YD

中华人民共和国通信行业标准

YD/T 1746-2008

IP 承载网安全防护要求

Security Protection Requirements for tne IP Bearer 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 1747-2008《IP承载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：杨剑锋、陈运清、陈敏时、叶　华、杜之亭、张云勇

IP承载网安全防护要求

1 范围

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

本标准适用于公众IP承载网。

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 1163-2001 IP网络安全技术要求——安全框架

YD/T 1170-2001 IP网络技术要求——网络总体

YD/T 1478-2006 电信管理网安全技术要求

YD/T 1099-2005 以太网交换机技术要求

YD/T 1627-2007 以太网交换机设备安全技术要求

YD/T 1255-2003 具有路由功能的以太网交换机技术要求

YD/T 1629-2007 具有路由功能的以太网交换机设备安全技术要求

YD/T 1691-2007 具有内容交换功能的以太网交换机设备安全技术要求

YD/T 1096-2001 路由器设备技术规范——低端路由器

YD/T 1097-2001 路由器设备技术规范——高端路由器

YD/T 1358-2005 路由器安全技术要求——中低端路由器

YD/T 1359-2005 路由器安全技术要求——高端路由器

YD/T 1452-2006 IPv6网络设备技术要求——支持IPv6的边缘路由器

YD/T 1454-2006 IPv6网络设备技术要求——支持IPv6的核心路由器

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

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本标准。

3.1.1

IP承载网安全等级 Security Classification of IP Bearer Network

IP承载网安全重要程度的表征。重要程度可从IP承载网受到破坏后，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。

3.1.2

IP承载网安全等级保护 Classified Security Protection of IP Bearer Network

对IP承载网分等级实施安全保护。

3.1.3

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。

3.1.4

IP承载网安全风险 Security Risk of IP Bearer Network

人为或自然的威胁可能利用IP承载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。

3.1.5

IP承载网安全风险评估 Security Risk Assessment of IP Bearer Network

指运用科学的方法和手段，系统地分析IP承载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程度，提出有针对性的抵御威胁的防护对策和安全措施。防范和化解IP承载网安全风险或者将风险控制在可接受的水平，为最大限度地为保障IP承载网的安全提供科学依据。

3.1.6

IP承载网资产 Asset of IP Bearer Network

IP承载网中具有价值的资源，是安全防护保护的对象。IP承载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IP承载网的设备、线路、网络布局等。

3.1.7

IP承载网资产价值 Asset Value of IP Bearer Network

IP承载网中资产的重要程度或敏感程度。IP承载网资产价值是IP承载网资产的属性，也是进行IP承载网资产识别的主要内容。

3.1.8

IP承载网威胁 Threat of IP Bearer Network

可能导致对IP承载网产生危害的不希望事件潜在起因，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IP承载网络威胁有攻击、嗅探、设备节点故障、火灾、水灾等。

3.1.9

IP承载网脆弱性 Vulnerability of IP Bearer Network

脆弱性是IP承载网中存在的弱点、缺陷与不足，不直接对IP承载网资产造成危害，但可能被IP承载网威胁所利用从而危及IP承载网资产的安全。

3.1.10

IP承载网灾难 Disaster of IP Bearer Network

由于各种原因，造成IP承载网故障或瘫痪，使IP承载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。

3.1.11

IP承载网灾难备份 Backup for Disaster Recovery of IP Bearer Network

为了IP承载网灾难恢复而对相关的网络要素进行备份的过程。

3.1.12

IP承载网灾难恢复 Disaster Recovery of IP Bearer Network

为了将IP承载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。

3.2 缩略语

下列缩略语适用于本标准。

BGP	Border Gateway Protocol	边界网关协议
DDoS	Distributed Denial of Service	分布式拒绝服务
DNS	Domain Name System	域名系统
DNSSEC	DNS SECurity	DNS安全性
DoS	Denial of Service	拒绝服务
IP	Internet Protocol	网际协议
MPLS	Multi-Protocol Label Switch	多协议标签交换
QoS	Quality of Service	服务质量
QPPB	QoS Policy Propagation Through the BGP	通过BGP的QoS策略传播
RSVP	Resource ReSerVation Protocol	资源预留协议
SNMP	Simple Network Management Protocol	简单网络管理协议
SSH	Secure Shell	安全外壳
SSL	Secure Socket Layer	安全套接层
TLS	Transport Layer Security	传输层安全
USM	User Security Model	用户安全模型
VACM	View-based Access Control Model	基于视图的访问控制模型

4 IP 承载网安全防护概述

4.1 IP 承载网安全防护范围

IP承载网是指以IP技术为基础的用于承载各类业务网数据的承载网络，是构成数据通信网的基础网络。IP承载网的基本功能包括为上层应用和业务网络提供分组数据的网络路由、交换和传送等。作为承载各种业务及上层应用的信息和数据、连接相关业务系统和功能平台的综合承载网络，IP承载网络的安全可靠性直接关联到业务网络及相关各类业务和上层应用的安全可靠性。

4.2 IP 承载网安全防护内容

根据YD/T 1728-2008《电信网和互联网安全防护管理指南》中电信网和互联网安全防护体系的要求，将IP承载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。

——IP承载网安全等级保护，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。

——IP承载网安全风险评估，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IP承载网进行资产分析、脆弱性分析、威胁分析，在IP承载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》。

——IP承载网灾难备份及恢复，主要包括灾难备份及恢复等级确定、针对灾难备份及恢复对各资源要素的具体要求等。

5 IP承载网定级对象和安全等级确定

我国公众IP承载网定级对象通常应为IP骨干网、IP城域网。网络和业务运营商应根据YD/T 1729-2008《电信网和互联网安全等级保护实施指南》附录A中确定安全等级的方法对IP承载网定级，即对IP骨干网、IP城域网根据社会影响力、所提供服务的重要性、服务规模的大小分别定级，权重α、β、γ可根据具体网络情况进行调节。

考虑到不同地域IP城域网络的规模、结构、运营、管理等因素对于网络安全防护要求的差异，网络和业务运营商可根据实际情况，将IP城域网下辖核心层、汇聚层等网络作为独立的对象，确定相应的安全等级以实施安全防护。

6 IP承载网资产、脆弱性、威胁分析

6.1 资产分析

IP承载网资产的识别与选取应符合科学性、合理性，IP承载网资产大致包括各类设备/主机、数据信息、业务、文件、人员、物理环境设施等。IP承载网的资产分析应包括但不限于表1所列范围。

表1 资产类别

类 别	资 产
网络设备/主机	包括：数据设备，如包括各类路由器、交换机等； 网管系统设备，如包括各类管理服务器、主机、终端、辅助设备等； 域名系统设备，如包括各类域名服务器、辅助设备等； 链路等。 （网络设备/主机资产中可包含与设备/主机直接相关且没有必要细分的软、硬件及相关附件）
独立软件	包括有必要独立识别的软件，如应用软件、系统程序、数据库等
文档/数据	包括数据信息，如网络、设备、功能系统相关的各类业务、配置、管理等方面的数据和信息等； 文档资料，如各类形式的文件、档案、资料（如设计文档、技术资料、管理规定、工作计划、财务报告、数据手册等）
服务/业务	包括网络、各功能/业务系统提供的各类服务和业务等
网络资源	包括网络相关的链路、带宽、各类设备容量、网络地址空间等资源
人员	包括各类人员以及相关技术经验、管理机制等，如掌握相关技术的网络维护人员、设备维护人员、组织、管理机制等
环境/设施	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、温湿度控制系统以及相关设备等

6.2 脆弱性分析

IP承载网的脆弱性包括技术脆弱性和管理脆弱性两个方面。脆弱性识别对象应以资产为核心。IP承载网的脆弱性分析应包括但不限于表2所列范围。

表2 脆弱性类别

类 别	对 象	脆弱性
技术脆弱性	网络	包括：网络规划和拓扑、设备部署、资源配置的缺陷等； 网络保护和恢复能力的缺陷、安全技术措施和策略等方面的漏洞等； 业务相关的接入、访问、服务优先级、资源管理、数据信息检查和过滤等业务接入管理方面的缺陷和漏洞等
	设备/主机	包括：设备硬件安全性、软件安全性的漏洞等； 可靠性、稳定性、业务支持能力和数据处理能力、容错和恢复能力的缺陷等； 设备访问的连接、授权、鉴别、代理和控制等方面的安全漏洞，以及授权接入的口令、方式、安全连接、用户鉴别、代理等访问控制方面存在的漏洞隐患等； 相关数据信息在使用、传送、备份、保存、恢复等环节的安全保护技术缺陷和安全策略的漏洞等
	物理环境	包括物理环境安全防护能力的缺陷：可分为机房场地选择，防火、供配电、防静电、接地与防雷、电磁防护、温湿度控制、通信线路、机房设施及设备的保护等
管理脆弱性		包括网络相关的方案和预案、人员、保障、组织等安全机制和管理制度在制定和实施等环节的漏洞和缺陷，可分为安全管理机构方面（如岗位设置、授权和审批程序、沟通和合作等），安全管理制度方面（如管理制度及相应的评审和修订等），人员安全管理方面（如人员录用、上岗、安全培训、组织、访问控制等），建设管理方面（如安全方案不完善、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），运维管理方面（如物理环境管理、设备维护、技术支持、关键性能指标监控、攻击防范措施、数据备份和恢复、访问控制、操作管理、应急保障措施等）

6.3 威胁分析

IP承载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。IP承载网的威胁分析应包括但不限于表3所列范围。

表3 威胁类别

类 别		威 胁
技术威胁		包括：未充分考虑冗余、可靠性及业务安全、应用需求等原因，妨碍相关功能完全实现的缺陷或隐患造成的安全事件等； 系统差错、节点/链路可靠性等原因造成的故障等； 错误响应和恢复等； 相关数据、信息在备份、保存、恢复过程中发生的差错、损坏、丢失等； 地址、带宽、处理能力、存储空间等资源的滥用、浪费和过渡消耗等； 突发流量和异常数据流量等
环境威胁	物理环境	包括：供电故障，灰尘、潮湿、温度超标，静电、电磁干扰等； 意外事故或通信线路方面的故障等
	灾害	包括：鼠蚁虫害； 洪灾、火灾、泥石流、山体滑坡、地震、台风、雷电等自然灾害； 战争、社会动乱、恐怖活动等

表3（续）

类 别		威 胁
人为威胁	恶意人员	包括：针对网络的恶意拥塞，针对业务、设备等相关数据的拦截、篡改、删除等攻击行为； 针对网络、业务数据、服务、设备进行的恶意扫描、监听、截获等嗅探行为； 恶意代码、病毒等； 非授权访问、越权操作等； 伪造和欺骗等； 物理攻击，损坏、盗窃等
	非恶意人员	包括：误操作； 无作为、技能不足等； 相关数据、信息无意泄漏，数据损坏和丢失等； 组织、安全管理制度不完善、制度推行不力、缺乏资源等非规范安全管理等

7 IP承载网安全等级保护要求

7.1 第1级要求

本标准对安全等级为第1级的IP承载网暂不作要求。

7.2 第2级要求

7.2.1 网络安全要求

7.2.1.1 网络拓扑

a） IP承载网的网络结构应符合YD/T1170-2001中相关要求。

b） IP承载网自治域划分应与网络结构和组织形式一致。

c） IP承载网的地址应统一规划，并体现网络层次性，应有利于路由的组织。

d） IP承载网路由的规划和设计合理，具有较高的可用性和可扩展性。

e） IP承载网应绘制与当前运行情况相符合的网络拓扑图。

7.2.1.2 网络保护与恢复

a） IP承载网节点重要部件和模块应配置为主备用方式。

b） IP承载网应能够根据业务或应用的需求采用链路倒换、链路聚合等安全保护措施。相关技术和指标应达到网络和业务运营商的要求，并符合相关行业技术标准的规定。

c） IP城域网应根据实际情况，合理选择核心节点设置为汇接节点；汇接节点原则上应至少与两个上层节点相连。

d） IP城域网络间原则上应通过骨干网络或城域汇接节点互联。

7.2.1.3 网络管理

a） IP承载网应根据网络结构形式，原则上采用多级分域的管理方式；应根据实际需求或运维体制设置分级权限，实现对网络的灵活管理。

b） IP承载网网管网络与业务网络应严格隔离。

c） IP承载网网络管理应采用安全的管理和控制信息的分发、过滤机制。网络管理信息应通过加密传送。对于专用管理接口，应对目的地址为设备本身的非管理报文和到数据业务接口的报文进行严格控制。

d） IP承载网网络管理应使用用户安全鉴别和认证措施，应符合YD/T 1478-2006中相关安全技术要求。

7.2.1.4 网络安全防范

a） 网络和设备应具有一定抵抗常见攻击、差错防范和处理的能力。

b） IP承载网应根据需要采用有效的QoS和流量管理策略，应保证管理和控制信息具有较高的优先级，应对广播、组播进行必要的控制。

c） 网络设备的软件应具备完善的实时操作、信息处理、更新升级、差错防护、故障定位等功能。

d） 通用服务器/主机设备的系统软件应当限制和禁用可能造成漏洞的服务和端口，应安装和使用防火墙和病毒查杀工具或采取其它防病毒和防攻击措施，软件应及时安装补丁，定期更新，及时消除可能的隐患。

e） 网络设备应具有安全日志的功能。日志应包含访问、配置、状态、统计、告警等安全相关事件的来源、时间、描述等信息内容。

7.2.2 设备安全要求

IP承载网设备按功能划分包括数据设备、网管系统设备和域名系统设备等。数据设备包括各类路由器、交换机设备等；网管系统设备指用于实现对网络和网元进行控制、维护、监测、采集与评估等功能的设备，主要包括各类服务器和终端等主机的软件系统及硬件平台、数据库、辅助设备（如外围设备、探针）等设备；DNS系统设备主要包括实现域名解析功能的服务器、数据库等。

IP承载网数据设备的安全应满足相关设备技术规范、设备安全要求以及设备入网管理相关要求的规定：

以太网交换机的安全应满足YD/T 1099-2005、YD/T 1627-2007等相关标准的安全要求；

具有路由功能的以太网交换机的安全应满足YD/T 1255-2003、YD/T 1629-2007等相关标准的安全要求；

具有内容交换功能的以太网交换机的安全应满足YD/T 1691-2007等相关标准的安全要求；

低端路由器或边缘路由器的安全应相应满足YD/T 1096-2001、YD/T 1358-2005、YD/T 1452-2006等相关标准的安全要求；

高端路由器或核心路由器的安全应相应满足YD/T 1097-2001、YD/T 1359-2005、YD/T 1454-2006等相关标准的安全要求。

IP承载网网管系统、域名系统相关服务器、主机等通用设备应进行必要的安全检测，出具安全测试及验收报告并妥善保存。相关设备应符合并满足网络和业务运营商相关通用设备的要求。

7.2.3 物理环境安全要求

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级的相关要求。

7.2.4 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级的相关要求。

7.3 第3.1级要求

7.3.1 网络安全要求

7.3.1.1 网络拓扑

除满足第2级的要求之外，还应满足以下几点：

a） IP承载网络结构根据网络的运营、管理或区域等因素在逻辑上合理的实现分层和分级；

b） IP承载网网络应保留一定的备用地址，满足业务扩展的需求；

c） IP承载网节点域内接口应使用内部路由协议，域间接口应使用外部路由协议；

d） IP城域网汇聚层节点组织和分布应能满足业务接入和汇聚的需求，节点功能应能满足网络可扩展的需求。

7.3.1.2 网络保护与恢复

除满足第2级的要求之外，还应满足以下几点：

a） IP承载网应具有一定的节点冗余、链路冗余和保护等措施；网络组织和分布应满足业务稳定性和安全性需求；

b） IP承载网应能够根据业务或应用的需求采用转发检测、保护倒换、重路由、负载均衡等安全保护措施。相关技术和指标应达到网络和业务运营商的要求，并符合相关行业技术标准的规定；

c） IP骨干网节点间链路原则上应至少保有两条不同物理路径的连接；

d） IP城域网汇聚层应根据实际情况，合理选择核心节点设置为汇接节点，汇接节点间原则上应至少保有两条不同物理路径的连接。

7.3.1.3 网络管理

除满足第2级的要求之外，还应满足以下几点：

a） IP承载网的网络管理应启用访问和资源控制的安全措施，遵循最小特权原则对接口使用、访问和资源等进行限制。

b） IP承载网络管理原则上应具有对业务相关数据进行检测、统计、控制、过滤的功能。

c） IP承载网络管理应能对节点、链路和各类资源的预警、告警、故障进行及时有效地定位，相关各类预警阈值设置合理。

d） IP承载网络管理使用的SNMP协议原则应支持SNMPv3并支持VACM和USM安全机制；对于远程登录应支持SSH以及相关加密和认证算法，对于Web管理应支持SSL/TLS安全协议；设备支持的SNMP、SSH服务等应能在必要情况下关闭和禁用。

7.3.1.4 网络安全防范

除满足第2级的要求之外，还应满足以下几点：

a） 在控制平面网络和设备应根据实际情况对相关控制信息进行有效合理地加密、认证和过滤；对于目的地址为设备本身的数据包，应具有有效的攻击识别和防范能力；对于异常数据流量具有识别和处理能力。

b） 网络应采用灵活、有效的服务质量和流量控制（如IP QoS、MPLS QoS、流量映射、RSVP、码点标记、流量限速、队列调度、QPPB等）技术策略，符合端到端业务的需求。

c） 网络设备的安全日志应通过特定的安全机制在本地或外部设备上进行记录、输出、存储，应支持日志的管理和审计。

7.3.2 设备安全要求

同第2级要求。

7.3.3 物理环境安全要求

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3.1级的相关要求。

7.3.4 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3.1级的相关要求。

7.4 第3.2级要求

7.4.1 网络安全要求

7.4.1.1 网络拓扑

除满足第2级、第3.1级的要求之外，还应满足以下三点：

a） IP承载网应合理设置分布式域名系统；域名系统层次结构应与网络拓扑一致。

b） IP骨干网节点分布应能满足周边网络接入的需求；节点功能应能满足网络可扩展的需求。

c） IP城域网核心层节点功能应能满足网络业务数据交换的需求。

7.4.1.2 网络保护与恢复

除满足第2级、第3.1级的要求之外，还应满足以下三点：

a） IP骨干网核心节点间应至少保有两条不同物理路径的连接，实现链路冗余。

b） IP城域网核心层应采用全网状结构；节点原则上应采用节点冗余的保护方式

c） IP城域网应具有双出口。

7.4.1.3 网络管理

除满足第2级、第3.1级的要求之外，还应满足以下几点：

a） IP承载网络管理应能实现分域定制的管理功能。

b） IP承载网络的管理应实现平面控制分离。

c） IP承载管理信息及数据的机密性和完整性在传送、接收、处理和存储过程中都应得到保证。

d） IP承载网络管理应具有和启用功能完整的系统安全日志功能。

7.4.1.4 网络安全防范

除满足第2级、第3.1级的要求之外，还应满足以下几点：

a） IP承载网应能够按照分层安全原则通过必要的安全技术实现相关网络安全防范的功能，符合YD/T 1163-2001中相关安全机制要求。

b） IP承载网络应建立完整的端到端电信级安全框架，并在安全框架内采用有效的QoS和流量管理策略，满足不同业务对承载网络的需求，相关技术和指标应符合行业技术标准的规定以及网络和业务运营商的要求。

c） IP承载网域名系统原则上应可通过DNSSEC，加密和保护DNS信息，支持DNSSEC相关资源记录；应能通过严格的安全策略和措施，抵御缓冲区溢出、域名劫持、DoS/DDoS、放大攻击、漏洞侦测等类型的攻击。

7.4.2 设备安全要求

同第2级要求。

7.4.3 物理环境安全要求

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》中相关规定。

7.4.4 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》中相关规定。

7.5 第4级要求

同第3.2级要求。

7.6 第5级要求

安全等级为第5级的IP承载网的安全要求待补充。

8 IP承载网灾难备份及恢复要求

8.1 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》，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。

IP承载网的灾难恢复应根据灾难的情况，首先保证应急通信、重要应用和业务网络的通信，然后恢复一般应用和业务网络的通信。

8.2 第1级要求

本标准对安全等级为第1级的IP承载网暂不作要求。

8.3 第2级要求

8.3.1 冗余系统、冗余设备及冗余链路要求

a） IP承载网应根据实际需求采取必要的链路冗余以保证网络具有抗灾以及灾难恢复能力。

b） IP承载网络单点故障或瘫痪，不应导致其他节点的业务提供发生异常；单一地区范围的网络瘫痪或灾难不应导致其他地区的业务提供发生异常。

c） IP承载网网络灾难备份和恢复时间应满足行业管理、网络和业务运营商应急预案相关要求。

8.3.2 冗余路由要求

a） IP承载网网络路由倒换等指标应符合相关要求。

8.3.3 数据备份要求

a） IP承载网相关关键数据（如业务数据、配置数据、性能数据、告警数据等）应有本地数据备份。

b） IP承载网数据备份范围、时间间隔、数据恢复能力应符合相关要求。

8.3.4 相关人员和技术能力要求

a） IP承载网运维应有相应的管理责任人。

b） IP承载网应有数据备份、管理等相关技术人员。

c） IP承载网应有设备和网络操作、维护、管理等相关技术人员。

8.3.5 运行维护管理能力要求

a） IP承载网应具有完善机房管理制度。

b） IP承载网应具有完善的设备、功能系统和网络运行管理制度。

c） IP承载网应具有介质存取、验证和转储管理制度，确保备份数据授权访问。

d） IP承载网应保持与外部组织间良好的联络和协作能力。

8.3.6 灾难恢复预案要求

a） IP承载网应具有完整的灾难恢复预案。

b） IP承载网应定期组织灾难恢复预案的教育、培训、演练。

c） IP承载网应具备完善的灾难恢复预案管理制度。

8.4 第3.1级要求

8.4.1 冗余系统、冗余设备及冗余链路要求

除满足第2级的要求之外，还应满足以下几点：

a） IP承载网应根据实际需求采用必要的节点冗余以保证网络具有抗灾以及灾难恢复能力。

b） IP骨干网核心节点链路应采用链路冗余的方式提供保护；核心节点原则上应设计并采用冗余节点保护。

c） IP城域网汇聚层节点应配置为双上行链路冗余保护；节点间原则上应设计并采用冗余链路。

8.4.2 冗余路由要求

除满足第2级的要求之外，还应满足以下两点：

a） IP承载网应有流量负荷分担设计；

b） IP承载网应结合网络节点、链路的冗余情况，设计并采用冗余路由的保护措施。

8.4.3 数据备份要求

除满足第2级的要求之外，还应满足：与IP承载网相关的关键数据（如配置数据、告警数据等）在原则上应具有异址数据备份的能力。

8.4.4 相关人员和技术能力要求

除满足第2级的要求之外，还应满足以下三点：

a） IP承载网原则上应有专职数据相关备份、管理技术人员；

b） IP承载网应有专职设备和网络相关操作、维护、管理技术人员；

c） 相关管理和技术人员应定期组织进行技术培训和考核。

8.4.5 运行维护管理能力要求

除满足第2级的要求之外，还应满足：IP承载网应按介质特性对备份数据进行定期的有效性验证。

8.4.6 灾难恢复预案要求

同第2级要求。

8.5 第3.2级要求

8.5.1 冗余系统、冗余设备及冗余链路要求

除满足第2级、第3.1级的要求之外，还应满足以下几点：

a） IP承载网关键系统（运维、域名系统）采用冗余系统的方式保证网络抗灾以及灾难恢复能力。

b） IP承载网骨干链路应采用冗余链路的方式提供网络保护。

c） IP承载网核心、汇接节点应采用冗余节点的方式提供网络保护。

d） IP骨干网应设置异地备用网管中心。

8.5.2 冗余路由要求

同第3.1级要求。

8.5.3 数据备份要求

除满足第2级、第3.1级的要求之外，还应满足：与IP承载网相关的关键数据（如配置数据、告警数据等）应进行异址数据备份，保证相关数据和信息及时恢复的能力。

8.5.4 相关人员和技术能力要求

同第3.1级要求。

8.5.5 运行维护管理能力要求

同第3.1级要求。

8.5.6 灾难恢复预案要求

同第2级要求。

8.6 第 4 级要求

同第3.2级要求。

8.7 第 5 级要求

安全等级为第5级的IP承载网的安全要求待补充。

参 考 文 献

1. YD/T 1171-2001　IP 网络技术要求——网络性能参数与指标
2. YD/T 1149-2001　IP 网络技术要求——计费
3. YD/T 1317-2004　IP 网络技术要求——IP 网与 PSTN、ATM、移动网互通
4. YD/T 1381-2005　IP 网络技术要求——网络性能测量方法
5. YD/T 1382-2005　IP 网络技术要求——流量控制
6. YD/T 1486-2006　承载电信级业务的 IP 专用网络安全框架
7. YDC 007-2002　城市宽带网框架