YD

中华人民共和国通信行业标准

YD/T 1747-2008

IP 承载网安全防护检测要求

Security Protection Testing Requirements for 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 1746-2008《IP承载网安全防护要求》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

本标准主要起草人：杨剑锋、龙维薇、陈敏时、叶　华

IP 承载网安全防护检测要求

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检测要求。

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 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 1755-2008 电信网和互联网物理环境安全等级保护检测要求

YD/T 1757-2008 电信网和互联网管理安全等级保护检测要求

3 定义和缩略语

3.1 定义

下列定义适用于本标准。

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。

3.1.13

访谈 Interview

检测人员通过与IP承载网有关人员（个人/群体）进行交流、讨论等活动，检查IP承载网安全等级保护、IP承载网风险评估和IP承载网灾难备份及恢复相关措施的落实情况以及相关工作的开展情况的一种方法。

3.1.14

检查 Examination

检测人员通过对检测对象进行观察、查验和分析等活动，检查IP承载网安全等级保护、IP承载网风险评估和IP承载网灾难备份及恢复相关措施的落实情况以及相关工作的开展情况的一种方法。

3.1.15

测试 Testing

检测人员通过对检测对象按照预定的方法/工具使其产生特定行为的活动，查看、分析输出结果，检查IP承载网安全等级保护、IP承载网风险评估和IP承载网灾难备份及恢复相关措施的落实情况以及相关工作的开展情况的一种方法。

3.2 缩略语

下列缩略语适用于本标准。

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
QoS	Quality of Service	服务质量
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 承载网安全防护检测概述

4.1 安全防护检测范围

本标准的安全防护检测范围为承载各类业务和上层数据的公众IP承载网络。

4.2 安全防护检测对象

IP承载网安全防护检测对象包括IP骨干网和IP城域网，其中IP城域网安全防护检测对象可进一步划分为核心层、汇聚层。

IP承载网安全等级保护的检测对象确定以后，风险评估的检测对象、灾难备份及恢复的检测对象应与安全等级保护的检测对象相一致。

4.3 安全防护检测内容

按照IP承载网安全防护检测的需要，将IP承载网安全防护检测分为IP承载网安全等级保护检测、IP承载网安全风险评估检测和IP承载网灾难备份及恢复检测三个部分。

IP承载网安全防护检测要求包括以下内容：

——IP承载网安全等级保护检测：主要包括网络安全检测、设备安全检测、物理环境安全检测、管理安全检测等；

——IP承载网安全风险评估检测：主要包括安全风险评估范围检测、安全风险评估内容检测、安全风险评估要素检测、安全风险评估赋值原则检测、安全风险评估计算方法检测、安全风险评估文件类型检测和安全风险评估文件记录检测等；

——IP承载网灾难备份及恢复检测：主要包括冗余系统、冗余设备及冗余链路检测、冗余路由检测、备份数据检测、人员和技术支持能力检测、运行维护管理能力检测和灾难恢复预案检测等。

4.4 安全防护检测结果判定

IP承载网安全防护检测包括对IP承载网的安全等级保护、安全风险评估、灾难备份及恢复三个部分的检测，应对三个部分的检测结果分别进行判定，并根据检测结果分别出具检测报告，检测报告中应具体说明安全防护工作的优势和不足。

对每一个部分中的每一个测试项，应根据具体实施情况进行等级化评价（分5级：很好、较好、一般、较差、很差）。参照表1将各测试项的评价等级换算成评分，各测试项的分数经过一定的算法（例如加权平均）分别得到安全等级保护、安全风险评估、灾难备份及恢复三个部分的总分数，根据总分数分别对安全等级保护、安全风险评估、灾难备份及恢复三个部分的检测结果进行等级化评定，总分数和评定等级的关系如表2所示。在计算总分数过程中，应充分考虑到各测试项在安全防护检测要求中所占的比重，例如，表3给出了安全等级保护子类所占的比重。

表1 测试项评分方法

评价结果	评 分
实施很好	5
实施较好	4
实施一般	3
实施较差	2
实施很差	1

表2 总评分和评定等级的关系

总评分 x	评定等级
$4.5 \leqslant x \leqslant 5$	很好
$3.5 \leqslant x < 4.5$	较好
$2.5 \leqslant x < 3.5$	一般
$1.5 \leqslant x < 2.5$	较差
$1 \leqslant x < 1.5$	很差

表3 安全等级保护子类所占的比重

比重（%）	安全等级保护子类
30	网络安全
10	设备安全
20	物理环境安全
40	管理安全

5 IP承载网安全等级保护检测要求

5.1 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。

5.2 第2级要求

5.2.1 网络安全

5.2.1.1 网络拓扑安全

5.2.1.1.1 检测方式

访谈、检查。

5.2.1.1.2 检测对象

网络设计/验收文档，网络管理文档，设备管理配置记录，网络和业务运营商提供的其他文档，网络及相关设备等。

5.2.1.1.3 检测实施

a）应访谈IP承载网管理人员，并查看网络设计/验收文档、网络和业务运营商提供的其他文档，网络及设备实际组网情况，检查IP承载网的实际结构、网络拓扑是否合理，检查网络结构是否符合YD/T1170-2001中相应的要求。

b）应访谈IP承载网管理人员，并查看网络设计/验收文档、网络及设备管理配置记录、核对网络及设备实际配置情况，检查IP承载网当前自治域（AS）划分与网络结构和组织形式是否一致。

c）应访谈IP承载网管理人员，并查看网络设计/验收文档、网络及设备管理配置记录、核对网络及设备实际配置情况，检查设备地址配置和网络地址规划是否具有层次性，是否有利于路由的组织。

d）应访谈IP承载网管理人员，并查看网络设计/验收文档、网络及设备管理配置记录、核对网络及设备实际配置情况，检查IP承载网当前路由的规划和设计是否合理，是否具有较高的可用性和可扩展性。

e）应访谈IP承载网管理人员，查看网络设计/验收文档、网络和业务运营商提供的其他文档，检查网络及设备的实际组网情况，检查是否绘制与当前运行情况相符合的网络拓扑图。

5.2.1.2 网络保护与恢复

5.2.1.2.1 检测方式

访谈、检查。

5.2.1.2.2 检测对象

网络设计/验收文档，网络管理文档，设备管理配置记录，网络、设备运行历史记录，故障告警记录，网络拓扑图，网络和业务运营商提供的其他文档，网络及相关设备等。

5.2.1.2.3 检测实施

a）应访谈网络管理员，并查看网络设计/验收文档、网络、设备故障告警记录、网络和业务运营商提供的其他文档，检查IP承载网网络节点设备重要部件是否采用主备用冗余保护措施。

b）应访谈网络管理员，并查看网络管理文档、设备管理配置记录、运行历史记录、故障告警记录、网络和业务运营商提供的其他文档，检查承载网络及设备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的情况，验证相关技术和指标是否达到网络和业务运营商的要求，是否符合相关行业技术标准的规定。

c）应访谈网络管理员，并查看网络设计/验收文档、网络和业务运营商提供的其他文档，检查城域网是否根据实际情况合理规划设置核心节点和汇接节点，检查汇接节点是否与两个上一级节点相连。

d）对于城域网存在有核心节点设置为汇接节点的情形，应访谈网络管理员，并查看网络设计/验收文档、网络拓扑图、网络和业务运营商提供的其他文档，检查验证城域网络间是否通过骨干网络或城域

汇接节点互联。

5.2.1.3 网络管理

5.2.1.3.1 检测方式

访谈、检查、测试。

5.2.1.3.2 检测对象

网络设计/验收文档，网络管理文档，设备管理配置记录，网络、设备运行历史记录，故障告警记录，日志文件资料，网络拓扑图，网络和业务运营商提供的其他文档，网络及相关设备等。

5.2.1.3.3 检测实施

a）应访谈网络管理员，并查看网络设计/验收文档、网络管理文档、设备管理配置记录、网络和业务运营商提供的其他文档，检查网络管理是否采用多级分域的管理方式，是否能根据需求或运维体制设置分级管理的权限，测试验证是否能实现对网络安全、灵活地管理，验证网络管理安全是否符合网络和业务运营商的要求。

b）应访谈网络管理员，并查看网络设计/验收文档、网络管理文档、设备管理配置记录、网络和业务运营商提供的其他文档，检查网络、设备的配置以及相关网管系统的连接和组网情况，检查网管网络是否与业务网络实现严格隔离。

c）应访谈网络管理员，并查看网络设计/验收文档、网络管理文档、设备管理配置记录、网络和业务运营商提供的其他文档，检查网络及相关设备的管理是否采用安全的管理和控制信息的分发、过滤机制；检查网络管理信息是否通过加密方式传送；检查和验证专用管理接口，是否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）应访谈网络管理员，并查看网络设计/验收文档、网络管理文档、设备管理配置记录、网络和业务运营商提供的其他文档，检查网络管理是否使用用户安全鉴别和认证措施，验证是否符合 YD/T 1478-2006 中安全技术的要求。

5.2.1.4 网络安全防范

5.2.1.4.1 检测方式

访谈、检查、测试。

5.2.1.4.2 检测对象

网络设计/验收文档，网络、设备管理配置记录，运行历史记录，故障、告警记录，日志文件资料，相关测试报告，网络和业务运营商提供的其他文档，网络及相关设备等。

5.2.1.4.3 检测实施

a）应访谈网络管理员，并查看网络设计/验收文档、网络、设备管理配置记录、故障告警记录、日志文件资料、相关测试报告、网络和业务运营商提供的其他文档，检查承载网络和设备是否采取相关措施抵抗常见攻击，检查是否具有差错防范和处理的能力。

b）应访谈网络管理员，并查看网络设计/验收文档、网络、设备管理配置记录、相关测试报告、网络和业务运营商提供的其他文档，检查网络及相关设备是否根据需要采用有效的 QoS 和流量管理策略，检查管理和控制信息是否具有较高的优先级，检查相关设备对广播、组播等数据是否具有必要的控制措施。

c）应访谈网络管理员，并查看网络设计/验收文档、设备测试报告、网络、设备管理配置记录、故

障告警记录、日志文件资料、网络和业务运营商提供的其他文档，检查网络相关设备的软件是否具有完善的实时操作、信息处理、更新升级、差错防护、故障定位等功能，是否符合网络和业务运营商相关要求。

d）应访谈网络管理员，并查看网络设计/验收文档、设备管理维护记录、故障告警记录、日志文件资料、相关测试报告、网络和业务运营商提供的其他文档，检查网络相关通用服务器/主机设备系统软件是否限制和禁用可能造成漏洞的服务和端口，是否安装和使用防火墙和病毒查杀工具或采取了其他防病毒和防攻击措施，检查相关软件是否及时安装补丁和定期更新，能够及时消除可能的隐患。

e）应访谈网络管理员，并查看网络设计/验收文档、设备测试报告、日志文件资料、网络和业务运营商提供的其他文档，检查网络相关设备是否具有安全日志的功能；检查验证日志信息是否包含访问、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。

5.2.2 设备安全

5.2.2.1 检测方法

访谈、检查。

5.2.2.2 检测对象

设备入网检测报告，设备入网证，安全检测报告，网络和业务运营商提供的其他文档。

5.2.2.3 检测实施

a）应访谈相关技术支持人员和管理人员，查看设备入网检测报告、设备入网证、安全检测报告、网络和业务运营商提供的其他文档，检查承载网络相关数据设备是否有有效的入网检测报告、设备入网证、安全检测报告等。

b）应访谈相关技术支持人员和管理人员，查看设备安全检测报告、网络和业务运营商提供的其他文档，检查承载网络相关通用服务器/主机等设备是否有安全检测报告，检查设备是否符合网络和业务运营商相关通用设备的要求。

5.2.3 物理环境安全

应按照 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》中第 2 级的相关要求进行检测。

5.2.4 管理安全

应按照 YD/T 1757-2008《电信网和互联网管理安全等级保护检测要求》中第 2 级的相关要求进行检测。

5.3 第 3.1 级要求

5.3.1 网络安全

5.3.1.1 网络拓扑安全

5.3.1.1.1 检测方式

访谈、检查。

5.3.1.1.2 检测对象

网络设计/验收文档，网络管理文档，设备管理配置记录，网络和业务运营商提供的其他文档，网络及相关设备等。

5.3.1.1.3 检测实施

除按照第 2 级的要求进行检测之外，还应按照本节内容进行检测。

a）应访谈 IP 承载网管理人员，并查看网络设计/验收文档、网络和业务运营商提供的其他文档，网络及设备实际组网情况，检查 IP 承载网的结构是否根据网络运营、管理或区域等因素在逻辑上合理的实现分层和分级。

b）应访谈 IP 承载网管理人员，并查看网络设计/验收文档、网络及设备管理配置记录、核对网络及设备实际配置情况，检查 IP 承载网是否保留一定的备用地址，是否能满足业务扩展的需求。

c）应访谈 IP 承载网管理人员，并查看网络设计/验收文档、网络及设备管理配置记录、核对网络及设备实际配置情况，检查 IP 承载网当前路由的规划和设计情况，节点域内接口是否使用内部路由协议，节点域间接口是否使用外部路由协议。

d）应访谈 IP 承载网管理人员，并查看网络设计/验收文档、网络及设备管理配置记录、核对网络及设备实际配置情况，检查 IP 城域网汇聚层节点组织和分布是否能满足业务接入和汇聚的需求，节点功能是否能满足网络可扩展的需求。

5.3.1.2 网络保护与恢复

5.3.1.2.1 检测方式

访谈、检查。

5.3.1.2.2 检测对象

网络设计/验收文档，网络管理文档，设备管理配置记录，网络、设备运行历史记录，故障告警记录，网络拓扑图，网络和业务运营商提供的其他文档，网络及相关设备等。

5.3.1.2.3 检测实施

除按照第 2 级的要求进行检测之外，还应按照本节内容进行检测。

a）应访谈网络管理员，并查看网络设计/验收文档、网络拓扑图、网络和业务运营商提供的其他文档，检查 IP 承载网络及相关设备是否根据需要采用节点冗余、链路冗余和保护等保护措施，检查验证网络组织和分布是否能满足业务稳定性和安全性需求。

b）应访谈网络管理员，并查看网络管理文档、设备管理配置记录、运行历史记录、故障告警记录、网络和业务运营商提供的其他文档，检查承载网络及设备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的情况，验证相关技术和指标是否达到网络和业务运营商的要求，是否符合相关行业技术标准的规定。

c）应访谈网络管理员，并查看网络设计/验收文档、网络拓扑图、网络和业务运营商提供的其他文档，检查骨干网节点间链路是否至少保有两条不同物理路径的连接，查对网络、设备运行历史记录，故障告警记录中链路连通和使用情况，检查链路是否具有较高的可靠性。

d）应访谈网络管理员，并查看网络设计/验收文档、网络和业务运营商提供的其他文档，检查城域网是否根据实际情况合理规划设置汇接节点，检查汇接节点是否至少与两个上一级节点相连。

5.3.1.3 网络管理

5.3.1.3.1 检测方式

访谈、检查、测试。

5.3.1.3.2 检测对象

网络设计/验收文档，网络管理文档，设备管理配置记录，网络、设备运行历史记录，故障告警记录，

日志文件资料，网络拓扑图，网络和业务运营商提供的其他文档，网络及相关设备等。

5.3.1.3.3 检测实施

除按照第2级的要求进行检测之外，还应按照本节内容进行检测。

a）应访谈网络管理员，并查看网络设计/验收文档、网络管理文档、设备管理配置记录、网络和业务运营商提供的其他文档，检查IP承载网的网络管理是否启用访问和资源控制的安全措施，是否遵循最小特权原则对接口使用、访问和资源等进行限制，验证网络管理安全是否符合网络和业务运营商的要求。

b）应访谈网络管理员，并查看网络设计/验收文档、网络管理文档、设备管理配置记录、网络和业务运营商提供的其他文档，检查网络管理是否具有对业务相关数据进行检测、统计、控制、过滤的功能。

c）应访谈网络管理员，并查看网络设计/验收文档、网络管理文档、设备管理配置记录、网络和业务运营商提供的其他文档，检查和验证IP承载网络管理是否能对节点、链路和各类资源的预警、告警、故障进行及时有效的定位，检查相关各类预警阈值设置是否合理。

d）应访谈网络管理员，并查看网络设计/验收文档、告警记录、日志文件资料、网络和业务运营商提供的其他文档，检查网络管理使用的SNMP协议是否能够支持SNMPv3版本，检查是否支持SNMPv3版本的VACM和USM安全机制；对于远程登录，检查相关设备是否支持SSH以及相关加密和认证算法；对于Web管理，检查相关设备是否支持SSL/TLS安全协议；对于设备支持的远程管理服务等，应检查相关设备，是否具有必要情况下的关闭和禁用的远程管理的功能。

5.3.1.4 网络安全防范

5.3.1.4.1 检测方式

访谈、检查、测试。

5.3.1.4.2 检测对象

网络设计/验收文档，网络、设备管理配置记录，运行历史记录，故障、告警记录，日志文件资料，相关测试报告，网络和业务运营商提供的其他文档，网络及相关设备等。

5.3.1.4.3 检测实施

除按照第2级的要求进行检测之外，还应按照本节内容进行检测。

a）应访谈网络管理员，并查看网络设计/验收文档、网络、设备管理配置记录、故障告警记录、日志文件资料、相关测试报告、网络和业务运营商提供的其他文档，检查在控制平面承载网络和设备是否根据实际情况对相关控制信息进行有效合理的加密、认证和过滤；对于目的地址为设备本身的数据包，检查相关设备是否具有有效的攻击识别和防范能力；对于异常数据流量，应检查相关设备是否具有识别和处理能力。

b）应访谈网络管理员，并查看网络设计/验收文档、网络、设备管理配置记录、相关测试报告、网络和业务运营商提供的其他文档，检查网络及相关设备是否根据需要采用灵活、有效的QoS和流量控制技术策略，检查相关管理和控制策略的实施是否能满足不同类型端到端业务的需求，检查相关指标是否符合行业、网络和业务运营商相关标准要求。

c）应访谈网络管理员，并查看网络设计/验收文档、设备测试报告、日志文件资料、网络和业务运营商提供的其他文档，检查网络相关设备是否启用安全日志的功能；检查和验证日志是否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；检查和验证相关设备是否具有日志的管理和审计的功能。

5.3.2 设备安全

同第 2 级的相关检测要求。

5.3.3 物理环境安全

应按照 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》中第 3.1 级的相关要求进行检测。

5.3.4 管理安全

应按照 YD/T 1757-2008《电信网和互联网管理安全等级保护检测要求》中第 3.1 级的相关要求进行检测。

5.4 第 3.2 级要求

5.4.1 网络安全

5.4.1.1 网络拓扑安全

5.4.1.1.1 检测方式

访谈，检查。

5.4.1.1.2 检测对象

网络设计/验收文档，网络管理文档，设备管理配置记录，网络和业务运营商提供的其他文档，网络及相关设备等。

5.4.1.1.3 检测实施

除按照第 2 级、第 3.1 级的要求进行检测之外，还应按照本节内容进行检测。

a）应访谈 IP 承载网管理人员，并查看网络设计/验收文档、网络及设备管理配置记录、核对网络及设备实际配置情况，检查 IP 骨干网节点分布是否能满足周边网络接入的需求；节点功能是否能满足网络可扩展的需求。

b）应访谈 IP 承载网管理人员，并查看网络设计/验收文档、网络及设备管理配置记录、核对网络及设备实际配置情况，检查 IP 城域网核心层节点功能是否能满足网络业务数据交换的需求。

c）应访谈 IP 承载网管理人员，并查看网络设计/验收文档、网络及设备管理配置记录、核对网络及设备实际配置情况，检查 IP 承载网域名系统是否与网络层次结构一致，系统规划和设备分布、配置是否合理。

5.4.1.2 网络保护与恢复

5.4.1.2.1 检测方式

访谈、检查。

5.4.1.2.2 检测对象

网络设计/验收文档，网络管理文档，设备管理配置记录，网络、设备运行历史记录，故障告警记录，网络拓扑图，网络和业务运营商提供的其他文档，网络及相关设备等。

5.4.1.2.3 检测实施

除按照第 2 级、第 3.1 级的要求进行检测之外，还应按照本节内容进行检测。

a）应访谈网络管理员，并查看网络设计/验收文档、网络拓扑图、网络和业务运营商提供的其他文档，检查骨干网核心节点间链路是否至少保有两条不同物理路径的连接，实现链路冗余；查对网络、设备运行历史记录，故障告警记录中链路连通和使用情况，检查链路是否具有较高的可靠性。

b）应访谈网络管理员，并查看网络设计/验收文档、网络拓扑图、网络和业务运营商提供的其他文档。检查城域网核心层节点是否采用全网状结构，实现冗余保护；查对网络、设备运行历史记录，故障告警记录中节点运行情况；检查节点是否具有较高的可靠性。

c）应访谈网络管理员，并查看网络设计/验收文档、网络拓扑图、网络和业务运营商提供的其他文档，检查 IP 城域网络是否具有双出口。

5.4.1.3 网络管理

5.4.1.3.1 检测方式

访谈、检查、测试。

5.4.1.3.2 检测对象

网络设计/验收文档，网络管理文档，设备管理配置记录，网络、设备运行历史记录，故障告警记录，日志文件资料，网络拓扑图，网络和业务运营商提供的其他文档，网络及相关设备等。

5.4.1.3.3 检测实施

除按照第 2 级、第 3.1 级的要求进行检测之外，还应按照本节内容进行检测。

a）应访谈网络管理员，并查看网络设计/验收文档、网络管理文档、设备管理配置记录、网络和业务运营商提供的其他文档。检查网络管理是否能实现分域定制的管理功能，验证是否能实现对网络安全、灵活的管理，验证网络管理安全是否符合网络和业务运营商的要求。

b）应访谈网络管理员，并查看网络设计/验收文档、网络管理文档、设备管理配置记录、网络和业务运营商提供的其他文档。检查网络的管理是否实现平面控制分离。

c）应访谈网络管理员，并查看网络设计/验收文档、网络和业务运营商提供的其他文档。检查网络管理相关数据和信息在传送、接受、处理和存储过程中是否有机密性保障措施；检查网络管理相关数据和信息在传送、接受、处理和存储过程中是否有完整性保障措施。

d）应访谈网络管理员，并查看网络设计/验收文档、告警记录、日志文件资料、网络和业务运营商提供的其他文档。检查网络管理相关功能是否支持系统安全日志；检查和验证网络管理是否启用系统安全日志功能。

5.4.1.4 网络安全防范

5.4.1.4.1 检测方式

访谈、检查、测试。

5.4.1.4.2 检测对象

网络设计/验收文档，网络、设备管理配置记录，运行历史记录，故障、告警记录，日志文件资料，相关测试报告，网络和业务运营商提供的其他文档，网络及相关设备等。

5.4.1.4.3 检测实施

除按照第 2 级、第 3.1 级的要求进行检测之外，还应按照本节内容进行检测。

a）应访谈网络管理员，并查看网络设计/验收文档、网络、设备管理配置记录、网络和业务运营商提供的其他文档、网络以及相关设备技术资料。检查承载网络是否按照分层安全原则通过必要的安全技术来实现相关网络安全防范的功能，询问网络分层安全的总体策略以及具体的采用安全措施；检查具体的实现技术是否符合 YD/T 1163-2001 的相关要求。

b）应访谈网络管理员，并查看网络设计/验收文档、网络、设备管理配置记录、网络和业务运营商

提供的其他文档、网络以及相关设备技术资料。询问承载网络是否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；询问相关策略是否满足不同业务对承载网络的需求；检查和验证相关技术和指标是否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）应访谈网络管理员，并查看网络设计/验收文档、网络、设备管理配置记录、故障告警记录、日志文件资料、相关测试报告、网络和业务运营商提供的其他文档。检查域名系统是否可通过 DNSSEC，加密和保护 DNS 信息，是否支持 DNSSEC 的各类资源记录；检查是否采用严格的安全策略和措施，是否能抵御缓冲区溢出、域名劫持、DoS/DDoS、放大攻击、漏洞侦测等类型的攻击。

5.4.2 设备安全

同第 2 级的相关检测要求。

5.4.3 物理环境安全

应按照 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》中第 3.2 级的相关要求进行检测。

5.4.4 管理安全

应按照 YD/T 1757-2008《电信网和互联网管理安全等级保护检测要求》中第 3.2 级的相关要求进行检测。

5.5 第 4 级要求

同第3.2级要求。

5.6 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。

6 IP 承载网安全风险评估检测要求

6.1 安全风险评估范围

6.1.1 检测方式

访谈、检查。

6.1.2 检测对象

风险评估报告。

6.1.3 检测实施

应访谈风险评估负责人，询问进行IP承载网风险评估时，选择的风险评估范围是什么；应检查风险评估报告，查看其风险评估范围是否与要求相一致。

6.2 安全风险评估内容

6.2.1 检测方式

访谈、检查。

6.2.2 检测对象

风险评估报告。

6.2.3 检测实施

a）应访谈承载网风险评估负责人，询问风险评估相关内容是否覆盖了技术安全和管理安全两大类，应检查承载网风险评估报告，查看风险评估报告是否覆盖了技术安全和管理安全；

b）应访谈承载网风险评估负责人，询问风险评估相关技术安全中是否覆盖了网络安全、设备安全

和物理安全，应检查承载网风险评估报告，查看风险评估报告中技术安全是否覆盖了网络安全、设备安全和物理安全等方面；

c）应访谈承载网风险评估负责人，询问风险评估相关管理安全中是否覆盖了安全管理机构、安全管理制度、人员安全管理、安全建设管理、安全运维管理等方面；应检查承载网风险评估报告，查看风险评估报告中管理安全是否覆盖了安全管理机构、安全管理制度、人员安全管理、安全建设管理、安全运维管理等方面。

6.3 安全风险评估要素

6.3.1 检测方式

访谈、检查。

6.3.2 检测对象

风险评估报告，历史记录。

6.3.3 检测实施

a）应访谈风险评估负责人，询问进行承载网风险评估时采用了哪些风险评估的要素和相关属性；应检查风险评估报告中风险评估要素是否包含了资产、脆弱性、威胁、安全措施、风险和残余风险等，同时是否包含了与这些要素密切相关的属性，如业务、资产价值、安全需求和安全事件等。

b）应检查风险评估报告中资产是否包含网络设备/主机、独立软件、文档/数据、服务/业务、网络资源、人员、环境/设施等。

c）应检查风险评估报告中资产价值的计算是否主要考虑了社会影响力、资产价值和可用性等因素，同时采用了合理的计算方法。

d）应检查风险评估报告中脆弱性识别是否包含了技术脆弱性和管理脆弱性等方面，其中技术脆弱性是否包含网络脆弱性、设备/主机脆弱性和物理环境脆弱性；管理脆弱性是否包含安全管理机构方面的脆弱性、人员管理方面脆弱性、建设管理方面的脆弱性、运维管理方面的脆弱性。

e）应检查风险评估报告中的威胁是否包含技术威胁、环境威胁和人为威胁，其中环境威胁是否包含物理环境和灾害，人为威胁是否包含恶意人员和非恶意人员。

f）应检查风险评估报告中威胁识别是否依据了已有安全事件报告数据、检测工具检测数据和国内外同行业报告数据等多个方面综合考虑。

g）应访谈风险评估负责人，询问风险评估结果是否满足风险阈值，应检查风险评估报告，查看风险评估报告中风险值的计算是否采用了合理的计算方法，是否制定了合理的风险阈值。

h）应检查风险评估报告，查看对于不可接收的风险，是否制定了相应的风险处理计划以及采用风险处理计划以后，IP 承载网风险值是否满足阈值要求。

i）应访谈风险评估负责人，对于不可接收的风险，采取了哪些风险处理计划，应检查风险评估报告，查看承载网风险评估时发现的主要问题及其解决方案，同时检查历史记录，查看风险评估并采取安全措施后，网络的安全性是否提高。

6.4 安全风险评估赋值原则

6.4.1 检测方式

访谈、检查。

6.4.2 检测对象

风险评估报告。

6.4.3 检测实施

a）应访谈风险评估负责人，检查风险评估报告，验证IP承载网风险评估的赋值是否遵循了合理的原则；应检查风险评估报告，查看资产的赋值是否从资产的社会影响力、资产价值和可用性三个方面和5个等级进行赋值；

b）应检查风险评估报告，查看脆弱性的赋值是否综合考虑赋值对象对资产损害程度、技术实现的难易程度、脆弱性流行程度等多个方面因素，同时是否按照5个等级进行赋值；

c）应检查风险评估报告，查看威胁的赋值是否依据经验和（或）有关的统计数据来进行分析。

6.5 安全风险评估计算方法

6.5.1 检测方式

访谈、检查。

6.5.2 检测对象

风险评估报告。

6.5.3 检测实施

a）应访谈风险评估负责人，询问风险评估中资产价值和风险值是否采用了合理的计算方法；应检查风险评估报告，查看资产价值的计算方法是否合理，是否具有对于所采用计算方法的理论分析；

b）应检查风险评估报告，查看风险值的计算方法是否合理，是否具有对于所采用计算方法的理论分析。

6.6 安全风险评估文件类型

6.6.1 检测方式

访谈、检查。

6.6.2 检测对象

风险评估方案、风险评估程序、资产识别清单、重要资产清单、脆弱性列表、威胁列表、已有安全措施确认表、风险评估报告、风险评估记录、风险处理计划等风险评估文件。

6.6.3 检测实施

a）应访谈风险评估负责人，询问是否制定了风险评估方案；查看此文件，检查是否包括风险评估的目标、范围、人员、评估方法、评估结果的形式和实施进度等内容。

b）应访谈风险评估负责人，询问是否制定了风险评估程序；查看此文件，检查是否包括风险评估的目的、职责、过程、相关的文件要求以及实施本次评估所需要的各种资产、威胁、脆弱性识别和判断依据等内容。

c）应访谈风险评估负责人，询问是否制定了资产识别清单；查看此文件，检查是否根据组织在风险评估程序文件中所确定的资产分类方法进行资产识别，形成资产识别清单，明确资产的责任人/部门等内容。

d）应访谈风险评估负责人，询问是否制定了重要资产清单；查看此文件，检查是否根据资产识别和赋值的结果，形成重要资产列表，包括重要资产名称、描述、类型、重要程度、责任人/部门等内容。

e）应访谈风险评估负责人，询问是否根据威胁识别和赋值的结果，制定了威胁列表；查看此文件，检查是否包括威胁名称、种类、来源、动机及出现的频率等内容。

f）应访谈风险评估负责人，询问是否根据脆弱性识别和赋值的结果，形成脆弱性列表；查看此文件，检查是否包括具体脆弱性的名称、描述、类型及严重程度等。

g）应访谈风险评估负责人，询问是否根据已采取的安全措施确认的结果，形成已有安全措施确认表；查看此文件，检查是否包括已有安全措施名称、类型、功能描述及实施效果等。

h）应访谈风险评估负责人，询问是否有风险评估报告；查看此文件，检查是否对整个风险评估过程和结果进行总结，详细说明被评估对象，风险评估方法，资产、威胁、脆弱性的识别结果，风险分析、风险统计和结论等内容。

i）应访谈风险评估负责人，询问是否有风险处理计划；查看此文件，检查是否对评估结果中不可接受的风险制定风险处理计划，选择适当的控制目标及安全措施，明确责任、进度、资源，并通过对残余风险的评价以确定所选择安全措施的有效性。

j）应访谈风险评估负责人，询问是否有风险评估记录；查看此文件，检查风险评估过程中的各种现场记录是否可复现评估过程，是否能够作为产生歧义后解决问题的依据。

6.7 安全风险评估文件记录

6.7.1 检测方式

访谈、检查。

6.7.2 检测对象

风险评估报告、风险评估文件。

6.7.3 检测实施

a）应访谈风险评估负责人，询问风险评估过程中对于文件记录进行了哪些限制和控制？应检查风险评估报告和风险评估文件，查看文件发布以前是否得到批准。

b）应检查风险评估报告和风险评估文件，查看文件的更改和现行修订状态是否是可识别的。

c）应检查风险评估报告和风险评估文件，查看是否有版本划分以及相应的版本使用说明。

d）应检查风险评估报告和风险评估文件，查看是否对于作废文件作了标识。

e）应检查风险评估报告和风险评估文件，查看是否规定其标识、储存、保护、检索、保存期限以及处置所需的控制。

7 IP 承载网灾难备份及恢复检测要求

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 冗余系统、冗余设备及冗余链路

7.2.1.1 检测方式

访谈、检查。

7.2.1.2 检测对象

IP 承载网络、设备和链路、设计/验收文档、灾难应急预案、网络和业务运营商提供的其他文档。

7.2.1.3 检测实施

a）应访谈安全管理人员，并查看设计/验收文档、灾难应急预案，检查网络是否根据实际需求采用冗余链路提供保护，是否具有一定的网络抗灾以及灾难恢复能力。

b）应访谈安全管理人员，并查看设计/验收文档、风险评估文件、网络和业务运营商提供的其他文档，检查网络单点故障或瘫痪对其他节点的影响以及检查单一地区范围的网络瘫痪或灾难对其他地区的业务的影响的威胁的风险分析，评估和验证是否不会造成其他节点或地区业务异常；

c）应访谈安全管理人员，并查看设计/验收文档、灾难应急预案，检查 IP 承载网网络灾难备份和恢复时间是否满足行业管理、网络和业务运营商应急预案相关的要求。

7.2.2 冗余路由

7.2.2.1 检测方式

访谈、检查。

7.2.2.2 检测对象

设计/验收文档、演习/历史记录、设备配置、灾难应急预案、网络和业务运营商提供的其他文档。

7.2.2.3 检测实施

应访谈安全管理人员，并查看设计/验收文档、演习/历史记录、灾难应急预案，检查 IP 承载网网络路由倒换等指标是否符合相关要求。

7.2.3 数据备份

7.2.3.1 检测方式

访谈、检查。

7.2.3.2 检测对象

设计/验收文档，演习/历史记录，设备配置，备份数据，灾难应急预案。

7.2.3.3 检测实施

a）应访谈安全管理人员，并查看设计/验收文档、灾难应急预案，检查 IP 承载网相关关键数据（如业务数据、设备配置数据、性能数据、告警数据等）是否有本地数据备份。

b）应访谈安全管理人员，并查看设计/验收文档、演习/历史记录、备份数据、灾难应急预案，IP 承载网数据备份范围、时间间隔、数据恢复能力是否符合相关要求。

7.2.4 人员和技术能力

7.2.4.1 检测方式

访谈、检查。

7.2.4.2 检测对象

各级安全负责人，各相关管理、技术、运维人员，人员任职信息，责任岗位规章，人员管理制度，值班记录，培训考核记录。

7.2.4.3 检测实施

a）应访谈安全负责人、其他相关人员，并查看人员任职信息、责任岗位规章、人员管理制度、培训考核记录，检查验证是否设置运维管理责任人岗位；

b）应访谈安全负责人、其他相关人员，并查看人员任职信息、责任岗位规章、人员管理制度、培训考核记录，检查验证是否设置数据备份、管理相关技术人员岗位；

c）应访谈安全负责人、其他相关人员，并查看人员任职信息、责任岗位规章、人员管理制度、培训考核记录，检查验证是否设置设备和网络操作、维护、管理相关技术人员。

7.2.5 运行维护管理能力

7.2.5.1 检测方式

访谈、检查。

7.2.5.2 检测对象

相关管理规章/制度。

7.2.5.3 检测实施

a）应访谈安全管理人员、各相关管理、技术、运维人员，询问是否有机房管理制度，询问机房管理制度覆盖的范围，检查验证是否具有机房管理制度，管理制度要求的覆盖范围是否完善；

b）应访谈安全管理人员、各相关管理、技术、运维人员，询问是否有设备、功能系统和网络运行管理制度，询问设备、功能系统和网络运行管理制度覆盖的范围，检查验证是否具有设备、功能系统和网络运行管理制度，管理制度要求的覆盖范围是否完善；

c）应访谈安全管理人员、各相关管理、技术、运维人员，询问是否有介质存取、验证和转储管理制度，询问介质存取、验证和转储管理制度覆盖的范围，检查验证是否具有介质存取、验证和转储管理制度，管理制度要求的覆盖范围是否完善，检查是否能实现备份数据授权访问的有效管理和控制；

d）应访谈安全管理人员，检查相关灾难备份及恢复预案、运维管理相关流程，验证是否能保持与外部组织间良好的联络和协作能力。

7.2.6 灾难恢复预案

7.2.6.1 检测方式

访谈、检查。

7.2.6.2 检测对象

灾难恢复预案，设计/验收文档，演练记录，相关管理制度，安全管理人员。

7.2.6.3 检测实施

a）应访谈安全管理人员，询问IP承载网是否具有灾难恢复预案，应检查IP承载网灾难恢复预案设计/验收文档，查看其是否具备完整的IP承载网灾难恢复预案；应检查IP承载网灾难恢复预案，查看其与设计是否一致；

b）应访谈安全管理人员，询问是否定期组织灾难恢复预案的教育、培训、演练，应检查IP承载网灾难恢复预案演练记录，查看其是否已经过灾难恢复预案演练以及灾难恢复预案演练的效果是否达到设计要求。

c）应访谈安全管理人员，询问是否具有灾难恢复预案管理制度，检查验证灾难恢复管理制度相关要求的覆盖范围是否完善。

7.3 第3.1级要求

7.3.1 冗余系统、冗余设备及冗余链路

7.3.1.1 检测方式

访谈、检查。

7.3.1.2 检测对象

IP承载网络，设备和链路，设计/验收文档，灾难应急预案，网络和业务运营商提供的其他文档。

7.3.1.3 检测实施

除按照第2级的要求进行检测之外，还应按照本节内容进行检测。

a）应访谈安全管理人员，并查看设计/验收文档、灾难应急预案，检查IP承载网是否根据实际需求采用冗余节点提供保护，是否具有一定的网络抗灾以及灾难恢复能力。

b）应访谈安全管理人员，并查看设计/验收文档，检查IP骨干网核心节点链路是否采用冗余链路的方式提供保护，检查和验证核心节点是否设计并采用冗余节点的保护方式。

c）应访谈安全管理人员，并查看设计/验收文档，检查城域网汇聚层节点是否配置为双上行链路冗余保护，检查和验证节点间是否设计并采用冗余节点的保护方式。

7.3.2 冗余路由

7.3.2.1 检测方式

访谈，检查。

7.3.2.2 检测对象

设计/验收文档，演习/历史记录，设备配置，灾难应急预案，网络和业务运营商提供的其他文档。

7.3.2.3 检测实施

除按照第2级的要求进行检测之外，还应按照本节内容进行检测。

a）应访谈安全管理人员，并查看设计/验收文档、灾难应急预案，检查IP承载网是否有流量负荷分担设计。

b）应访谈安全管理人员，并查看设计/验收文档、灾难应急预案，询问IP承载网是否结合网络节点和链路冗余情况，设计冗余路由的保护措施；检查并验证网络路由是否采用冗余方式提供保护。

7.3.3 数据备份

7.3.3.1 检测方式

访谈、检查。

7.3.3.2 检测对象

设计/验收文档，演习/历史记录，设备配置，备份数据，灾难应急预案。

7.3.3.3 检测实施

除按照第2级的要求进行检测之外，还应按照本节内容进行检测。

应访谈安全管理人员，并查看设计/验收文档、灾难应急预案，检查相关关键数据（如配置数据、告警数据等）是否具有异址数据备份的能力。

7.3.4 人员和技术能力

7.3.4.1 检测方式

访谈、检查。

7.3.4.2 检测对象

各级安全负责人，各相关管理、技术、运维人员，人员任职信息，责任岗位规章，人员管理制度，值班记录，培训考核记录。

7.3.4.3 检测实施

除按照第2级的要求进行检测之外，还应按照本节内容进行检测。

a）应访谈安全负责人、其他相关人员，并查看人员任职信息、责任岗位规章、人员管理制度、培训考核记录，检查验证是否设置专职数据备份、管理相关技术人员岗位；

b）应访谈安全负责人、其他相关人员，并查看人员任职信息、责任岗位规章、人员管理制度、培

训考核记录，检查验证是否设置专职设备和网络操作、维护、管理相关技术人员。

c）应访谈安全负责人、其他相关人员，并查看人员任职信息、责任岗位规章、人员管理制度、培训考核记录，检查相关管理和技术人员是否定期组织进行技术培训和考核，检查各相关人员的岗位要求是否符合网络相关运维安全要求。

7.3.5 运行维护管理能力

7.3.5.1 检测方式

访谈、检查。

7.3.5.2 检测对象

安全管理人员，相关管理规章/制度。

7.3.5.3 检测实施

除按照第 2 级的要求进行检测之外，还应按照本节内容进行检测。

应访谈安全管理人员，检查数据备份、管理相关制度，检查验证是否按介质特性对备份数据进行定期的有效性验证。

7.3.6 灾难恢复预案

同第 2 级的相关检测要求。

7.4 第 3.2 级要求

7.4.1 冗余系统、冗余设备及冗余链路

7.4.1.1 检测方式

访谈、检查。

7.4.1.2 检测对象

IP 承载网络，设备和链路，设计/验收文档，灾难应急预案，网络和业务运营商提供的其他文档。

7.4.1.3 检测实施

除按照第 2 级、第 3.1 级的要求进行检测之外，还应按照本节内容进行检测。

a）应访谈安全管理人员，并查看设计/验收文档、灾难应急预案，检查 IP 承载网是否根据实际需求采用冗余系统的方式对关键系统提供保护，是否具有一定的网络抗灾以及灾难恢复能力。

b）应访谈安全管理人员，并查看设计/验收文档，检查 IP 承载网骨干链路是否采用冗余链路的方式提供保护。

c）应访谈安全管理人员，并查看设计/验收文档，检查 IP 承载网核心、汇接节点是否采用冗余节点的方式提供网络保护。

d）应访谈安全管理人员，并查看设计/验收文档、灾难应急预案，检查 IP 骨干网是否设置有异地备用网管中心。

7.4.2 冗余路由

同第 3.1 级的相关检测要求。

7.4.3 数据备份

7.4.3.1 检测方式

访谈、检查。

7.4.3.2 检测对象

设计/验收文档，演习/历史记录，设备配置，备份数据，灾难应急预案。

7.4.3.3 检测实施

除按照第 2 级、第 3.1 级的要求进行检测之外，还应按照本节内容进行检测。

应访谈安全管理人员，并查看设计/验收文档、灾难应急预案，检查相关关键数据（如配置数据、告警数据等）是否具有异址数据备份。

7.4.4 人员和技术支持能力

同第 3.1 级的相关检测要求。

7.4.5 运行维护管理能力

同第 3.1 级的相关检测要求。

7.4.6 灾难恢复预案

同第 2 级的相关检测要求。

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。

参 考 文 献

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 1754-2008	电信网和互联网物理环境安全等级保护要求
6	YD/T 1756-2008	电信网和互联网管理安全等级保护要求
7	YD/T 1171-2001	IP 网络技术要求——网络性能参数与指标
8	YD/T 1149-2001	IP 网络技术要求——计费
9	YD/T 1317-2004	IP 网络技术要求——IP 网与 PSTN、ATM、移动网互通
10	YD/T 1381-2005	IP 网络技术要求——网络性能测量方法
11	YD/T 1382-2005	IP 网络技术要求——流量控制
12	YDC 007-2002	城市宽带网框架
13	YD/T 1486-2006	承载电信级业务的 IP 专用网络安全框架
14	YD/T 1099-2005	以太网交换机技术要求
15	YD/T 1627-2007	以太网交换机设备安全技术要求
16	YD/T 1255-2003	具有路由功能的以太网交换机技术要求
17	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
18	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
19	YD/T 1452-2006	IPv6 网络设备技术要求——支持 IPv6 的边缘路由器
20	YD/T 1454-2006	IPv6 网络设备技术要求——支持 IPv6 的核心路由器
21	YD/T 1096-2001	路由器设备技术规范——低端路由器
22	YD/T 1097-2001	路由器设备技术规范——高端路由器
23	YD/T 1358-2005	路由器安全技术要求——中低端路由器
24	YD/T 1359-2005	路由器安全技术要求——高端路由器