢复等级

根据YD/T 1731-2008《电信网和互联网灾难备份及恢复实施指南》5.1节，灾难备份及恢复定级应与安全等级保护确定的安全等级一致。

接入网的灾难恢复应根据灾难的情况，首先保证重要用户的接入，然后恢复一般用户的接入。

### 9.2 第1级要求

不作要求。

### 9.3 第2级要求

#### 9.3.1 备份数据要求

a）接入网关键数据如局端设备配置数据、性能数据、告警数据和安全数据等应有本地数据备份；

b）接入网数据备份范围和时间间隔、数据恢复能力应符合相关要求。

#### 9.3.2 人员和技术支持能力要求

a）接入网应有数据备份技术支持人员；

b）相关技术支持人员应有定期的技术培训。

#### 9.3.3 运行维护管理能力要求

a）接入网应有介质存取、验证和转储管理制度，确保备份数据授权访问；

b）接入网应按介质特性对备份数据进行定期的有效性验证。

#### 9.3.4 灾难恢复预案要求

对重要用户的接入网应有完整的灾难恢复预案。

### 9.4 第3.1级要求

与9.3的要求相同。

### 9.5 第3.2级要求

与9.3的要求相同。

### 9.6 第4级要求

同第3.2级要求。

### 9.7 第5级要求

待补充。