前　言

本标准是根据住房和城乡建设部《关于印发〈2009年工程建设标准规范制订、修订计划〉的通知》(建标〔2009〕88号)的要求，由中国移动通信集团设计院有限公司会同有关单位共同编制完成。

本标准适用于公用互联网的网络工程设计。在编制过程中，编制组进行了深入的调查研究，认真总结了公用互联网网络工程设计的实践经验，分析了各种技术的应用与发展状况，广泛征求全国有关单位和专家的意见，并参考了国内外相关标准规定的内容，最后经审查定稿。

本标准共分14章，主要技术内容包括：总则，术语和代号，网络组成与功能，网络结构，路由协议与路由策略，网间互联，网络管理，传送技术，业务承载和接入，编号方案、地址分配与域名系统，网络性能与服务质量，网络与信息安全，设备配置原则，机房设计。

本标准由住房和城乡建设部负责管理，工业和信息化部负责日常管理，中国移动通信集团设计院有限公司负责具体技术内容的解释。本标准在应用过程中如有需要修改与补充的地方，请将有关意见和建议反馈给中国移动通信集团设计院有限公司(地址：北京市海淀区丹棱街甲16号，邮政编码：100080)，以供修订时参考。

本标准主编单位、参编单位、主要起草人和主要审查人：

主 编 单 位：中国移动通信集团设计院有限公司

参 编 单 位：山东省邮电规划设计院有限公司
华信邮电咨询设计研究院有限公司
江苏省邮电规划设计院有限责任公司

中广电广播电影电视设计研究院

华为技术有限公司

主要起草人：崔海东　田海建　周振勇　牛瑛霞　唐利莉

王保兵　程　烨　刘春林　詹叶青　岳卫民

主要审查人：鲁华伟　周晓杰　叶宇煦　马　科　包秀国

张锡跃　舒华峰　蔡善奇　赵丽红　孙晶红

王庆辉

目　　次

Contents

1 总　　则

1.0.1　为使公用互联网网络工程设计做到技术先进、经济合理、安全适用、节能节材、可持续发展，制订本标准。

1.0.2　本标准适用于新建、改建、扩建公用互联网网络的工程设计。

1.0.3　公用互联网网络设计应遵循开放性的原则，设计的网络应具有可管理性、可运营性、可扩展性，设计的网络应安全可靠。

1.0.4　工程设计应选用符合国家现行有关技术要求的定型产品。未经产品质量监督检验机构鉴定合格的设备及主要材料，不得在工程中使用。

1.0.5　在我国抗震设防烈度7度以上（含7度）地区，公用互联网网络工程中使用的主要电信设备应经电信设备抗地震性能检测合格。

1.0.6　公用互联网网络工程设计除应符合本标准外，尚应符合国家现行有关标准的规定。

2 术语和代号

2.1 术　　语

2.1.1 公用互联网　　Internet

面向公众用户提供服务，可承载语音、数据和多媒体类业务的IP网络。

2.1.2 网络节点　　network node

构成IP网络的基本单元之一。提供与其他网络节点的连接，提供节点之间的路由选择机制，转发IP数据包。网络节点提供一种或多种网络功能，一般由位于同一机房的一台或几台互相本地连接的路由器、交换机等网络设备、服务器设备等组成。

2.1.3 中继电路　　trunk

构成IP网络的基本单元之一。连接网络的不同网络节点，提供网络节点之间通信的物理或逻辑媒介。

2.1.4 业务接入控制系统　　service access control system

将用户和业务接入互联网网络，并实现用户和业务接入的认证、授权和计费等功能，实现服务质量控制、组播控制等功能的系统。

2.1.5 运行维护支撑系统　　operation and maintenance support system

支撑网络、保障正常运行的系统，主要包括网管系统和安全系统等。

2.1.6 安全系统　　security system

保障各类网元设备正常运行，保证信息在IP网络上安全传输，保障网络的运营维护管理安全，保障业务安全的有关系统。

2.1.7 网管系统　　network management system

保障网元及网络正常运行，实现配置管理、资源管理、故障管理、性能管理等功能的系统。

2.1.8 双栈　　dual stack

在服务器或路由器、交换机等网络设备中同时支持 IPv4 和 IPv6 双协议栈的技术。

2.1.9 数据包　　packet

通过 IP 网络传送数据的分组，是 IP 网络端到端的传输单元。

2.1.10 骨干网　　backbone network

互联网网络的骨干部分，主要用于各城域网的广域互联，并与其他 IP 网络进行网间互联，同时可直接接入大型 IDC、大型业务系统和重要用户。

2.1.11 城域网　　metro area network

城域范围内的 IP 网络，位于骨干网与城域接入网之间，是 IP 骨干网在城域范围内的延伸和覆盖，是覆盖城市、郊区及其所辖的县市和地区，提供多种业务在城域内的互联、接入及用户接入的网络。

2.1.12 连通度　　connectivity

断开一对节点之间所有通路所需要去掉的最少节点数。

2.1.13 路由器　　router

通过转发数据包来实现网络互联、工作在 IP 层的网络设备。路由器可以支持多种协议，本标准中主要指支持 TCP/IP 协议簇和(或)MPLS 相关协议。

2.1.14 带宽平均峰值利用率　　bandwidth mean peak utilization ratio

在一天业务最忙的一个小时内，每个统计粒度下的电路带宽利用率的算术平均值。

2.1.15 自治域　　autonomous system

包含一组由一系列路由器等网络设备互联而成的子网，构成网络拓扑一个可连接的分段。这些子网和路由器等网络设备一般

都由一个单一的操作维护管理组织来控制，拥有单一和明确的路由政策，并使用一个自治域号来标识。

2.1.16 网间互联 network interconnection

使用IP协议把多个IP网络连接起来，在网络层提供相互转发IP包和路由信息服务，使一个IP网络中的用户能够与所连接的IP网络中的用户相互通信或者能够使用所连接的IP网络中的各种业务应用资源。

2.1.17 转接方式 transfer mode

提供方互联单位向客户方互联单位提供必要的路由信息，并提供IP数据包转发服务，使客户方互联单位可以访问提供方互联单位IP网络内的业务与应用资源，并通过提供方互联单位的IP网络实现对其他IP网络的访问。

2.1.18 对等方式 peer mode

两个互联单位之间进行平等互联，交换双方IP网络的路由信息并实现双方IP网络内用户与业务应用的互访，不转接与第三方互联单位之间的流量。

2.1.19 隧道 tunnel

一种协议封装到另外一种协议中的技术，通过在荷载数据报文前封装传送数据报头建立点到点的传送通道，实现荷载数据在传送报文网络中传送。

2.1.20 翻译 protocol translation

将一种数据包中的每个字段与另一种数据包中的每个字段建立起一一映射的关系，从而在两个网络的互联处实现数据报文转换的技术。

2.1.21 网络地址转换 network address translation

将IP数据包头中的IP地址转换为另一个IP地址的过程。

2.1.22 IP地址 IP address

按照IP协议分配的固定长度数字标识符，用于标识数据发送的源和目的地，包括IPv4地址和IPv6地址。

2.1.23 域名系统　　domain name system

域名系统是一种将域名映射为某些预定义类型资源记录的分布式 IP 网络服务系统，网络中域名服务系统间通过相互协作实现域名到相应资源记录的解析。

2.1.24 IP 包传输时延　　IP packet transfer delay

IP 数据包从网络一个节点进入到离开网络另一个节点所需要的传输时间。

2.1.25 IP 包时延变化　　IP packet delay variation

IP 包传输时延不超过概率为 $1-10^{-3}$ 的上限减去 IP 包传输时延的最小值。

2.1.26 IP 包误差率　　IP packet error ratio

错误 IP 包传送结果与成功 IP 包传送加错误 IP 包传送结果之和的数量比值。

2.1.27 IP 包丢失率　　IP packet loss ratio

丢失的 IP 包传送结果与所有 IP 包的数量比值。

2.1.28 服务质量　　quality of service

IP 网络承载业务所需要的资源保证。服务质量采用指标来表征，可包括丢包率、时延、时延变化、链路传输码率及其精度等。

2.1.29 接入连接建立成功率　　access connection establishment success ration

有线接入方式下为在用户账号、密码正确的前提下，接入服务器的接通次数与用户申请建立连接的总次数之比；无线接入方式下为无线终端发起分组数据连接建立请求并成功建立连接的次数与无线终端发起分组数据连接建立请求总次数之比。

2.1.30 用户接入认证平均响应时间　　user access authentication average response time

有线接入方式下为用户申请建立网络连接时，从用户提交完账号和密码起，至接入服务器完成认证并返回响应止的时间平均值；无线接入方式下为从用户提交完数据连接建立请求时起，至网

络返回连接响应时止的时间平均值。

2.1.31 有线接入速率　　wired access rate

有线接入方式下，从用户终端到接入服务器之间的接入速率。

2.2 代　　号

英文缩写	英文名称	中文名称
ACL	Access Control List	访问控制列表
AFTR	Address Family Transition Router	地址族转换路由器
BFD	Bidirectional Forwarding Detection	双向转发检测
BGP	Border Gateway Protocol	边界网关协议
BRAS	Broadband Remote Access Server	宽带接入服务器
BSS	Business Support System	业务支撑系统
CIDR	Classless Interdomain Routing	无类域间路由
CGN	Carrier-Grade NAT	运营商级网络地址翻译
DiffServ	Differentiated Services	区分服务
DWDM	Dense Wavelength Division Multiplexing	密集波分复用
ECMP	Equal Cost Multi-Path	等价多路径
E-LSP	EXP-Inferred-PSC LSPs	使用 EXP 字段的 LSP
FRR	Fast Reroute	快速重路由
IDC	Internet Data Center	互联网数据中心
IGP	Interior Gateway Protocol	内部网关协议
IP	Internet Protocol	互联网协议
IPDV	IP packet Delay Variation	IP 包时延变化
IPER	IP packet Error Ratio	IP 包误差率
IPLR	IP packet Loss Ratio	IP 包丢失率
IPTD	IP packet Transfer Delay	IP 包传输时延
IPv4	Internet Protocol version 4	互联网协议第 4 版

IPv6	Internet Protocol version 6	互联网协议第6版
IS-IS	Intermediate System-to-Intermediate System	中间系统到中间系统
LDP	Label Distribution Protocol	标记分发协议
LSP	Label Switched Path	标记交换路径
MPLS	Multiprotocol Label Switching	多协议标记交换
NAP	Network Switching Point	网络交换点
OSPF	Open Shortest Path First	开放最短路径优先路由协议
OSS	Operation Support System	运行支撑系统
OTN	Optical Transport Network	光传送网
QoS	Quality of Service	服务质量
RD	Route Distinguisher	路由区分器
RIP	Route Information Protocol	路由信息协议
RT	Route Target	路由目标
SDH	Synchronous Digital Hierarchy	同步数字系列
SDN	Software Designed Network	软件定义网络
SNMP	Simple Network Management Protocol	简单网络管理协议
SR	Service Router	业务路由器
TE	Traffic Engineering	流量工程
uRPF	unicast Reverse Path Forwarding	单播反向路径转发
VLSM	Variable-Length Subnet Mask	可变长子网掩码
VPN	Virtual Private Network	虚拟专用网
XML	Extensible Markup Language	可扩展标记语言

3 网络组成与功能

3.1 组　　成

3.1.1 公用互联网网络应由网络节点、中继电路、业务接入控制系统和运行维护支撑系统组成。

3.1.2 公用互联网网络的运行维护支撑系统可包括安全系统和网管系统等。

3.2 功　　能

3.2.1 公用互联网网络应具备同时转发 IPv4 和 IPv6 数据包能力及向下一代互联网平滑过渡能力，可采用双栈方式。

3.2.2 公用互联网网络应具备动态路由机制功能，建立维护数据包转发路由表。

3.2.3 公用互联网网络宜支持 MPLS 协议。

3.2.4 公用互联网网络可支持 SDN 相关协议。

3.2.5 公用互联网网络应能接入各类用户承载各种业务，应支持对用户和业务的计费，应支持 IPv4 和 IPv6 用户业务间的互通。

3.2.6 公用互联网网络应具备安全功能。

3.2.7 公用互联网网络应具备网管功能。

4 网络结构

4.1 网络层次

4.1.1 公用互联网网络的层次应根据规模、运营、维护管理等因素确定，应符合下列规定：

1 网络层次可分为骨干网、城域网两级；

2 可根据业务需求在省内城市和地区组建城域网，根据业务流量、流向和管理等因素也可组织跨地区的区域城域网；

3 在城域网之上组建骨干网，接入汇聚来自各个城域网的流量并转接疏通；

4 规模较小的网络可仅由一级层次构成，可不区分骨干网和城域网。

4.1.2 公用互联网骨干网可包含省际骨干网和省内骨干网两个子层次，在维护管理条件允许时，宜采用扁平化设计方式，不区分省际、省内子层次。

4.1.3 公用互联网城域网的子层次应根据规模等因素确定，可分为核心层、业务接入控制层和汇聚层。汇聚层应通过城域接入网、城域传送网接入用户和业务。

4.1.4 公用互联网在骨干网内应设置国内网间互联互通子层，实现与其他公用互联网之间的互联互通。

4.1.5 公用互联网在有国际业务需求时，可设置国际互联互通子层，实现与国外公用互联网之间的互联互通；可设置国际网络部分，可由国际流量交换层和国际接入层组成。

4.2 节点设置

4.2.1 公用互联网的网络节点设置应综合考虑节点间业务流量、

网络覆盖和运营维护等因素，根据业务发展需要确定。未设置网络节点的区域，可通过传送网延伸。

4.2.2 根据建设需求，公用互联网的骨干网可由汇接节点、国内互联互通节点及国际互联互通出入口节点组成。

4.2.3 不区分省际、省内子层次的公用互联网骨干网，根据网络规模以及维护管理边界的不同，汇接节点可覆盖至省会级或地市级。节点设置应符合下列规定：

1 汇接节点覆盖至省会级时，可设置核心汇接节点和一般汇接节点，并应符合下列规定：

1) 核心汇接节点用于汇聚、转接一般汇接节点的流量，数量不宜多于30个；

2) 一般汇接节点接入疏通城域网的流量，数量不宜多于70个，每个省内的一般汇接节点数量不宜少于2个。

2 汇接节点覆盖至地市级时，可设置核心汇接节点、汇聚汇接节点和一般汇接节点，并应符合下列规定：

1) 核心汇接节点用于转接汇聚汇接节点的流量，数量不宜多于30个；

2) 汇聚汇接节点用于汇聚、转接一般汇接节点的流量，数量不宜多于70个，每个省内的汇聚汇接节点数量不宜少于2个；

3) 一般汇接节点接入疏通城域网的流量，数量不宜多于350个。

4.2.4 区分省际、省内子层次的公用互联网骨干网，在省际骨干网内和省内骨干网内可分别设置核心汇接节点和一般汇接节点，并应符合下列规定：

1 省际骨干网的核心汇接节点用于汇聚、转接省际骨干网的一般汇接节点的流量，数量不宜多于30个；一般汇接节点用于接入疏通省内骨干网，数量不宜多于70个，每个省内的一般汇接节点数量不宜少于2个；

2 省内骨干网的核心汇接节点用于疏通省间流量，汇聚、转接省内骨干网一般汇接节点的流量，一般汇接节点用于接入疏通城域网流量。每个省内骨干网的核心汇接节点数量宜为2个～4个，一般汇接节点数量不宜多于30个。

4.2.5 骨干网国内网间互联互通子层应设置互联互通节点，主要功能应为转接与国内其他公用互联网之间的流量，实现国内网间互联。

4.2.6 骨干网国际互联互通子层应设置国际出入口节点，主要功能应为转接国际业务流量，实现国际网间互联。

4.2.7 城域网可由核心节点、业务接入控制节点、汇聚节点组成，并应符合下列规定：

1 城域网的核心节点应用于汇聚、转接业务接入控制节点的流量，与骨干网互联；根据城域网规模的不同，核心节点的数量宜为2个～4个；

2 城域网的业务接入控制节点应实现城域网业务的接入及控制、转接汇聚节点的流量，节点数量应综合考虑业务发展、网络建设成本、故障影响面、光纤资源、传输资源和机房条件等因素进行核算；

3 城域网汇聚节点应用于汇聚来自城域接入网的流量，节点数量应基于接入节点的数量，根据业务需求取定适当的收敛比核算；

4 城域接入网的主要功能应为通过各种接入技术和线路资源实现对用户的覆盖，应提供多种方式的用户接入，必要时可配合完成用户流量控制功能。

4.2.8 国际网络部分可根据业务需要设置国外节点，由国际流量交换节点和国际接入节点组成。

4.3 中继电路组织

4.3.1 公用互联网网络节点之间可采用直达中继电路或转接方

式实现业务流量疏通，电路组织应符合业务流量流向特点，并应根据节点间的业务流量需求规划疏通方式、设定各级电路组织阀值。

4.3.2 公用互联网骨干网整体上可采用不完全网状结构进行中继电路组织，并应符合下列规定：

1 骨干网内设置核心汇接节点、汇聚汇接节点和一般汇接节点时，汇接节点之间的中继电路组织应符合下列规定：

1) 一般汇接节点应和2个以上(含2个)的汇聚汇接节点之间设置中继电路，汇聚关系宜为在同一业务运营维护管理域内；

2) 汇聚汇接节点应和2个以上(含2个)的核心汇接节点之间设置中继电路，汇聚关系应综合考虑传输路由方向和本级电路组织阀值确定；

3) 同一业务运营维护管理域内的汇聚汇接节点之间宜设置直达中继电路；

4) 业务流量大、超过本级电路组织阀值时，不同业务运营维护管理域内的部分汇聚汇接节点之间可设置高效直达中继电路，该电路宜只用于疏通局部流量。

2 骨干网内设置核心汇接节点和一般汇接节点时，汇接节点之间的中继电路组织应符合下列规定：

1) 一般汇接节点应和2个以上(含2个)的核心汇接节点之间设置中继电路，汇聚关系应综合考虑传输路由方向和本级电路组织阀值确定；

2) 业务流量大、超过本级电路组织阀值时，部分一般汇接节点之间可设置高效直达中继电路，该电路宜只用于疏通局部流量；

3) 包含省际、省内子层次的骨干网中，省内骨干网的核心汇接节点应和2个以上(含2个)的省际骨干网的一般汇接节点之间设置中继电路。

3 核心汇接节点之间的中继电路组织应符合下列规定：

1)可采用不完全网状结构或完全网状结构进行电路组织，应综合考虑传输路由方向和本级电路组织阀值确定拓扑结构；

2)核心汇接节点间的连通度不宜小于3。

4 互联互通节点、国际出入口节点应和核心汇接节点间设置直达中继电路。

4.3.3 公用互联网城域网节点间的电路组织应符合下列规定：

1 核心节点之间可采用完全网状结构进行电路组织；

2 业务接入控制节点宜和2个以上(含2个)的核心节点之间设置中继电路；

3 汇聚节点宜和2个以上(含2个)的业务接入控制节点之间设置中继电路，连接方式可选择星形、双星形、口字形等；

4 接入网络出入口节点宜和2个以上(含2个)的汇聚节点之间设置中继电路，汇聚关系应根据传输路由方向确定；

5 城域网的核心节点与骨干网的一般汇接节点之间应设置中继电路。

4.3.4 若存在国际网络部分，电路组织应符合下列规定：

1 国际流量交换节点应和2个以上(含2个)的国际出入口节点之间设置国际中继电路；

2 国际流量交换节点、国际业务接入节点的中继电路可参照国内网络部分电路组织规定设置，应根据业务需求确定。

4.3.5 公用互联网的中继电路组织应保障网络的可靠性，中继方向可按重要性分级，具体规定如下：

1 中继方向重要性可分为R1级、R2级和R3级。R1级为最重要级中继方向，该中继方向所属中继电路的中断将导致较大面积网络路由迂回、流量拥塞，或流量疏通能力明显下降。R2级为重要级中继方向，该中继方向所属中继电路的中断将导致部分网络路由迂回、增加流量拥塞可能性，或流量疏通能力明显下降。R3级为一般级中继方向，该中继方向所属中继电路的中断将导致

少量网络路由迂回、增加流量拥塞可能性，或流量疏通能力下降；

2 R1 级重要性中继方向的中继电路的可用性不宜低于 99.999%，R2 级重要性中继方向的中继电路的可用性不宜低于 99.99%，R3 级重要性中继方向的中继电路的可用性不宜低于 99.9%；

3 具备条件时，R1 级、R2 级中继方向的中继电路可采用 MPLS TE FRR 等技术配置逻辑备份电路，备份电路和被保护电路的中间路由不应相同，备份电路应能实现在 50ms 内倒换；

4 核心汇接节点间的中继方向、互联互通的中继方向可为 R1 级重要性；

5 一般汇接节点至汇聚汇接节点或核心汇接节点、汇聚汇接节点至核心汇接节点的中继方向可为 R2 级重要性；

6 汇聚汇接节点之间、一般汇接节点之间、城域网内的中继方向可为 R3 级重要性。

4.3.6 公用互联网的中继电路组织应满足网络性能的要求，宜符合下列规定：

1 2 个城域网经由骨干网转接业务时，经过的骨干网汇接节点数量不宜超过 8 个；

2 用户在骨干网内到达互联互通节点、国际出入口节点所经过的骨干网汇接节点数不宜超过 4 个。

4.3.7 公用互联网的中继电路组织应和传输网络进行联合优化，宜符合下列规定：

1 中继电路组织应结合传输网络路由情况，减少业务流量在传输网络物理路径上迂回；

2 源自一个节点不同方向的中继电路宜采用不同的传输系统开通，并采用不同的光缆路由；

3 R2、R3 级中继方向的中继电路，在可用性符合第 4.3.5 条第 2 款要求且 IP 网络层面已经配置有一定可靠性措施时，可不要求传输网络为该中继电路提供保护机制。

4.4 中继电路带宽计算

4.4.1 公用互联网网络中继电路带宽计算可采用以下步骤：

1 预测网络流量；

2 估算网络节点间流量矩阵；

3 根据中继电路组织结果以及网络路由策略计算每条中继电路方向的流量；

4 配置中继电路带宽，并进行优化调整。

4.4.2 预测网络流量应考虑网络承载的所有各类用户和业务，网络流量可估算为各类用户网络流量之和。某一类用户的网络流量可按下式计算：

某类用户网络流量＝该类用户设计业务带宽×用户数×用户使用网络并发系数×统计复用系数 (4.4.2)

式中，用户使用网络并发系数应通过分析业务统计数据结合业务预测取定，一般范围在0.2～0.9；统计复用系数应通过分析业务统计数据结合业务预测取定，一般范围在0.2～0.9。

4.4.3 网络节点间流量矩阵估算可采用以下方法：

1 可根据网络流量预测结果结合历史统计流向数据推算；

2 缺乏流向统计数据时也可采用吸引系数法估算，并根据网络路由策略和网络中内容源分布适当调整。吸引系数法估算可按下式计算：

$$S_{(i,j)} = a_{(i,j)} \times \frac{S_i \times S_j}{\sum_{k=1,k\neq i}^{n} S_k} \tag{4.4.3}$$

式中：$S_{(i,j)}$——节点 i 到节点 j 的流量；

S_k——节点 k 的出流量；

n——节点数；

$a_{(i,j)}$——调整系数。

3 宜估算网络稳态情况下的流量矩阵。对于服务质量有特定要求的，流量矩阵可叠加网络部分中继电路中断时的迂回流量和逻辑备份电路的流量。

4.4.4 中继电路带宽应以计算得出的流量为基础，综合考虑网络设备端口带宽颗粒、传输网络带宽颗粒进行配置，宜符合下列规定：

1 稳态下中继电路的带宽平均峰值利用率可为45%～80%；

2 路由器和中继电路单点故障下中继电路的带宽平均峰值利用率不宜超过90%；

3 有特定服务质量需求的中继电路可采用轻载方式，带宽平均峰值利用率可为10%～40%；

4 同局向中继电路宜采用同类型端口，可采用链路捆绑、ECMP等技术进行配置以实现链路的负载均衡；

5 同局向中继电路流量需求超过3条155Mb/s电路时，宜直接配置2.5Gb/s带宽；

6 同局向中继电路流量需求超过2条2.5Gb/s电路时，宜直接配置10Gb/s带宽，超过4条GE电路带宽时宜直接配置10GE带宽；

7 同局向中继电路流量需求超过8×10Gb/s带宽时，宜直接配置100Gb/s带宽。

5 路由协议与路由策略

5.1 路 由 协 议

5.1.1 公用互联网网络可划分自治域，并宜符合下列规定：

1 骨干网、城域网可分别采用独立自治域设置。城域网规模较小时可不设置为独立的自治域，而是将其作为一个 IGP 路由域连接至骨干网；

2 不区分省际、省内子层次的骨干网宜采用单一自治域设置；

3 区分省际、省内子层次的骨干网中，省际骨干网和省内骨干网可分别采用独立自治域设置；

4 网络包含国际网络部分时，国际网络部分可纳入骨干网自治域。

5.1.2 公用互联网网络在自治域内应配置合适的域内路由协议，域内路由协议应采用动态路由机制，可选用 IS-IS 协议或 OSPF 协议。

5.1.3 公用互联网网络在自治域之间应配置合适的域间路由协议，域间路由协议应采用 BGP 协议。

5.1.4 用户接入可采用静态路由配置，有需求的用户接入也可采用 RIP、IS-IS、OSPF、BGP 等动态路由配置。

5.1.5 公用互联网网络配置的路由协议应具备同时支持 IPv4 和 IPv6 路由的能力。

5.2 路 由 策 略

5.2.1 路由策略设计应符合下列规定：

1 路由策略的实施应实现正确的路由信息接收与宣告；

2　路由策略的实施在保证网络结构的前提下，应避免网络中出现单故障点，提高网络的生存能力；

3　路由策略的实施应实现预期的路由选择方案，使网络业务流量合理分布在各条中继电路上；

4　路由策略应保证网络具有可扩展性，使得网络扩展后全部资源可以被优化利用；

5　路由策略应简洁、便于维护管理，对业务流量流向的变化应具有适应性，能够根据流量流向变化方便、快速地进行调整。

5.2.2　路由信息的接收与宣告应符合下列规定：

1　采用域内路由协议承载网络拓扑路由信息，并确定域间路由的下一跳信息；

2　可采用域间路由协议 BGP 承载外部网络路由信息及用户路由信息；

3　根据与其他网络的互联互通协议以及对用户的服务协议要求，正确地接收对方网络的路由信息及用户的路由信息，向对方网络正确宣告本网络的路由信息及用户的路由信息，并可采用 BGP 控制实现对接收、宣告的内容控制；宣告路由时应采用 CIDR 等方式进行路由聚合；接收路由时应控制外网路由信息的分布范围；

4　在域内和域间两类路由协议之间不宜互相注入路由信息。

5.2.3　流量流向规划与路由选择规则宜符合下列规定：

1　网络应进行流量流向规划，网络正常情况下应符合下列规定：

1）核心汇接节点之间的流量应在核心汇接节点之间内部疏导，不应经由汇聚汇接节点疏导；

2）汇聚汇接节点之间的流量应通过核心汇接节点之间疏导，不应通过一般汇接节点疏导，当汇聚汇接节点之间存在直连的时候，应优先选择直连电路疏导流量；

3）一般汇接节点之间的流量应通过汇聚汇接节点之间疏

导，当接入汇接节点之间存在直连的时候，应优先选择直连电路疏导流量；

4）根据所承载的业务情况，多条可选路由间可采用主备方式或分担方式规划流量疏通方案。

2 路由选择规则应与流量流向规划相匹配，可依据就近原则或指定路径原则制定。

3 路由选择规则的设计实现可采用下列方式：

1）合理设计域内路由协议的链路权值；

2）合理设计使用域间路由协议的各种属性赋值；

3）采用 MPLS TE 技术。

4 网络路由宜进行聚合。

5 网络中不应存在路由选择循环，并不应存在路由黑洞。

5.2.4 路由协议应正确进行运行参数属性设计，并应符合下列规定：

1 合理设计域内路由协议的分级或分区域；

2 合理确定网络中运行 BGP 协议的节点范围；

3 可采用 BGP 路由反射器技术，路由反射器可根据网络规模、管控需求分级、分区成组冗余设置；

4 合理运用路由协议的快速收敛技术；

5 可采用 BFD 快速故障检测技术；

6 可采用不间断转发、不间断路由技术。

5.2.5 网络可通过广域 SDN 技术，根据用户需求和全网的链路状态进行流量疏导。

6 网间互联

6.1 国内网间互联

6.1.1 不同经营者的公用互联网应在国内实现网间互联，可通过国内 NAP 或者网间直连电路实现互联。

6.1.2 互联地点不应少于 3 个不同城市，宜实现不同互联地点之间互联流量的疏通备份，互联设备应设置在骨干网的国内网间互联互通子层内。

6.1.3 根据业务需要，可设置省内网间互联电路用于疏通省内网间业务。

6.1.4 国内网间互联带宽应满足互联业务需要并保证互联服务质量。

6.1.5 国内网间互联应支持对来去流量进行计费或根据互联带宽进行计费，应支持对互联电路进行监控、管理和统计。

6.2 国际网间互联

6.2.1 有国际业务需求时，公用互联网可与国外公用互联网互联。互联应通过批准的国际出入口节点实现。

6.2.2 具备条件时，公用互联网可和 2 家或 2 家以上的国外公用互联网互联，实现互联网国际业务的疏通备份或分担。

6.2.3 国际网间互联带宽应根据业务需求双方协商确定，带宽应满足业务互通需要。

6.3 网间互联路由策略

6.3.1 根据业务需求，网间互联可采用转接方式或对等方式。

6.3.2 应合理设计网间互联路由策略，实现互联业务疏通的路由

优化，尽量减少不合理的互联业务路由走向，并有效利用互联带宽。

6.3.3 网间互联可对入网流量进行控制，主要可通过控制向互联对方网络宣告的路由信息内容、通过配置调整相应 BGP 路由的有关属性参数，引导入网流量。

6.3.4 网间互联可对出网流量进行控制，主要可通过配置 BGP 路由的有关属性参数、与互联对方网络协商有关 BGP 路由有关属性参数赋值含义及方式，引导出网流量。

7 网络管理

7.1 网管体系结构

7.1.1 公用互联网的网管体系结构可采用三级结构或两级结构，并宜符合下列规定：

1 采用两级网管体系时可设置骨干网网管中心和城域网网管中心，并宜符合下列规定：

1) 骨干网网管中心负责管理骨干网，可采用集中管理、省级分级操作的管理方式，同时在各省设置省级操作维护中心；

2) 骨干网网管中心可在异地设置备用网管中心；

3) 城域网网管中心负责管理城域网，城域网网管中心也可在省内全省集中设置；

4) 城域网网管中心与骨干网网管中心之间通过接口实现信息交互。

2 采用三级网管体系时可设置一级网管中心、二级网管中心和城域网网管中心，并宜符合下列规定：

1) 一级网管中心全国设置 1 个，负责省际骨干网络的管理；

2) 二级网管中心每省设置 1 个，负责省内骨干网络的管理；

3) 城域网网管中心负责管理城域网；

4) 各级网管中心之间通过接口实现信息交互。

7.1.2 网管中心与被管设备之间的网管信息通道宜优先采用带内方式，并应保证网管数据流的可靠传输，可同时提供带外网管通道作为应急备份。

7.1.3 网管中心可通过接口与综合网管系统实现连接，以实现综合的资源、故障、性能等管理功能，也可通过接口与其他支撑系统

连接。

7.2 网管接口

7.2.1 网管中心与被管设备之间的接口协议应符合下列规定：

1 应具备 SNMP 接口，提供配置、性能、故障管理等功能；

2 应具备流量流向统计接口，实现网络性能的监测、安全管理和计费管理等功能；

3 宜能详细记录系统活动日志，实现系统运行评估；

4 宜支持远程登录和虚拟终端功能；

5 宜支持远程主机之间的文件传输；

6 宜提供 XML 接口及配置模板，实现网管中心对被管设备的配置；

7 应支持 IPv4 单协议栈及 IPv6 单协议栈场景下接口通信，应同时支持 IPv4、IPv6 双协议栈场景下接口通信。

7.2.2 被管网络设备应支持通用的公有信息模型，应符合网管接口功能要求，可提供动态资源配置信息、实时告警信息、准实时性能信息、计费和安全信息、流量流向信息、QoS 和 LSP 管理信息、VPN 管理信息等。

7.3 网管功能

7.3.1 配置管理实现功能应符合下列规定：

1 可提供单点接入、日志采集与管理、自动巡检、局数据制作等功能；

2 应支持网元配置和管理，创建、删除、查询网络设备，查询设备内部的物理状态信息；

3 可支持业务配置和管理，支持有关业务相关参数的创建和修改；

4 应支持配置数据管理，支持对配置数据的合法性检查，自动生成配置数据，支持数据备份和恢复能力。

7.3.2 资源管理实现功能应符合下列规定：

1 应支持拓扑管理功能，支持拓扑编辑，支持拓扑自动发现、监视与浏览，支持不同层次的拓扑视图展示，实现基于拓扑的流量显示、资源显示、配置显示和故障显示等；

2 宜提供设备管理、电路管理、IP 地址管理、自治域号管理、软件版本管理等功能；

3 宜支持路由管理功能，可对网络中的路由实体进行监测，对网络路由信息及其变化情况进行分析；

4 宜提供资源报表统计、资源预警等功能。

7.3.3 故障管理实现功能应符合下列规定：

1 应支持告警的收集与显示、屏蔽与过滤、转发、确认与升级、存储与清除、查询与统计；

2 应支持对告警分类，可按严重等级划分；

3 应支持告警相关性抑制和故障定位。

7.3.4 计费管理实现功能应符合下列规定：

1 可通知用户所承担的费用或所消耗的资源；

2 可设置计费限量并使费率安排与资源的使用联系起来；

3 可把为获得一种给定的通信目标而调用多个资源的费用组合起来；

4 计费原始数据保存时限不应小于 5 个月。

7.3.5 性能管理实现功能应符合下列规定：

1 应支持大规模网络性能监控，支持设备监控、链路监控、服务质量监控，能及时了解设备健康状况、链路的资源利用情况和故障情况、监控分析业务质量；

2 应支持性能数据存储、查询，支持性能趋势分析，支持性能统计数据报表输出；

3 应支持性能门限管理，支持性能指标阈值告警。

7.3.6 安全管理实现功能应符合下列规定：

1 应具备用户管理功能，能提供基于控制点和角色的权限

控制；

2 应具备对系统操作日志记录功能，提供日志的管理和查询；

3 应能提供与安全有关事件的报告；

4 可通过访问控制和备份等手段保证网管数据安全。

7.3.7 流量流向分析实现功能应符合下列规定：

1 可支持不同统计粒度分析，并可支持多个网络设备输出的流量统计数据的收集、存储；

2 应支持过滤器定制，支持接收、拒绝特定类型的流量数据；

3 应支持聚合规则定制，支持按不同聚合规则聚合数据；

4 应支持对流量统计数据进行统计分析及其分析结果的图表方式呈现，支持流量排队分析、趋势分析、明细数据分析等。

7.3.8 QoS 管理实现功能宜符合下列规定：

1 可支持 DiffServ QoS 管理，并可支持 IP DiffServ、E-LSP 管理；

2 可支持 MPLS TE QoS 管理；

3 可支持 QoS 网络资源、QoS 策略自动发现；

4 可支持 QoS 策略的规划、部署、审计和监控；

5 可对流量按照特定规则进行分类，可实现基于类的流量监管、流量整形、拥塞管理、重新标记优先级等功能。

7.3.9 MPLS 管理实现功能应符合下列规定：

1 应支持 MPLS 网络资源、MPLS TE 隧道、静态 LSP 自动发现；

2 应支持 MPLS TE 网络拓扑自动发现；

3 可支持 MPLS 能力配置、LDP 能力配置、MPLS TE 能力配置；

4 可支持 MPLS TE 隧道端到端的规划、部署、审计和监控；

5 应支持静态 LSP 端到端的规划、部署、审计和监控，支持 LSP 拓扑显示、LSP 保护组管理、性能统计、支持 LSP 告警管理。

7.3.10 MPLS VPN 管理实现功能应符合下列规定：

1 应支持 VPN 网络资源、VPN 业务发现功能；

2 宜支持 VPN 业务规划、业务部署；

3 宜支持 VPN 业务配置审计、连通性审计、业务监控；

4 应支持 VPN 网络视图、客户视图显示；

5 应支持 VPN 性能统计、告警管理；

6 宜支持 VPN 客户管理，支持 VPN 客户 WEB 自助管理。

8 传送技术

8.0.1 公用互联网骨干网的传输网宜以光传送网为主构建，宜采用 IP over SDH、IP over DWDM(OTN)等技术，骨干网路由器可采用 SDH 帧结构、以太网帧结构或 OTN 帧结构进行传输，采用 SDH 帧结构时路由器的时钟同步定时系统应符合 SDH 系统对同步时钟的要求。

8.0.2 公用互联网城域网的传输网宜以光传送网为主，以其他方式为辅构建。

8.0.3 公用互联网网络内部采用的保护机制应和传送网的保护倒换机制进行协同。

8.0.4 公用互联网网络设备应可靠接入时间同步定时设备，可采用时间服务器和时间客户端工作方式，宜选 NTP 协议。

9 业务承载和接入

9.0.1 公用互联网可承载语音、数据和多媒体类业务，业务形式可包括网络接入类业务、资源出租类业务、能力服务类业务和应用内容类业务等。

9.0.2 公用互联网可配置接入设备实现网络接入类业务、配合实现资源出租类中的 VPN 业务等，并应符合下列规定：

1 公用互联网可与固定电话网、移动通信网互联，宜实现通过固定电话网、移动通信网接入；

2 公用互联网城域网可与各种接入网互联，应支持宽带接入方式、专线接入方式。

9.0.3 公用互联网可通过接入 IDC 提供资源出租类、能力服务类等业务。根据 IDC 业务量大小，可选择在核心汇接节点、汇聚汇接节点或一般汇接节点接入。

9.0.4 公用互联网可通过与叠加建设的各类业务网络互联，提供能力服务类和应用内容类等业务。业务网络设施可入驻在 IDC 中或作为独立系统接入。

9.0.5 公用互联网可叠加建设内容分发系统，引导业务内容在网络中的分布，改善用户使用体验。

9.0.6 公用互联网承载业务应根据各种业务的服务质量、可靠性、安全性等方面的要求，采用一定的承载技术实现。对于可靠性要求，可通过网络冗余等方式实现；对于安全性和服务质量要求，可通过网络承载隔离以及各种服务质量保证技术实现；业务有对时钟同步和对时间同步的传送需求时，有关网络设备应支持高精度时间同步协议。

9.0.7 公用互联网的业务承载能力应根据业务需求预测确定。

为保证网络易于扩展，网络设备的业务承载能力满足期可适当超前，网络中继电路的业务承载能力满足期超前不宜超过2年。

9.0.8 公用互联网业务运营所需的BSS、OSS系统宜与运营者的其他业务需求综合建设，并应能通过逐步扩展支持IPv6及向下一代互联网平滑过渡技术相关属性等方式，满足相应的业务运营需求。

9.0.9 公用互联网可综合采用隧道、翻译等机制，支持IPv4公网地址、IPv4私网地址、IPv6地址共存情况下的业务使用，可在城域网核心层或业务接入控制层部署CGN、AFTR等网络地址转换设备。

10 编号方案、地址分配与域名系统

10.1 编号方案

10.1.1 公用互联网的业务接入号码应合理规划，并应符合有关行业主管部门的要求。

10.1.2 公用互联网骨干网应采用公开的自治域号码，网内的其他独立自治域可采用公开自治域号码或私有自治域号码，私有自治域号码在内部应统一规划、分配，并应在网络互联出口过滤。

10.1.3 公用互联网提供 MPLS VPN 时，RT、RD 应由全网统一规划、分配。

10.2 地址分配

10.2.1 公用互联网的网络设备端口互联地址、网络设备管理地址、用户地址和业务地址等应统一规划，并应支持 IPv4 地址、IPv6 地址长期共存。

10.2.2 IP 地址规划分配应符合下列规定：

1 应根据网络规模、建设周期、业务发展等因素按需分配；

2 应尽量提高地址利用率；

3 可进行合理的地址预留；

4 应便于溯源；

5 IPv4 地址分配应符合下列规定：

1）应利用 CIDR、VLSM 等技术，分子网掩码时应保持地址的连续和路由表的优化；

2）宜保持地址分配的连续性，宜按地域分配连续的 IP 地址块；

3）在不影响业务开展的前提下，可规划和使用 IPv4 私有

地址。

6 IPv6 全球单播地址分配应符合下列规定：

1）IPv6 全球单播地址应包括全球路由前缀、子网 ID 和接口标识符部分，前缀和子网 ID 部分与接口标识符可按照 64/64 划分；

2）地址前缀规划应易于地址聚合，可基于相同地理位置、相同业务类型或者相同组织类别的子网使用相同前缀，应兼顾等级结构和扁平化寻址结构的使用；

3）接入用户宜根据规模需求不同采用下列地址块尺寸进行分配：/48、/56、/64、/128。

7 组播业务需要的组播地址可采用静态地址分配方法分配。

10.3 域名系统

10.3.1 公用互联网应根据业务需要对域名统一规划。

10.3.2 应根据业务和运营管理需要确定域名系统的层次，并可相应地设置各层次的域名服务器，具备条件的可引入域名根服务器镜像。

10.3.3 域名服务器部署应符合下列规定：

1 功能上应由权威服务器和递归服务器组成，两类解析服务器宜分离部署；

2 同一区的权威服务器不应少于 2 台，应支持域名解析的冗余、负荷分担，域名数据在各服务器上应主辅同步，各服务器应保持时间同步，可采用 NTP 协议；

3 同一服务域内的递归服务器应支持域名解析的冗余、负荷分担。

10.3.4 域名服务器宜采用双栈工作方式同时支持 IPv4 域名解析和 IPv6 域名解析。

10.3.5 域名服务器应保存解析日志，保存时长不应小于 3 个月。

11 网络性能与服务质量

11.1 网络性能

11.1.1 公用互联网骨干网的性能宜符合下列规定：

1 网内任意两个国内节点间忙时算术平均 IPTD 不宜大于 50ms(个别偏远节点除外)；

2 网内任意两个国内节点间忙时 IPDV 不宜大于 10ms；

3 网内任意两个国内节点间忙时 IPLR 不宜大于 0.1%；

4 网内任意两个国内节点间忙时 IPER 不宜大于 0.01%；

5 骨干网的 IGP 路由收敛时间不宜大于 30s。

11.1.2 公用互联网城域网的性能宜符合下列规定：

1 网内任意两个节点间忙时 IPTD(不包含接入链路)不宜大于 20ms；

2 网内任意两个节点间忙时 IPDV(不包含接入链路)不宜大于 5ms；

3 网内任意两个节点间忙时 IPLR(不包含接入链路)不宜大于 0.1%；

4 网内任意两个节点间忙时 IPER(不包含接入链路)不宜大于 0.01%。

11.2 服务质量

11.2.1 公用互联网接入类业务的服务质量宜符合下列规定：

1 接入连接建立成功率不应小于 95%；

2 用户接入认证平均响应时间不宜大于 8s。

11.2.2 公用互联网业务的计费准确率不宜小于 99.99%。

11.2.3 权威域名服务器的服务可用性不宜小于 99.999%，95%

域名解析请求的响应时间不宜大于500ms；递归域名服务器的服务可用性不宜小于99.99%，95%域名解析请求的响应时间不宜大于1500ms。

11.2.4 可根据业务需要对业务进行服务质量分级，可设置8个不同的质量服务等级，不同的业务可根据服务质量需求映射到这8个服务等级中。

11.2.5 可采用DiffServ、E-LSP和MPLS-TE等IP QoS技术实现服务质量保证。

11.2.6 宜部署服务质量监测平台为用户提供服务质量监测服务。

12 网络与信息安全

12.1 安全目标与框架

12.1.1 公用互联网的网络与信息安全目标应在合理的安全成本基础上，保证各类网元设备的正常运行，保证信息在网络上的安全传输，保障网络的运营维护管理安全，保障业务安全和内容安全，并应符合相关行业管理要求。

12.1.2 公用互联网的安全框架应由防护、检测与评估、响应闭环构成，并应符合下列规定：

1 防护部分应提供基本的安全技术和安全措施；

2 检测与评估部分宜实现对全网的实时监控，定期对全网进行安全扫描和风险评估，并将结果传给响应系统；

3 响应部分应能根据检测和评估结果，调整安全策略、产生安全告警、修补安全漏洞、进行安全加固等；

4 安全框架所需保障设施应与网络同步规划、设计、建设。

12.2 安 全 管 理

12.2.1 公用互联网宜设立安全管理中心，作为实现网络安全管理的技术平台。

12.2.2 安全管理中心的功能宜符合下列规定：

1 安全管理中心宜实现对各种 IP 安全工具的统一管理，并宜建立位于安全产品之上，面向管理层的监视、管理、统计、分析系统；

2 宜实现安全事件集中监控，并在各类安全设备、安全软件、系统软件之上建立安全事件的集中监控体系，实现安全事件的采集、处理、关联性定义、实时监控功能，提供安全设备部署的拓扑信

息，具有一定的安全事件的统计分析和报表功能；

3 宜建立信息资产与安全风险管理中心，统一管理信息资产的识别、赋值、建档、变更、停用等活动，并对资产进行的漏洞和风险评估结果进行管理，同时提供统计分析功能，为建立统一的信息资产安全管理和信息安全风险评估与管理体系提供支撑；

4 宜实现安全策略管理，实现安全配置管理，根据安全检测和评估结果调整安全策略，实现有关的安全配置；

5 宜实现安全事件预警，提供安全趋势分析和预警机制；

6 宜建立安全信息库，积累安全管理相关知识经验，为形成专家知识库提供基础；

7 宜实现与其他管理信息系统的信息交换。

12.3 内 容 安 全

12.3.1 公用互联网应在业务的审核、检查、拨测等环节部署内容安全管理和技术手段。

12.3.2 公用互联网宜在 IDC 出口处、网间互联处和网络内不同层次之间设置流量检测与控制系统，应主要实现下列功能：

1 异常流量检测及控制；

2 不良信息检测及控制。

12.4 业 务 安 全

12.4.1 公用互联网的用户信息应加密存储，访问用户信息应进行权限控制。

12.4.2 用户使用公用互联网接入业务应可溯源，网络接入访问日志记录保存不应少于 6 个月。

12.4.3 公用互联网接入、承载的业务系统应符合下列规定：

1 应划分安全域，应配置防火墙进行安全域边界控制；

2 业务提供、控制与管理过程应保护用户隐私，不泄漏用户相关敏感信息；

3 业务控制与管理应提供并启用身份鉴别、标识唯一性检查、鉴别信息复杂度检查及登录失败处理功能；

4 业务控制与管理应严格限制默认账号的权限，各账号应依据最小授权原则授予完成各自承担任务所需的权限，按安全策略要求控制对文件、数据库表等内容的访问；

5 系统访问控制策略应由授权主体配置；

6 业务控制与管理应提供覆盖到每个账号的安全审计功能，应保证无法删除、修改或覆盖审计记录，业务相关审计记录的内容至少应包括事件日期、时间、发起者信息、类型、描述和结果等；

7 宜对业务及应用相关通信过程中的关键报文或会话过程提供必要的保护，并提供业务及应用相关访问、通信等数据的防抵赖功能；

8 宜对业务及应用服务水平进行检测，具有当服务水平降低到预先规定的阀值时进行告警、控制的功能。

12.5 网络安全

12.5.1 公用互联网应从控制、管理和数据三个层面保障自身安全。

12.5.2 公用互联网应在域内路由协议和域间路由协议中启用校验和认证功能，保证路由信息的完整性和已授权性。

12.5.3 在网络关键节点，可根据源地址及端口、目的地址及端口以及协议类型等参数实施 ACL，可根据路由表中的网段和物理接口实施 uRPF。

12.5.4 网络设备应支持对自身的访问控制和访问日志记录功能。

12.5.5 网络设备的远程维护应使用加密协议。

12.5.6 网络设备应关闭未使用的功能和服务。

12.5.7 网络设备应关闭未使用的 SNMP 协议和未使用的读写权限。

12.5.8 网络的域名服务器应实现域名数据安全和解析安全。

13 设备配置原则

13.0.1 网络各节点配置的主要网络设备可包括路由器、交换机等设备。配套设备可包括设备机架、电源架、配线架等。

13.0.2 设备配置应以近期需求为基础，兼顾远期业务发展的需要。选用的设备应性能稳定、安全可靠、技术先进、兼容性好、能效比好、模块化、扩展性强，具备在线升级能力。

13.0.3 采用的各种网络设备应符合有关的设备技术规范，并应符合下列规定：

1 应符合下列能耗管理要求：

1) 对于机框插槽式设备，应有高温报警功能；

2) 对于机框插槽式设备，应具备能源监控及管理功能；

3) 对于机框插槽式设备，应支持通过命令行或网管工具远程关闭设备部分模块或功能，或进入微电状态；

4) 对于机框插槽式设备，应支持根据实际情况动态调整风扇转速；

5) 宜具有可根据用户需求和不同应用场合配置交流或直流供电的选择；

6) 设备内部应有合理的气流组织。

2 应符合下列环保与包装要求：

1) 设备的主要部分应减少铅、镉、汞、六价铬、溴化阻燃剂等有害物质；

2) 应采用用量最少的适度包装，包装材料对人体和生物应无毒无害，包装应易于重复利用或易于回收再生，包装废弃物可以降解腐化。

13.0.4 路由器设备配置应符合下列规定：

1 应在完成网络节点局域网结构设计的基础上配置路由器设备；

2 应充分考虑该节点在网络中的位置和功能，所配置的路由器设备的功能与性能应与其在网络中的角色一致；处理的业务量相对设备能力较小时，一台路由器设备也可兼做两种功能角色；

3 当一个节点存在多条对外连接中继电路、节点配置多台路由器设备时，应注意对整体网络结构的影响以及对流量流向规划的影响；

4 骨干网路由器设备和城域网核心层路由器设备的主控板卡、交换板卡、电源模块、风扇模块等关键部件应冗余配置，应支持热备份功能和热插拔功能；

5 路由器设备的接口板应根据网络中继电路设计情况进行配置；当一个节点存在多条对外连接中继电路时，电路与接口板的对应应考虑安全可靠性要求；

6 国际出入口节点的国际出入口路由器设备应单独配置，不与其他功能路由器合设；

7 路由器设备应同时支持 IPv4 和 IPv6 协议栈。

13.0.5 业务接入控制系统设备配置应符合下列规定：

1 业务接入控制系统设备可由一台设备完成，也可单独设置为业务路由器 SR 或宽带接入服务器 BRAS；

2 SR 可主要作为用户专线接入网络的网关、MPLS VPN PE、组播网关等，BRAS 可主要作为用户宽带接入网络的网关、组播网关等；

3 SR、BRAS 应实现对用户的接入及接入认证控制、QoS 策略控制和计费统计等功能；

4 SR、BRAS 应以综合成本最低为原则，考虑传输资源条件和用户数量部署；对于中、大规模的城域网，宜在汇聚层分布配置，小规模的城域网可在核心层集中配置；接入重要业务的 SR 可单独设置，并可直接接入骨干网一般汇接节点；

5 SR(BRAS)宜成对设置，成对的 SR(BRAS)之间宜互为冗余备份，可同机房或不同机房设置。

13.0.6 设备机架、电源架、配线架等配套设备应根据工程实际需要配置。

13.0.7 备品备件的配置应根据设备的重要性、故障率以及工程售后服务内容确定，宜采用集中备件方式。

14 机房设计

14.0.1 网络设备应选择安装在便于与传送网连接、便于维护管理的通信机房内，机房设计应符合现行行业标准《通信建筑工程设计规范》YD 5003 和《通信局（站）节能设计规范》YD/T 5184 的规定。

14.0.2 机房的工作地、保护地、建筑防雷接地应符合现行国家标准《通信局（站）防雷与接地工程设计规范》GB 50689 的规定。

14.0.3 设备安装应符合现行行业标准《电信设备安装抗震设计规范》YD 5059 的规定。

14.0.4 设备机房的防火措施应符合现行国家标准《建筑设计防火规范》GB 50016 的规定。

本标准用词说明

1 为便于在执行本标准条文时区别对待，对要求严格程度不同的用词说明如下：

1）表示很严格，非这样做不可的：

正面词采用“必须”，反面词采用“严禁”；

2）表示严格，在正常情况下均应这样做的：

正面词采用“应”，反面词采用“不应”或“不得”；

3）表示允许稍有选择，在条件许可时首先应这样做的：

正面词采用“宜”，反面词采用“不宜”；

4）表示有选择，在一定条件下可以这样做的，采用“可”。

2 条文中指明应按其他有关标准执行的写法为：“应符合……的规定”或“应按……执行”。

引用标准名录

《建筑设计防火规范》GB 50016
《通信局(站)防雷与接地工程设计规范》GB 50689
《通信建筑工程设计规范》YD 5003
《电信设备安装抗震设计规范》YD 5059
《通信局(站)节能设计规范》YD/T 5184