

附件二：

ICS

HJ

中华人民共和国国家环境保护标准

HJ/T ××××—××××

环境信息网络建设规范

Construction specification for environmental information network

(征求意见稿)

20□□-□□-□□发布

20□□-□□-□□实施

环 境 保 护 部 发布

目 次

前 言	II
1 适用范围	1
2 规范性引用文件	1
3 术语和定义	1
4 缩略语	2
5 全国环境信息网络建设原则和基本流程.....	2
6 全国环境信息骨干网网际互连.....	3
7 全国环境信息局域网网络建设.....	9
8 全国环境信息网络机房建设.....	14
9 全国环境信息网络验收测试标准.....	21
附 录 A（规范性附录） 全国环境信息网络系统域名命名规则	29
附 录 B（规范性附录） 全国环境信息网络 IP 地址规划表.....	31
附 录 C（资料性附录） 路由器性能指标	32
附 录 D（规范性附录） 防火墙安全等级划分	33
附 录 E（资料性附录） 防火墙性能指标	35
附 录 F（规范性附录） 对不同高度房间的火灾探测器的选择.....	36
附 录 G（资料性附录） 感烟、感温探测器的保护面积和保护半径	36

前 言

为加强对全国环境信息网络建设的统一规范，保障环境业务数据的有效传输和信息共享，实现全国环境保护部门网络的互联互通，制定本标准。

本标准规范了全国环境信息网络建设的原则、基本流程；骨干网络建设、局域网络建设；IP地址和域名的规划以及机房建设的技术要求。

本标准附录A、附录B、附录D、附录F为规范性附录，附录C、附录E、附录G为资料性附录。

本标准首次发布。

本标准为指导性标准。

本标准由环境保护部科技标准司提出。

本标准主要起草单位：环境保护部信息中心。

本标准环境保护部20□□年□□月□□日批准。

本标准自20□□年□□月□□日起实施。

本标准由环境保护部解释。

环境信息网络建设规范

1 适用范围

本标准规定了全国环境信息三级骨干网络网际互连，中华人民共和国环境保护部（以下简称环境保护部）、各省级和市级环境保护部门内部局域网建设、机房建设和管理、以及网络测试方面的基本要求和技术指标。

本标准适用于环境保护部，全国省、自治区、直辖市、新疆生产建设兵团和市级环境保护部门；县级环境保护部门及各级环境保护部门直属单位亦可参照执行。

2 规范性引用文件

本标准内容引用了下列文件中的条款。凡是不注日期的引用文件，其有效版本适用于本标准。

GB/T 19668 《信息化工程监理规范》

GB/T 20281-2006 信息安全技术—防火墙技术要求和测试评价方法

GB/T 20275-2006 信息安全技术—入侵检测系统技术要求和测试评价方法

GB/T 20278-2006 《信息安全技术 网络脆弱性扫描产品技术要求》

GB/T 20280-2006 《信息安全技术 网络脆弱性扫描产品测试评价方法》

GB/T 50311-2000 建筑与建筑群综合布线系统工程设计规范

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 1099-2001 千兆以太网交换机设备技术规范

YD/T 1170-2001 IP网络技术要求-网络总体

YD/T926.1-2001 大楼通信综合布线系统第1部分：总规则

YD/T926.2-2001 大楼通信综合布线系统第2部分：综合布线用电缆、光缆技术要求

YD/T926.3-2001 大楼通信综合布线系统第3部分：综合布线用连接硬件技术要求

ISO/IEC 11801-2002 建筑物通用布线国际标准

3 术语和定义

下列术语和定义适用于本标准。

3.1

环保系统电子政务内网

全国环境保护系统各级环境保护局建设的用于电子公文传输、内部政务管理以及内部信息服务等的网络。电子政务内网为独立的网络，必须与互联网和电子政务外网物理隔离。

3.2

环保系统电子政务外网

全国环境保护系统各省、市、自治区环境保护局内部局域网通过专线互连，用于污染源监测数据传输、环保系统综合业务平台、以及数据共享的网络。电子政务外网为全国性互连网络，该网络必须与互联网安全隔离。

3.3

环保系统城域网

指环境保护部连接其在京环保单位所形成的网络；各省、自治区环境保护局连接其同城环境保护单位所形成的网络；直辖市、各城市级环境保护局连接其同城环境保护单位所形成的网络。

3.4

国家级环境信息广域网

指环境保护部通过专线连接全国各省、自治区、直辖市环境保护局所形成的广域网。

3.5

省级环境信息广域网

指省级环境保护局通过专线连接省、自治区内各城市级环境保护局所形成的广域网。

4 缩略语

DMZ	非军事区	Demilitary Zone
DNAT	目的网络地址转换	Destination NAT
DNS	域名系统	Domain Name System
FTP	文件传输协议	File Transfer Protocol
HTTP	超文本传输协议	Hypertext Transfer Protocol
ICMP	网间控制报文协议	Internet Control Messages Protocol
IDS	入侵检测系统	Intrusion Detection System
IP	网际协议	Internet Protocol
NAT	网络地址转换	Network Address Translation
POP3	邮局协议3	Post Office Protocol 3
SMTP	简单邮件传送协议	Simple Mail Transfer Protocol
SNAT	源网络地址转换	Source NAT
VLAN	虚拟局域网	Virtual Local Area Network
VPN	虚拟专用网	Virtual Private Network

5 全国环境信息网络建设原则和基本流程

5.1 网络建设原则

网络建设应根据以下主要原则组建：

- 应满足各政务部门的应用业务系统的要求；
- 应利用已有的网络资源，与已有的专用政务网络兼容；
- 电子政务网络体系结构应以 TCP/IP 互连技术组建，即三层及三层以上统一采用 TCP/IP 协议栈，各种物理传输媒体之上采用多种协议栈的形式支持统一的 IP 层协议；
- 应根据应用业务系统及安全保障的不同需求，满足可分级管理和控制等特殊需要，采用分布式组织架构进行分级、分权的管理；
- 应是安全可靠、可管理、可控制和可扩展的网络，应具有服务分类和服务质量保障能力。

5.2 网络建设基本流程

全国环境信息网络建设应该经过立项阶段、确定监理公司及签订合同、招标投标阶段、工程设计阶段、工程实施阶段、工程验收阶段和运行及维护阶段。

5.2.1 立项阶段

立项及可行性研究阶段在环境信息网络建设的整个生命周期中，属于前期阶段。网络建设项目的建设方须向相应的政府管理部门提交立项申请报告及可行性研究报告，待相应部门批准及项目资金到位后，开展下一阶段的项目招投标工作。

立项阶段需编制立项申请报告和项目可行性研究报告。报告应依据主管部门的要求和适用的技术标准编制。

5.2.2 确定监理公司及签订合同

根据《国务院信息化工作办公室、科学技术部、信息产业部关于印发《电子政务工程技术指南》的通知》（国信办〔2003〕2号）的第十六条规定：“电子政务工程建设要按照信息产业部《信息系统工程监理暂行规定》（信部信〔2002〕570号），加强电子政务工程监理市场的规范化管理，确保电子政务工程的安全和质量。从事电子政务工程监理活动的单位要具备信息产业部信息工程工程的相应资质，同一工程的建设和监理要由相互独立的机构分别承担，监理单位要先于承建单位介入，没有确立监理单位的工程，建设单位不得开始建设。”，在招投标确定承建方之前，应确定监理合同，以便在技术上得到支持。监理合同在工程中作用，可见GB/T 19668 《信息化工程监理规范》

5.2.3 招标投标阶段

为了规范环境信息网络建设工程建设项目施工招标投标活动，所涉及的法规、管理规定和技术标准包括：

- 《工程建设项目施工招标投标办法》；
- 《计算机信息系统集成资质管理办法》；
- 工程建设项目符合《工程建设项目招标范围和规模标准规定》（国家计委令第3号）规定的范

围和标准的，必须通过招标选择施工单位。任何单位和个人不得将依法必须进行招标的项目化整为零或者以其他任何方式规避招标；

- d) 涉密系统集成单位必须经过保密工作部门资质认定，并取得《涉及国家秘密的计算机系统集成资质证书》，涉密系统建设单位应选择具有《涉及国家秘密的计算机系统集成资质证书》的集成单位来承建涉密系统；

- e) 相关技术标准。

5.2.4 工程设计阶段

环境信息网络系统工程的设计阶段是保证工程质量的关键性环节，工程管理方应该重视工程设计的重要性。承担工程设计任务的单位可以是：建设方、相关咨询或设计方、承建方。建设方可以根据工程实际情况来选择设计方。承建方、建设方和监理方在网络建设工程设计应当遵循国家标准、行业标准和地方标准，并符合网络建设工程招标文件的要求。

5.2.5 工程实施阶段

环境信息网络建设工程实施应当符合国家标准、行业标准和地方标准，符合网络建设工程设计方案的要求。

5.2.6 工程验收阶段

重大项目的竣工验收，必须有信息化主管部门、质量技术监督部门推荐的专家参与评审；其他项目的竣工验收，建设单位应当根据工程备案管辖邀请市或者区、县信息化主管部门参加。重大项目在验收前应当通过国家指定的测评认证机构的测试，未经测评认证的，不予验收。信息网络建设工程验收应当符合国家标准、行业标准和地方标准，符合信息化工程招标文件的要求，涉及保密和隐蔽工程的验收参照相关规定。从事工程验收设计的单位，应当执行有关的国家标准、行业标准和地方标准。主管部门要在信息化建设中遵循《电子政务标准化指南》和《电子政务标准体系》。

5.2.7 运行及维护阶段

网络维护是环境信息网络正常运行的保证，必须给予充分的重视，并从人员、规章制度和资金等各个方面作好相应的安排。应建立网络建设工程质量保修制度。承建方应按合同，履行保修责任。保修期自工程竣工验收合格之日起不得少于两年。

6 全国环境信息骨干网网际互连

6.1 网络结构及拓扑

全国环境信息网络结构可分为三级网络，一级骨干网主要负责环境保护部至各省级、自治区、直辖市和新疆建设兵团环保局的网络互连；二级网络主要负责各省级、自治区至其所属城市环保局的网络互连和直辖市至其所属区、县级环保局的网络互连；三级网络主要负责各城市至其所属县、区级环保局的网络互连。环境保护部为一级骨干网络核心节点，各省级、自治区、直辖市环保局为二级网络核心节点，各市级环保局为三级网络核心节点。

全国环境信息网络分为四级节点：环境保护部为一级节点，各省级、自治区、直辖市环境保护局为二级节点，各城市环境保护局为三级节点，各区、县环境保护局为四级节点，各级环境保护局直属单位可以根据其业务需要由各级环保局自行规划建设。

6.1.1 互联网网际互连网络结构及拓扑

互联网接口为全国各级环保部门连接国际互联网的出口，内部局域网（外网）为星型拓扑结构。

6.1.2 广域网网络结构及拓扑

全国环境信息广域网络主要包括环境保护部与各省级、自治区、直辖市、新疆生产建设兵团环保局的网络互连（一级网络），各省级、自治区、新疆建设兵团与其所属城市级环保局的网络互连（二级网络），各直辖市、城市至其所属县、区级环保局的网络互连（三级网络），广域网为星型拓扑结构。

6.1.3 城域网网络结构及拓扑

全国环境信息城域网网络主要包括：各级环保部门至同城直属单位的网络互连，城域网为星型拓扑结构。

6.2 链路和带宽

6.2.1 互联网链路和带宽

互联网的链路由运行商提供，互联网的带宽由业务需求而定，以下为带宽升级的参考标准：

当一条链路具有高的利用率，由于优先级高的流量还可以被正常的路由，业务应用质量还不是问题，Ping测试时所经历的延迟也不显著。在这些情况下，可以不必升级带宽。但是，如果优先级高的流量的可用带宽接近带宽的极限，那么就需要开始考虑升级带宽了。如果网络正常业务流量长时间达到整个互

联网带宽的70%，并且关键业务应用明显受到影响，在Ping测试时所经历的延迟显著，并伴随一定的丢包率，则须考虑互联网带宽升级。

6.2.2 城域网链路和带宽

环境保护部与在京环保单位的网络互连应采用专线连接，带宽不低于2M，总局连接总局信息中心数据中心带宽不低于100M。

各省级、自治区、直辖市、新疆建设兵团与其同城环保单位的网络互连可采用专线连接，带宽不低于2M。

6.2.3 广域网链路和带宽

环境保护部与各省级、自治区、直辖市、新疆建设兵团环保局的网络互连线路（一级网络）采用专线连接，带宽不低于6M。

各省级、自治区与其所属城市级环保局的网络互连（二级网络）可采用专线连接，带宽不低于2M。

各城市至其所属县、区级环保局的网络互连（三级网络）可采用VPN技术，带宽不低于512K。

6.3 网络接入设备标准

6.3.1 接入设备

6.3.1.1 互联网接入设备

互联网接入路由器可选择支持百兆带宽的中低端路由器。

6.3.1.2 城域网接入设备

全国环境信息城域网接入设备等级主要由设备所在节点角色功能来决定。环境保护部与在京环保单位的网络互连，总局为一级核心节点，采用高端路由器，各在京环保单位可采用低端路由器。各省级、自治区与同城环保单位的网络互连，各省、自治区环境保护局为二级核心节点，采用中高端路由器，各同城环保单位可采用低端路由器。

6.3.1.3 广域网接入设备

全国环境信息广域网主要包括环境保护部与各省级、自治区、直辖市环境保护局的网络互连（一级网络），总局为一级节点，应采用高端路由器。各省级、自治区与其所属城市级环境保护局的网络互连（二级网络），各省级、自治区、直辖市环境保护局为二级节点，采用中高端路由器，各城市级环境保护局采用低端路由器。

6.3.2 接入设备标准

6.3.2.1 高端路由器

高端路由器通常位于骨干网接入节点，为骨干网转发数据提供路由处理能力和传输带宽。

1. 高端路由器功能主要包括：

- a) 路由器的功能特性
- b) 通信规程
- c) 协议要求
- d) 路由协议
- e) 接口类型
- f) 网管协议等

2. 高端路由器性能指标主要包括：

- a) 吞吐量
- b) 丢包率
- c) 包转发率
- d) 可靠性和安全性
- e) 路由表容量
- f) 接口转发时延等

有关高端核心路由器的详细要求见YD/T 1097-2001，《路由器设备技术规范-高端路由器》。

6.3.2.2 低端路由器

低端路由器一般位于网络边缘，是通过数据转发包来实现连接一级网与二级网的路由器。

1. 高端路由器功能主要包括：

- a) 路由器的功能特性
- b) 通信规程
- c) 协议要求

- d) 路由协议
- e) 接口类型
- f) 网管协议等

2. 高端路由器性能指标主要包括：

- a) 接口转发时延
- b) 丢包率
- c) 包转发率
- d) 内存容量等

有关低端核心路由器的详细要求见YD/T 1096-2001，《路由器设备技术规范-低端路由器》。路由器性能指标转请参见附录C 路由器性能指标

6.4 网络安全设备标准

6.4.1 安全设备

6.4.1.1 互联网安全设备

互联网接入的安全设备可以选择支持百兆带宽的中低端防火墙。并可根据实际情况部署入侵检测设备、上网行为管理设备、流量管理设备等安全产品。

6.4.1.2 广域网和城域网安全设备

在全国环境信息广域网和城域网建设中网络安全设备主要是指防火墙设备，入侵检测系统和网络脆弱性扫描系统。环境保护部、各省级、市级环保局必须在网络节点部署防火墙、入侵检测系统和网络脆弱性扫描系统，区、县级环保局可以采用软件防火墙。

6.4.2 防火墙设备标准

防火墙作为一个或一组在不同安全策略的网络或安全域之间实施访问控制的系统，通用技术要求分为功能、性能、安全和保证要求四大类。

1. 防火墙设备主要功能如下：

- a) 包过滤
- b) 应用代理
- c) 内容过滤
- d) NAT
- e) 动态开放端口
- f) VPN
- g) 安全审计
- h) 安全管理等

2. 防火墙设备主要性能指标如下：

- a) 吞吐量
- b) 延迟
- c) 最大并发连接数
- d) 最大连接速率

3. 安全要求是对防火墙自身安全和防护能力提出具体的要求，例如：

- a) 抗渗透
- b) 恶意代码防御
- c) 系统应构建于安全增强的操作系统之上

4. 保证要求则针对防火墙开发者和防火墙自身提出具体的要求，例如：

- a) 管理配置
- b) 交付与操作
- c) 指南文件等

防火墙等级分为一级、二级、三级三个逐级提高的级别，功能强弱、安全强度和保证要求高低是等级划分的具体依据。安全等级突出安全特性，性能高低不作为等级划分依据。详细划分情况见：附录D 防火墙安全等级划分

有关防火墙设备要求详见：GB/T 20281-2006《信息安全技术 防火墙技术要求和测试评价方法》

6.4.3 入侵检测设备标准

入侵检测设备可分为主机型入侵检测系统和网络型入侵检测系统，可划分为三个等级。三个逐级提高的级别，功能强弱、安全强度和保证要求高低是等级划分的具体依据。

1. 入侵检测设备主要功能如下：

- a) 数据探测
- b) 入侵分析
- c) 入侵响应
- d) 管理控制
- e) 检测结果处理
- f) 安全审计

2. 入侵检测设备主要性能指标如下：

- a) 误报率
- b) 漏报率

有关入侵检测系统要求详见：GB/T 20275-2006 《信息安全技术 入侵检测系统技术要求和测试评价方法》

6.4.4 网络脆弱性扫描系统

网络脆弱性扫描是网络安全防御中的一项重要技术，其原理是对采用的安全策略和规章制度进行评审，发现不合理的地方，采用模拟攻击的形式对目标可能存在的已知网络脆弱性进行逐项检查，确定存在的安全隐患和风险级别。使用网络脆弱性扫描产品可自动对计算机系统进行安全评估分析，对网络进行检查，发现其中可能被利用的脆弱性，并提出解决的建议或自动进行修复，提高网络系统的安全性能，达到在入侵发生之前及时弥补系统及网络安全脆弱性，消除入侵隐患的目的，保证网络安全的运行。

网络脆弱性扫描主要功能如下：

- a) 自身安全要求
- b) 脆弱性扫描
- c) 网络旁路检查
- d) 信息获取
- e) 端口和服务扫描
- f) 授权管理员访问
- g) 扫描结果分析处理
- h) 扫描策略定制
- i) 扫描对象的安全性等

网络脆弱性扫描主要性能指标如下：

- a) 速度
- b) 稳定性
- c) 容错性

有关网络脆弱性扫描产品详见：GB/T 20278-2006 《信息安全技术 网络脆弱性扫描产品技术要求》和GB/T 20280-2006 《信息安全技术 网络脆弱性扫描产品测试评价方法》。

6.5 网络管理平台标准

6.5.1 网络管理软件系统平台主要功能要求

全国环境信息网络网管系统主要功能包括：故障管理、性能管理、拓扑管理、综合视图呈现等。

6.5.1.1 故障管理

- a) 网络全面监控，集成整个网络的告警/故障事件信息，统一处理、呈现和分析告警/故障事件信息，以便提高网络事件处理效率。
- b) 实现告警/故障事件信息的实时交换，通过将这些事件信息进行集中的相关性和关联性分析，可以使操作维护人员迅速找到根源问题所在，并能够通过这些相关联的事件信息，确定对网络承载业务的影响情况。

6.5.1.2 网络性能管理

- a) 通过专用网络管理工具监测网络性能，对全国环境信息网络运行状况进行监控，通过性能管理，判断网络的运行质量、运行效率、流量流向以及连通率水平等。网络性能监控制定性能测量的标准和手段，分析网络服务的趋势和行为，在发现性能下降时立即报告，使管理员及时采取措施进行处理。

- b) 生成的性能报告必须提供实时和历史的性能报告，可以实时查看每个性能当前的状态和服务水平状态，并查看详细的性能曲线，报告包括小时、三小时、天、周、月报表。性能报表可以按照每个配置文件的要求分发到相应的Web站点上。运行在不同地点的监视器报表可以汇集到某个集中的地点，从而可以完整地反映出服务的性能状况。

6.5.1.3 网络拓扑管理

- a) 网络拓扑管理系统能提供准确的网络三层、二层连接视图，可以清楚的反映网络实际的物理连接，发现网络拓扑结构包括网络所有节点之间的连接关系，如交换机划分的VLAN、每个VLAN包含的端口、端口连接的节点，路由器的端口，其连接的设备，服务器或PC地址、连接在交换机的哪个端口上，通过这些网络连接信息构建完整的网络拓扑视图。在其拓扑图中，可以准确的标识出PC或服务器是通过哪个交换机进行连接，属于交换机的哪个VLAN，交换机与路由器之间是如何连接的，而且精确到物理端口一级。
- b) 网络拓扑管理系统能针对不同用户，定制用户的拓扑查看权限。

6.5.1.4 综合视图呈现

网络管理软件系统综合视图呈现须具备以下特点：

- a) 灵活直观，根据管理需要和习惯定义适合客户的实时监控界面，这种界面可以综合网络的信息，而不是单个功能的简单呈现，因此管理界面可以更加切合运维的监控需要和领导了解全网状况的需要
- b) 集成，由于采用浏览器界面，不同的管理功能之间更容易集成，可以真正建立网管的统一界面，并实现不同功能的互操作。
- c) 分权，不同的管理人员根据管理权限和职能，可以定义不同的管理界面，可以使用的工具，可以查看的事件，可以访问的拓扑等等。这种分权管理能力，可以充分保证国家环保局网络管理分布式管理的需要，可以充分支持不同网络的分权管理，保证每个操作维护人员只查看和处理自己的拓扑信息、事件信息。实现各网络设备的统一管理。

6.6 网络互连协议及典型业务协议

全国环境信息网络骨干网网际互连协议选择TCP/IP协议，并基于TCP/IP协议可以开展如下典型业务。

1. Web业务

- a) 基本技术
基于Web技术，为了增强多媒体检索的功能，采用JAVA、公共网关接口（CGI）等技术，以适合各种场合的需要。
- b) 协议及标准
通信协议：超文本传送协议（HTTP）。
- c) 多媒体信息检索业务可应用于：新闻、信息查询、课程培训、文化教育、法律、法规、广告等。

2. E-mail

- a) 基本技术
利用电子邮件技术
- b) 协议及标准
通信协议：简单邮件传输协议（SMTP）、POP3。
- c) 电子邮件业务可应用于：接收信件、发送信件、文件转发等。

3. FTP

- a) 基本技术
利用异地主机的FTP文件交换或用Telnet仿真终端接入，完成远程异地科学计算及信息处理。
- b) 协议及标准
通信协议：FTP等。
- c) 科学计算及信息处理业务可应用于：翻译业务、软件共享业务、远程计算机辅助设计业务等。

4. 虚拟专用网（VPN）业务

- a) 基本技术
在IP网上实现VPN业务，就是使用加密的IP隧道，实现专有IP包和其他网络协议（IPX、NetBEUI等）包在Internet上传输，从而实现不同的虚拟专用网（VPN）。
- b) 协议和标准

点对点隧道协议：点到点隧道协议（PPTP）。
第二层隧道协议：第2层隧道协议（L2TP）。
第三层隧道协议：通用路由协议GRE（参见RFC 1071/1072）。
IP安全协议：IPSec协议。

c) 虚拟专用网（VPN）业务可应用于：内联网互连、外联网互连、远程用户接入等。
有关IP VPN业务的具体要求参见相关的标准。

5. 多媒体会议业务

a) 基本技术

基于TCP/IP的会议业务。由于LAN上业务质量得不到保证，因而图像编码和语音编码都要尺度可伸缩的。为保证实时及同步的要求，实时信息（视频音频）RTP、RTCP、UDP协议栈，数据信息用TCP协议栈。为了进一步保证一定的质量，要有一定的信道带宽预约机制。

b) 协议和标准

通信协议：H. 323、H. 225、RTP、UDP、HTTP。

服务质量协议：RSVP、Diffserv。

语音编码协议：G723.1、G. 729。

图像编码协议：H. 263。

多点会议协议：T. 120协议、T. 130协议。

c) 多媒体会议业务可应用于：专网或虚拟专网中的多媒体会议业务、公众多点多媒体会议业务等。

6.7 全国环保系统 IP 地址规划

6.7.1 原则

a) 国家电子政务网络地址统一规划，中央和地方分级管理，支持各部门、各地方网络的互连

b) IP 地址的分配应具有层次性、连续性，以提高IP 地址利用率、减少路由表表项；

6.7.2 政务内网地址

政务内网网络地址分为三类：系统地址、共享地址和互联地址。各部门内部网络使用系统地址，部门间、系统间网络互通使用共享地址或互联地址。

a) 系统地址：是指部门内部网络的设备地址和接入政务内网所需使用的地址，包括个人主机地址、部门网络设备地址、部门应用服务器地址等。

b) 共享地址：是指用于政务内网中提供信息服务的主机地址。

c) 互联地址：包括链路地址（网络设备间的点对点互联地址）和设备管理地址。对未使用本规划地址的网络设备，在连接政务内网进行设备地址转换时，采用互联地址。互联地址分配到用户接入设备的上连（网络侧）端口，不包含用户内部网络接入政务内网所使用的地址。

6.7.3 政务外网地址

政务外网的网络地址包括用户地址和互联共享地址。各部门内部网络使用用户地址，部门间、系统间网络互通使用互联共享地址。

a) 用户地址：是指部门内部网络的设备地址和接入政务外网所需使用的地址，包括个人主机地址、部门网络设备地址、部门应用服务器地址等。此地址作为政务外网内部地址专用，不用于互联网。

b) 互联共享地址：是指政务外网中提供信息服务的主机地址，该地址能够在整个政务外网范围内被访问。互联共享地址包括链路地址（网络设备间的点对点互联地址）和设备管理地址，互联共享地址分配到用户接入设备的上连（网络侧）端口。

6.8 全国环保系统域名管理

6.8.1 原则

a) 国家电子政务网络的域名系统统筹规划，中央和地方分级管理。

b) 域名命名主要采用中文域名，辅以英文域名。中文域名的命名应符合中文书写的特点。

c) 政务内网域名系统采用三级域名管理，政务外网域名系统可采用多级域名管理。

6.8.2 中文域名

6.8.2.1 使用原则

a) 不使用含有“China”、“Chinese”、“CN”、“National”“中国”、“中华”字样的名称；

b) 不应使用其它国家或地区名称、国外地名、国际组织名称；

c) 不应使用行业名称或商品名称；

- d) 不应使用他人已在中国注册过的企业名称或者商标名称；
- e) 不应使用对国家、社会或者公共利益有损害的名称。

6.8.2.2 语法

中文域名语法规则如下：

域 ::= <子域>
 <子域> ::= <顶级域> | <子域><分隔符><标记>
 <分隔符> ::= . | 。
 <顶级域> ::= <汉字串>
 <汉字串> ::= <汉字> | <汉字串><汉字>
 <标记> ::= <字符> | <标记><字符>
 <字符> ::= <汉字> | <字母> | <数字> | <连字符>
 <字母> ::= [A..Z] | [a..z]
 <数字> ::= [0..9]
 <连字符> ::= -

在中文域名中，不区分英文字母大小写，即A和a在域名中是等同的。域名必须以汉字或字母或数字开始，以汉字或字母或数字结束，内部可以使用汉字、字母、数字和连字符。域名字段必须小于64个字节。

字母、数字、“.”和连字符是指GB/T 1988-1998中规定的字符，汉字和“。”是指GB 18030-2005中规定的字符。

为了区分中文域名和英文域名，所输入的中文域名应当至少出现一个非GB/T 1988-1998的字符。

6.8.3 结构

中文域名采用三级结构。其中地方名称按照GB/T 2260的规定命名。

6.8.4 英文域名

英文域名使用原则同中文域名使用原则，见5.9.2.1。

域名均在从域名管理部门申请的域名下，下一级域名为各省级环境保护局名、各下级单位域名由上级部门统一管理，再下一级域名由分配到次一级域名的各省自定。域名中省、市、自治区的缩写遵照《中国互联网络域名注册暂行管理办法》执行。全国环境信息网络系统域名命名规则请见表1.1附录A：全国环境信息网络系统域名命名规则

7 全国环境信息局域网网络建设

7.1 电子政务内网局域网网络建设

7.1.1 网络平台

7.1.1.1 网络选型

网络结构选用星型拓扑结构，支持或扩展后能够支持三层交换技术；局域网应使用TCP/IP协议，所需IP地址要使用私有内部地址，内部IP地址的使用必须由各单位、各部门统一规划，统一配置；局域网须支持以太网协议，网络主干的传输速率不低于1000Mbit/s，到桌面的传输速率不低于100Mbit/s。

7.1.1.2 网络接口设备

核心网络设备网络接口速率不低于1000M bit/s；网络设备网络接口速率不低于100Mbit/s；为客户端提供接入服务的交换设备接口速率不低于100M bit/s。

核心应用服务器端均应配备速率不低于1000M bit/s的网络接口卡；普通应用服务器端均应配备速率不低于100M bit/s的网络接口卡；客户端应尽量选用兼容性强的网卡，并且传输速率不低于100M bit/s。

7.1.1.3 网络交换设备

网络交换设备主要应用于局域网络建设，分为汇聚层交换设备和接入层交换设备，汇聚层交换设备应使用千兆比以太网第3层交换设备，接入层交换设备应使用千兆比以太网第2层交换设备。

1. 千兆比以太网第3层交换设备

千兆比以太网第3层交换设备是拥有第3层路由功能的以太网交换设备，主要功能除实现数据帧转发功能外，第3层交换设备能根据收到的数据包中网络层地址以及交换设备内部维护的路由表决定输出口以及下一条交换设备地址或主机地址，并且重写链路层数据包头。第3层交换设备路由表必须动态维护来反映当前的网络拓扑。

千兆比以太网第3层交换设备主要功能包括：

- a) 接口功能
- b) 逻辑链路层功能
- c) 数据帧转发功能
- d) 数据帧过滤功能
- e) IP包转发功能
- f) 路由信息维护功能
- g) 维护决定数据帧转发及过滤的信息
- h) 运行维护和网络管理功能

有关千兆比以太网第3层交换设备详细要求见YD/T 1099-2001《千兆比以太网交换机设备技术规范》中相应的要求。

2. 千兆比以太网第2层交换设备

千兆比以太网第2层交换设备通常拥有多个千兆比特以太网口，以硬件实现MAC层报转发。

千兆比以太网第2层交换设备主要功能包括

- a) 接口功能
- b) 业务量控制功能
- c) VLAN功能
- d) 支持组播功能
- e) 支持带宽管理
- f) 管理维护
- g) 支持生成树功能

有关千兆比以太网第2层交换设备详细要求见YD/T 1099-2001，《千兆比以太网交换机设备技术规范》中相应的要求。

7.1.1.4 网络服务器

在服务器的选型标准上，应考虑 Web 服务器、应用服务器、数据库服务器等，以保证数据库资源中心数据的统一、完整、安全的存放。服务器需要有强大的数据处理能力，提供并行处理功能和负载均衡措施。当多个用户同时在线访问数据库时，保证系统能够正常运行；当系统未来的业务量增加时，应通过系统升级平滑地适应用户的要求；作为系统的核心处理部件，服务器应有足够的容量，提供海量级数据的存储能力和强大的处理能力，保障高响应速度；它应具备可靠的数据备份和恢复工具，应付可能出现的意外；服务器应具有高可靠性、高可用性，保证系统能够长时间无故障运行。因此，服务器的设计与选型必须满足如下总原则。

a) 一体化原则

对于硬件产品和系统软件应作为一个有机的整体来考虑，包括包内部各组成部分的合理性、兼容性和一致性。因此需考虑硬件产品与系统软件之间的合理性、兼容性和一致性。

b) 兼容性和可扩展性

考虑到整个国家环境数据中心，以及整个环境数据共享平台建设项目，从目前和发展的角度考虑各种软硬系统的兼容性和可扩展性。

c) 可靠性，易维护原则

要求选择成熟、可靠的主流产品，保证系统高可靠性，高可管理性，易操作性，有良好的售后服务和承诺支持。

d) 标准化原则

所选产品需遵循国际通用标准和行业规范。

e) 前瞻性原则

所选服务器必须是当前成熟的产品，同时还应满足先进性要求。

在网络服务器选型中，如使用计算机集群技术、负载均衡技术、单元组合技术，配以 N 层模式，还需考虑：

- a) 采用高可用集群系统，保证系统的不间断运行；必须具有足够的 CPU 处理能力、内存、外存容量；
- b) CPU 数量、内存、内置或外置硬盘容量、I/O 及系统本身都有能满足未来要求的扩展能力，以适应处理大数据量及系统发展的需要；
- c) 数据的存放采用高可靠性的数据存储管理系统，并对重要的数据有可靠的备份机制，硬盘应具

有工业标准的热插拔功能，保证更换硬盘时系统仍能继续正常运行；

- d) 操作系统必须具有 C2 级以上的安全性，运行稳定可靠，支持大规模数据库系统，界面友好，方便管理维护和应用软件开发，并保证应用软件有良好的可移植性。

7.1.2 网络存储设备

存储设备可根据实际需求选用合适容量的存储设备，选用专门的存储备份系统和专用的备份服务器，并制定相应的存储备份及恢复方案。如大容量硬盘、磁盘阵列、带库等。

7.1.3 网络综合布线

7.1.3.1 综合布线系统设计

综合布线系统应在充分考虑信息点分布和数量的基础上，统筹规划，合理设计，精心施工。信息点分布和数量应能至少满足未来 2-3 年内的应用和用户需求，避免短期内重复施工。

在综合布线系统中，布线硬件主要包括：配线架、传输介质、通信插座、插座板、线槽和管道等。综合布线包括六个子系统：工作区子系统、水平布线子系统、管理子系统、干线子系统、设备间子系统和建筑群主干子系统。

7.1.3.2 综合布线设计基本步骤

- a) 获得建筑物平面图：这是整个综合布线系统的设计基础，因为无论哪个子系统都直接与建筑物结构平面图息息相关。
- b) 分析用户需求：具体选择哪种布线方式，哪个工作区布置多少个信息点，干线系统采用什么电缆，配线间和设备间打算安排在哪个位置等，都在相当大程度上是由分析用户需求基础决定的。
- c) 布线系统结构设计：这是综合布线系统设计的开始，主要完成布线系统的总体结构，特别是各工作区、水平子系统的布线系统设计。
- d) 布线系统的路由设计：这一步是完成整个布线系统中各个工作间子系统通过干线子系统与设备间子系统、管理子系统的路由连接设计，以及建筑群子系统（可选）之间的路由连接设计。
- e) 绘制布线施工图：这个施工图要对一些关键信息点、交接点、电缆拐点等位置的施工注意事项和布线线槽（或线管）规格、材质等进行详细的标注或说明。
- f) 编制布线用材料清单：编制具体布线施工中用到的材料清单，布线材料包括各种规格的电缆（如双绞线、光纤）、水晶头、跳线、配线架、线槽、线管等。

7.1.3.3 综合布线各主要组成部分设计

a) 工作区子系统

工作区子系统是整个布线系统的终端子系统，是用户的最终工作区，包括终端设备（如计算机、电话等）到信息插座的区域。在用户工作区的信息插座要能同时提供相应功能的接口，语音接口是电话线 RJ-11 接口，数据用户接口是 RJ-45 双绞线接口，多媒体用户是单模光纤接口（LX），或多模光纤接口（SX），以满足多媒体用户的高带宽需求；注意工作区电缆总长度不能超过 10m；最后，根据各工作区的用户需求决定具体信息点的数量。

b) 水平子系统

水平子系统是指从楼层配线间到工作区信息插座之间的连接，经过工作区信息插座、楼层配线间的配线架，最终是楼层各级交换机端口。设计该子系统时要针对用户对带宽的需求选择相应的传输介质，目前一般是超 5 类、6 类双绞线和光纤；要充分考虑到走线的距离，尽量采用最短路径方式，一定要位直，也应尽量以水平或垂直方式走线。通常在水平子系统中是以双绞线为传输介质的，这就要求整个水平子系统布线长度不能大于 90m。如果是光纤则基本没有限制。

c) 垂直子系统

垂直子系统又叫干线子系统，指提供建筑物的主干电缆的路由，是实现中心配线架与楼层配线架、PBX（用户交换机）、控制中心与各管理子系统间的连接。垂直子系统布线通常是通过弱电竖井统一布线的，所采用的电缆通常采用光纤，光线主要为 62.5/125 μm 多模光纤或 10/125 μm 单模光纤。

d) 设备间子系统

设备间是在每幢大楼的适当地点设置进线设备，进行网络管理以及管理人员值班的场所。设备间子系统的电话、数据、计算机主机设备及其保安配线设备宜集中设在一个设备间内，机架设备可以通过机柜统一安装在一起。

e) 管理子系统

管理子系统设置在楼层配线房间，是水平系统电缆端接的场所，也可是主干系统电缆端接的场

所；由大楼主配线架、楼层分配线架、跳线、转换插座等组成。可以在管理子系统中更改、增加、交接、扩展线缆，用于改变线缆路由。

f) 建筑群子系统

建筑群子系统是实现建筑之间的相互连接，提供楼群之间通信设施所需的硬件。

光纤、水平线接口模块和面板需符合国家标准 GB/T 50311-2000 《建筑与建筑群综合布线系统工程设计规范》。

大楼综合布线，以及选用的电缆、光缆、各种联接器、跳线和配线等所有配件，均应符合 ISO/IEC 11801-2002 《建筑物通用布线国际标准》。

7.1.4 安全平台

7.1.4.1 网络防病毒系统

局域网内计算机在20台以上的网络中应部署网络版防病毒系统，20台以下的网络中可部署单机版防病毒软件。

1. 网络版防病毒系统便于维护和管理，安装专用的集中管理服务器，用做病毒的防、控系统中心。这个监控中心的具备以下功能：

- a) 强大、灵活的管理和任务调度手段，可以通过中心控制台，集中地实现全网范围内防毒策略的定制、分发和执行。
- b) 通过控制台，集中地实现所有节点上防毒软件的监控、配置、查询等管理工作。能够通过控制台看到客户端的病毒版本、查杀毒记录及各种日志信息。
- c) 负责病毒扫描引擎和代码库的更新，并能将此扫描引擎和代码库自动提供给各种服务器和工作站。
- d) 提供多种软件安装和软件升级的手段，必须提供远程安装客户端、基于 WEB 的软件安装和手动、定时病毒库版本升级功能。
- e) 提供远程病毒报警手段，网内任何一台计算机上发现病毒时，杀毒软件自动将病毒信息传递给网络防病毒监控中心。
- f) 分组管理：对所有的网络终端结点进行任意分组。可将不同物理地点的服务器分组，对于客户端也可根据配置的需要分组，包括设置客户端密码、实时监控客户端配置、统一刷新客户端状态、统一发送广播、查询历史记录等。不同组可以执行不同的防病毒策略。
- g) 传染源统计功能：网络中一旦有病毒发作，部署防病毒软件的众多机器就可以将传染源机器的 IP 或机器名记录下来，在管理控制台上生成传染源排行榜，便于掌握网络中的薄弱节点并快速采取措施。
- h) 扫描有防病毒部署漏洞的计算机：通过防毒系统自带的客户机漏洞扫描工具，可以将网络中所有客户机做一个整体的扫描，将没有安装防病毒客户端软件的计算机的 IP 地址，计算机名字，操作系统等详细的信息生成报表，便于防病毒管理人员及时定位网络中未安装防病毒软件的计算机。

2. 网络防病毒系统客户端基本功能：

- a) 应用层病毒的防护：客户机的文件共享，访问 WEB 网页，客户端收发邮件等应用进行全面防护，彻底消除应用层病毒对客户机的破坏，保证所有用户都有一个干净、安全的平台；
- b) 网络层病毒的防护：直接在网络层针对像冲击波、震荡波等病毒的攻击包进行清除，降低的网络病毒的危害，提高了病毒的防护效果；
- c) 病毒爆发阻止策略：应用该策略能够有选择性的关闭某些病毒攻击网络服务器和客户机的端口或共享文件夹等，从而阻挡大量的蠕虫病毒在网络中大面积爆发，保护用户网络中的所有计算机不受到病毒攻击。当网络内部不幸遭遇到新病毒攻击而病毒码还未更新时，利用病毒爆发阻止策略能够将新病毒所利用的网络漏洞和系统漏洞完全堵死，让还没有进来的病毒进不进来，让已经进来的病毒无法扩散；
- d) 集成网络版防火墙和 IDS 抵御复合式攻击：通过防火墙在客户机和网络之间创建屏障，来帮助保护客户机免受黑客和网络病毒的侵扰，同时，IDS 确保客户机不受到内部或外部的入侵攻击，确保内部网络计算机的系统安全和资料安全；
- e) 集成病毒专杀工具，清除病毒更彻底：病毒专杀工具和客户端防病毒软件无缝集成，专杀工具的扫描引擎和病毒码可以自动更新；
- f) 抵御间谍软件和其他类型灰件的侵害：防病毒网络版下载间谍软件/灰件特征码文件以保护网

络内计算机免受病毒之外各种潜在威胁（包括广告软件和间谍软件）的侵害。

3. 单机版防病毒软件可以参照网络防病毒系统客户端基本功能。

7.1.4.2 网络安全域逻辑划分

电子政务内网安全域只包含内部域。内部域主要是指内部局域网的办公、运维和应用计算机，在内部域中又可以划分为：各业务用户域（按照职能部门）、内部平台域、管理员域等。各业务用户域主要是指办公人员按照所在职能部门划分的逻辑区域；内部平台域主要是指内部应用服务器，管理员域是指运维人员办公设备所在用区域。

在环境信息网络电子政务内网建设中通过配置三层交换设备来划分内部域，将各业务用户域按照办公人员所在职能部门划分 VLAN，将内部平台域和管理员域划分 VLAN，并可根据业务需求划分更多的 VLAN。

7.1.5 用户平台

用户平台主要包括客户计算机、桌面操作系统、浏览器及客户端应用软件等

7.1.5.1 用户操作系统

计算机须安装Windows 98版本以上，或linux的操作系统，具有较强网络功能；系统操作便捷，运行稳定；具备容错能力和故障恢复能力；支持图像、图形界面、视频、音频等多媒体功能；支持汉字输入（国标码）环境；支持多客户、多线程、多处理工作方式。

7.1.5.2 用户应用软件

用户计算机应安装计算机防病毒客户端、Web浏览器、办公管理软件等应用软件。对于带有安全漏洞，黑客程序的应用软件严禁下载和安装。

7.2 电子政务外网局域网网络建设

7.2.1 网络平台

7.2.1.1 网络选型

网络结构选用星型拓扑结构，支持或扩展后能够支持三层交换技术；局域网应使用 TCP/IP 协议，所需 IP 地址要使用私有内部地址，内部 IP 地址的使用必须由各单位、各部门统一规划，统一配置；局域网须支持以太网协议，网络主干的传输速率不低于 1000Mbit/s，到桌面的传输速率不低于 100Mbit/s。

7.2.1.2 网络传输设备

核心应用服务器端均应配备速率不低于1000M bit/s的网络接口卡；普通应用服务器端均应配备速率不低于100M bit/s的网络接口卡；客户端应尽量选用兼容性强的网卡，并且传输速率不低于100M bit/s。

7.2.1.3 网络交换设备

见章节7.1.1.3

7.2.1.4 网络服务器

见章节7.1.1.4

7.2.2 网络存储设备

见章节7.1.2

7.2.3 网络综合布线

见章节7.1.3

7.2.4 安全平台

7.2.4.1 网络防病毒系统

见章节7.1.4.1

7.2.4.2 网络安全域逻辑划分

电子政务外网安全域可以划分为三个大区域，分别是外部域、接入域（DMZ 区域）和内部域，安全等级从低到高，内容如下：

1. 外部域主要是指各级环保部门连接的外部网络。
2. 接入域（DMZ 区域）主要指各级环保部门与外部接入部分和对外提供服务的逻辑边界部分，如各级环保部门对外提供访问的 WEB 服务器、MAIL 服务器等。
3. 内部域主要是指局域网的办公、运维和应用计算机，在内部域中又可以划分为：各业务用户域（按照职能部门）、内部平台域、管理员域等。各业务用户域主要是指办公人员按照所在职能部门划分的逻辑区域；内部平台域主要是指内部应用服务器，不需要向外发布的逻辑区域；管理员域是指运维人员办公设备所在用区域。

在环境信息网络电子政务外网建设中可以通过配置防火墙来划分外部域、接入域和内部域这三大区域；通过配置三层交换设备来划分内部域，将各业务用户域按照办公人员所在职能部门划分 VLAN，将内部平台域和管理员域划分 VLAN，并根据业务需求划分更多的 VLAN。

8 全国环境信息网络机房建设

8.1 机房建设

8.1.1 机房建设的指导思想

- a) 合理分布工作空间及各类设备安装场所，缩短工艺流程，降低劳动强度，提高工作效率，确保电子设备系统稳定可靠运行，保障机房工作人员良好的工作环境，并且以国家有关标准及规范为依据。
- b) 根据实际需求与现场实际情况以及电子设备系统实际操作运行等情况进行设计，力求在设计、选材中做到整体布局的合理化和科学化。
- c) 机房各项功能完整配套，达到专业规范、技术先进、经济合理、安全适用、质量优良、管理方便之目的。
- d) 在经济实用的前提下，选择优质机房专用装修材料，主体装修材料宜选用吸音效果好、不易变形、变色、易清洁、防火性好，且高度耐用的材料，达到最佳装修效果。
- e) 室内控制设备、电器设备、布线系统的选材注重其可靠性，全部采用符合国家标准的优质产品，以确保系统投入运行后故障率为最低。

8.1.2 机房总体建设

8.1.2.1 机房土建结构方面的要求

- a) 电子计算机机房的建筑平面和空间布局应具有适当的灵活性，主机房的主体结构宜彩大开间大跨度的柱网，内隔墙宜具有一定的可变性。
- b) 主机房净高，依机房面积大小而定，一般为2.5m~3.2m。
- c) 电子计算机机房的楼板荷载依设备而定。一般分为两级。
A级： $\geq 500\text{Kg}/\text{m}^2$
B级： $\geq 300\text{Kg}/\text{m}^2$
- d) 空调设备、供电设备用房的楼板荷重应依据设备重量而定，一般应 $\geq 1000\text{Kg}/\text{m}^2$ 或采用加固措施
- e) 电子计算机机房主体结构应具有耐久、抗震、防火、防止不均匀沉陷等性能。变形缝和伸缩缝不应穿过主机房。
- f) 主机房中各类管线宜暗敷，当管线需穿楼层时，宜设技术竖井。
- g) 室内顶棚上安装的灯具、风口、火灾控制器及喷嘴等应协调布置，并应满足各专业的技术要求。
- h) 电子计算机机房围护结构的构造和材料应满足保温、隔热、防火等要求。
- i) 电子计算机机房各门的尺寸均应保证设备运输方便。

8.2 机房环境

8.2.1 机房地點

电子计算机机房位置选择应符合下列要求：

- a) 水源充足，电力比较稳定可靠，交通通讯方便，自然环境清洁。
- b) 远离产生粉尘、油烟、有害气体以及生产或贮存具有腐蚀性、易燃、易爆物品的工厂、仓库，堆场等。
- c) 远离强振源和强噪声源。
- d) 避开强电磁场干扰。
- e) 电子计算机机房在多层建筑或高层建筑内宜设于第二、三层。
- f) 空气含尘量：机房应保持清洁，空气中大于0.5Micron的杂质 在每立方英尺不得多于45,000个，若空气中灰尘过多很容易造成资料读写错误及磁盘中磁盘或读写磁头损毁。

注：机房颤动度：不得高于0.5g。磁场杂波干扰：机房附近无线电杂波干扰，应低于0.5伏特/米（频率范围从14KHz到1GHz）。

8.2.2 机房面积

计算机机房最小使用面积不得小于50平方米，除了系统安放之外，应预留足够的空间作安装、维修及操作之用。另外，还应预留空间作系统扩展之用。

计算机使用面积一般按照以下两种方法之一确定：

第一种方法：当计算机系统设备已选型时，可按此公式计算：

$$A=k\Sigma S \quad \dots\dots\dots (1)$$

此公式中：A——计算机主机房使用面积（m²）；

K——系数，取值为5~7；

S——计算机系统及辅助设备的投影面积（m²）；

ΣS——机房内所有设备占地面积的总和（m²）；

第二种方法：当计算机系统设备尚未选型时，可按此公式计算：

$$A=KN \quad \dots\dots\dots (2)$$

此公式中：A——计算机主机房内使用面积；

K——单台设备占用面积，可取4.5~5.5（m²/台）

N——计算机主机房内所有设备的总台数

8.2.3 机房内部环境要求

8.2.3.1 机房温、湿度

a) 主机房、基板工作间内的温、湿度必须满足计算机设备要求；

b) 计算机机房内温、湿度应满足下列要求：

1) 开机时计算机机房内的温、湿度符合表1的规定

2) 关机时计算机机房内的温、湿度符合表2的规定

表1 开机时计算机机房内的温、湿度

项 目 \ 级 别	A 级		B 级
	夏季	冬季	全年
温 度	23±2℃	20±2℃	15~30℃
相 对 湿 度	45%~65%		40%~70%
温度变化率	< 5℃/h 并不得结露		<10℃/h 并不得结露

表2 关机时计算机机房内的温、湿度

项 目 \ 级 别	A 级	B 级
温 度	5~35℃	5~35℃
相 对 湿 度	40%~70%	20%~80%
温度变化率	< 5℃/h 并不得结露	<10℃/h 并不得结露

开机时主机房的温、湿度应执行 A 级，基本工作间可根据设备要求按 A、B 两级执行，其他辅助房间应按工艺要求确定；

注：根据计算机系统对温、湿度的要求，将温、湿度分为 A、B 两级，机房可按某一级执行，也可按某些级综合执行。

综合执行指的是一个机房可按某些级执行，而不必强求一律，如某机房按机器要求可选：开机是按 A 级温、湿度，，停机是按 B 级温、湿度。

8.2.3.2 机房噪声、电磁干扰、振动及静电

a) 机房内的噪声，在计算机系统停机条件下，在机房中心位置测量应小于65dB（A）。

b) 机房内无线电干扰场强，在频率为0.15~1000MHz时，不应大于126dB。

c) 机房内磁场干扰环境场强不应大于800A/m。

d) 在计算机系统停机条件下主机房地板表面垂直及水平向的振动加速度值，不应大于500mm/s²

- e) 机房地面及工作台面的静电泄漏电阻,应符合现行国家标准《计算机机房用活动地板技术条件》的规定。
- f) 主机房内绝缘体的静电电位不应大于1kV。

8.2.3.3 机房空气含尘浓度

主机房内的空气含尘浓度,在静态条件下测试,每升空气中大于或等于 $0.5\mu\text{m}$ 的尘粒数,应少于18000粒/ cm^3 (相当于500 000粒/英尺³)。

8.2.3.4 机房照明

- a) 照明:计算机机房在距地面0.8米处,照明不应低于300 lx,基本工作间和第一类辅助间不低于200 lx,其他房间按照具体情况决定。(参照执行GB50034—2004《建筑照明设计标准》)
- b) 事故照明:计算机机房、终端室、已记录的媒体存放间应设置事故照明,其照度在距地面0.8米处不低于5 lx。主要通道及有关房间依据需要应设置事故照明,其照度在距地面0.8米处不低于1 lx。

8.2.3.5 机房接地

- a) 计算机系统直流地电阻的大小应依不同计算机系统的要求而定。
- b) 交流工作地的接地电阻应不大于 4Ω 。
- c) 安全保护地的接地电阻应不大于 4Ω 。
- d) 防雷保护地的接地电阻应不大于 10Ω 。
- e) 诸地之间的关系及接法应依不同计算机系统的要求而定。

8.2.3.6 机房供电

- a) 计算机场地的供电电源应满足下列要求:
 - 频率:50Hz;
 - 电压:380V/220V;
 - 相数:三相五线或三相四线制/单相三线制
- b) 供电方式:
 - 依据计算机用途,其供电方式可分为三类:
 - 一类供电:需建立不间断供电系统;
 - 二类供电:需建立备用供电系统;
 - 三类供电:按一般用户供电考虑

8.3 UPS 规范

8.3.1 UPS 额定输出容量的选择

应根据所用设备的负荷量统计值来选择所需的UPS输出功率(KVA值)。为确保UPS系统的效率和尽可能延长UPS的使用寿命,一般推荐参数是:

- a) 用户的负载量仅占UPS的输出功率的60%~70%为宜。
- b) 尽可能先用单台大容量UPS实践;采用单台容量较大的UPS集中供电方式,不仅有利于集中管理UPS,有效利用电池能量,而且降低了UPS的故障率。

8.3.2 根据不同配送系统,有三种UPS机型可供选择

- a) 单进(220V输入)/单出(220V输出)机型:选用此机型时,虽然用户无需考虑市电三相输入平衡带载问题,但必须考虑市电配电的三相均衡带载问题。
- b) 三进(380V输入)/单出(220V输出)机型:表面上看起来,似乎用户无需考虑电三相输入平衡带载问题,其实不然,用户应为它的交流旁路市电输入的相线和中线配置上可单相承担UPS额定输出电流的导线截面积。
- c) 三进(380V输入)/三出(380V输出)机型:一般说来,要求用户将UPS输出端的负载不平衡度控制在不超过30%~40%范围内。

8.3.3 UPS 容错冗余供电

对供电质量要求很高的计算中心、网管中心,为确保对负载供电的万无一失,常需要采用如下几种具有“容错”功能的冗余供电系统。

- a) 1. 主机-从机型“热备份”冗余供电系统:其结构形式是将主机UPS的交流旁路连接到从机UPS的逆变器电源输出端,万一主机UPS出故障时,改由从机UPS带载。这种冗余工作方式由于没有“扩容”功能和可能出现4MS的供电中断,而使其应用范围有限。

- b) 2. “1+1”型直接并机冗余供电系统：它是通过将两台具有相同功率UPS的输出置于同幅度、同相位和同频率的状态而直接并联起来。正常工作时，由两台UPS各承担1/2负载电流，万一其中一台UPS出故障时，由剩下的一台UPS来承担全部负载。这种并机系统的平均故障工作时间MTBF是单机UPS的7-8倍，从而大大提高系统的可靠性。
- c) 3. 多机直接并机冗余供电系统：某些UPS，可以将多台UPS以“N+1”冗余方式直接并机工作。请注意：随着多台并机系统中的N数量增大，并机系统的MTBF值会逐渐下降。因此，在条件允许时，应尽可能减少多机并机系统中UPS单机的数量。

8.3.4 UPS 运行环境

- a) 应将UPS用蓄电池组置于20℃-25℃的环境下运行，不管UPS的充电器是否具有充电温度补偿功能，都必须将UPS用的蓄电池置于20℃-25℃范围内。过低的环境温度会造成蓄电池的放电容量下降，超过25℃时，会造成蓄电池的使用寿命缩短。
- b) 对于后备时间长，需要电池较多的UPS电源，应考虑机房的单位面积承重量。
- c) UPS应具备网管功能，可以进行远程的监测控制。

8.3.5 UPS 供电系统中的中线截面积应加粗

鉴于计算机和通讯设备等非线性负载均属于“整流滤波型”负载，从而造成流过供电系统中的中线电流急剧增大，为防止因中线过流或中线电压过高而造成不必要的麻烦，应将中线的截面积加粗为相线的1.5-2倍。

8.3.6 其他

宜选用具有双原边绕组（交流旁路和逆变器）输出隔离变压器的UPS机型，大量运行实践证明，如果出现在UPS输出端的中线对地线的“干扰”电位过高，会导致计算机网络的数据通讯的误码率增高

8.4 机房空气调节系统

8.4.1 一般规定

- a) 主机房和基本工作间均应设置空气调节系统
- b) 当主机房和其他房间的空调参数不同时，宜分别设置空调系统

8.4.2 气流组织

- a) 主机房和基本工作间空调系统的气流组织，应根据设备对空调的要求、设备本身的冷却方式、设备布置密度、设备发热量及房间温湿度、室内风速、防尘、消声等要求，并结合建筑条件综合考虑
- b) 气流组织的形式应按计算机系统的要求确定。对设备布置密度大、设备发热量大的主机房宜采用活动地板下送上回的方式，但楼板应采取保温措施。
- c) 采用活动地板下送上回的方式时，出口风速不应大于3m/s，送风气流不应直对工作人员。

8.4.3 空调系统

- a) 计算机机房要求空调的房间宜集中布置；室内温、湿度要求相近的房间，宜相邻布置。
- b) 主机房不宜设采暖散热器。如设采暖散热器必须采取严格的防漏措施。
- c) 风管不宜穿过防火墙和变形缝。如必须穿过时，应在穿过防火墙处设防火阀门；穿过变形缝处，应在两侧设防火阀门。防火阀门既能手控又能自控。穿过防火墙、变形缝的风管两侧各2m范围内的风管保温材料必须采用非燃烧材料。
- d) 空调系统应设消音装置
- e) 主机房必须维持一定的正压。主机房与其他房间、走廊的压差不应小于4.9Pa，与室外静压差不应小于9.8Pa。
- f) 空调系统的新风量应取下列三项中的最大值
 - A. 室内总风量的5%
 - B. 按工作人员每人40m³/h
 - C. 维持室内正压所需风量
- g) 主机房的空调送风系统，应设初效、中效两级空气过滤器，中小空气过滤器计数效率应不大于80%，末级过滤装置宜设在正压端或送风口。
- h) 计算机机房空气调节控制装置应满足计算机系统对温度、湿度、及防尘对正压的要求。
- i) 空调真冷设备的制冷能力，应留有15%~20%的余量。当计算机系统长期连续运行时，空调系统应有备用装置。
- j) 在每台空调机周围应安装漏水检测报警系统。

8.4.4 新风系统

- a) 机房内的新风系统是必不可少的。清新的新风提高机房的洁净度，使机房保证正压，并提供新鲜空气。
- b) 新风应满足两个指标：其一，是每人每小时40立方米；其二，是应占空调系统总风量的5~10%。
- c) 根据国家有关规范和标准规定，计算机房内应设排风系统，用以排除可能出现的烟雾及灭火后出现的气体。
- d) 新风系统内设防烟防火阀。排风系统内设排风阀。阀门既可手动又需和消防报警系统联动。根据消防报警指示要求关闭或开启阀门。

8.5 机房消防

8.5.1 机房消防一般规定

- a) 计算机机房的入口至主机房应设通道，通道净宽不应小于1.5米。
- b) 计算机主机房、基本工作间应设二氧化碳或卤代烷灭火系统。
- c) 计算机机房应设火灾自动声光报警系统。
- d) 报警系统和自动灭火系统应与空调、通风系统连锁。空调系统所采用的电加热器，应设置无风断电保护。

8.5.2 机房消防报警系统

- a) 报警区域内应安装火灾探测器，并同时有自动声光报警系统和手动报警装置。还应有自动和手动取消报警装置。
- b) 音响报警装置发出的音响，应与背景噪音有明显区别。灯光报警信号应作为音响报警信号的辅助手段。
- c) 报警区域内每个防火分区，应至少设置一只手动火灾报警按钮。从一个防火分区内的任何位置到最邻近的一个手动火灾报警按钮的步行距离不应大于30m。
- d) 手动火灾报警按钮应设置在明显的和便于操作的位置。当安装在墙上距地面1.5m处，且应有明显标志。
- e) 灯光报警装置和音响报警装置其中一种发生任何故障，不应影响另一种装置正常工作。

8.5.3 机房消防设施

- a) 凡设置二氧化碳或卤代烷固定灭火系统及火灾探测器的电子计算机机房，其吊顶的上、下及活动地板下，均应设置探测器和喷嘴。
- b) 主机房宜采用感烟探测器。当设有固定灭火系统时，应采用感烟、感温两种探测器的组合。
- c) 当主机房内设置空调设备时，应受主机房内电源切断开关的控制。机房内的电源切断开关应靠近工作人员的操作位置或主要出入口
- d) 火灾探测器的种类可根据房间的高度而定，具体见：附录F 对不同高度房间的火灾探测器的选择
- e) 火灾探测器的设置数量与布局根据火灾探测器的保护面积和保护半径而定，具体见：附录G 感烟、感温探测器的保护面积和保护半径

8.5.4 机房消防安全措施

- a) 计算机机房的安全出口不应少于两个，并宜设置于机房两端。门应向疏散方向开启，并应保证在任何情况下都能从机房内打开。走廊、楼梯间应畅通壁并有明显疏散指示标志。
- b) 凡设有卤代烷灭火装置的电子计算机机房，应配置专用的空气呼吸器或氧气呼吸器。
- c) 电子计算机机房内存放废弃物应采用有防火盖的金属容器。
- d) 电子计算机机房内存放记录介质应采用金属柜或其它能防火的容器。
- e) 根据主机房的重要性，可设警卫室或保安设施。
- f) 电子计算机机房应有防鼠、防虫措施。

8.6 防雷、接地保护系统

8.6.1 防雷系统

8.6.1.1 计算机机房防雷等级

根据《建筑物防雷设计规范》中的建筑物的防雷分类中规定，预计雷击次数大于或等于0.012次/a，且小于或等于0.06次/a的部、省级办公建筑物及其他重要或人员密集的公共建筑物，应属于第三类防雷建筑物。

建筑物年预计雷击次数计算方法：

$$N=kNgAe$$

式中 N ——建筑物预计雷击次数（次/a）

k ——校正系数，在一般情况下取 1，在下列情况下取相应数值：

位于狂野孤立的建筑物取 2；金属屋面的砖木结构建筑取 1.7；

位于河边、湖边、山坡下或山地中土壤电阻率较小处、地下水露头处、土山顶部、山谷风口处的建筑物，以及特别潮湿的建筑物取 1.5；

Ng ——建筑物所处地区雷击大地的年平均密度[次/($\text{km}^2 \cdot \text{a}$)]；

Ae ——与建筑物截收相同雷击次数的等效面积(km^2)。

8.6.2 防雷措施

8.6.2.1 一般规定

- 各类防雷建筑物应采取防直击雷和防雷电波侵入措施
- 装有防雷装置的建筑物，在防雷装置与其他设施和建筑物内人员无法隔离的情况下，应采取等电位连接

8.6.2.2 第三类防雷建筑物的防雷措施

- 根据《建筑物防雷设计规范》第三类防雷建筑物防直击雷的措施，宜采用装设在建筑物上的避雷网或避雷针或由这两种混合组成的接闪器。并应在整个屋面组成不大于 $20\text{m} \times 20\text{m}$ 或 $24\text{m} \times 16\text{m}$ 的网格。
- 平屋面的建筑物，当其宽度不大于 20m 时，可仅沿周边敷设一圈避雷带。
- 每根引下线的冲击接地电阻不宜大于 10Ω ，其接地装置宜与电气设备等接地装置共用。防雷的接地装置宜与埋地金属管道相连。当不共用时，两者间在地中的距离应不小于 2m 。共用接地装置与埋地金属管道相连的情况下，接地装置宜围绕建筑物敷设成环形接地体。
- 建筑物宜用钢筋混凝土屋面板、梁、柱和基础的钢筋作为接闪器、引下线和接地装置。
 - 利用基础内钢筋网作为接地体时，在周围地面以下距地面不小于 0.5m ，每根引下线所连接的钢筋表面总和应符合下列表达式的要求：

$$S \geq 1.89kc^2$$

式中 S ——钢筋表面积总和 (m^2)

- 当在建筑物周边的无钢筋的闭合条形混凝土基础内敷设人工基础接地体时，接地体的规格尺寸不得小于表 3 的规定

表3 第三类防雷建筑物环形人工基础接地体的规格尺寸表

闭合条形基础的周长(m)	扁钢 (mm)	圆钢, 根数×直径 (mm)
≥ 60		$1 \times \phi 10$
≥ 40 至 < 60	4×20	$2 \times \phi 8$
< 40	刚才表面积总和 $\geq 1.89 \text{ m}^2$	

注：当长度相同、截面相同时，宜优先选用扁钢；

采用多根圆钢时，其敷设净距不小于直径 2 倍；

利用闭合条形基础内的钢筋作接地体时可按本表校验。除钢筋外，可计入箍筋的表面积。

- 引下线不应少于两根，但周长不超过 25m 且高度不超过 40m 的建筑物可只设一根引下线。引下线应沿建筑物四周均匀或对成布置，其间距不应大于 25m 。当仅利用建筑物四周的钢柱或柱子钢筋作为引下线时，可按跨度设引下线，但引下线的平均间距不应大于 25m 。
- 防雷电波侵入的措施，应符合下列要求：
 - 对电缆进出线，应在进出端将电缆的金属外皮、钢管等与电气设备接地相连。当电缆转换为架空线时，应在转换处装设避雷器；避雷器、电缆金属外皮和绝缘子铁脚、金具等应连在一起接地，其冲击接地电阻不宜大于 30Ω 。
 - 对低压架空进出线，应在进出处装设避雷器并于绝缘子铁脚、金具连在一起接到电气设备的接地装置上。当多回路架空进出线时，可在母线或总配电箱处装设一组避雷器或其他形式的过电保护器，但绝缘子铁脚、金具仍应接到接地装置上。
 - 进出建筑物的架空金属管道，在进出处应就近接到防雷或电气设备的接地装置上或独自接地，其冲击接地电阻不宜大于 30Ω 。

8.6.3 防雷装置

- 接闪器

- b) 引下线
- c) 接地装置

8.6.4 接地保护系统

8.6.4.1 一般规定

1. 电气装置的下列金属部分，均应接地或接零
 - a) 室内外配电装置的金属或钢筋混凝土构架以及靠近带电部分的金属遮栏和金属门；
 - b) 配电、控制、保护用的屏（柜、箱）及操作台等的金属框架和底座；
 - c) 交、直流电力电缆的接头盒、终端盒和膨胀器的金属外壳和可触及的电缆金属护层和穿线的钢管。穿线的钢管之间或钢管和电器设备之间有金属软管过渡的，应保证金属软管段接地畅通；
 - d) 承载电气设备的构架和金属外壳；
 - e) 电热设备金属外壳。
2. 电气装置的下列金属部分不可接地或接零
 - a) 安装在已接地的金属构架上的设备，如穿墙套管等；
 - b) 额定电压为220V及以下的蓄电池室内的金属支架；
 - c) 安装在配电屏、控制屏和配电装置上的电气测量仪表、继电器和其他低压电器等的外壳，以及当发生绝缘损坏时，在支持物上不会引起危险电压的绝缘子的金属底座等。
3. 需要接地的直流系统的接地装置应符合下列要求
 - a) 能与地构成闭合回路且经常流过电流的接地线应沿绝缘垫板敷设，不得与金属管道、建筑物和设备的构件有金属的连接；
 - b) 直流电力回路专用的中性线和直流两线制正极的接地体、接地线不得与自然接地体有金属连接；当无绝缘隔离装置时，相互间的距离不应小于1m；
 - c) 三线制直流回路的中性线宜直接接地。
4. 接地线不应作其他用途

8.6.5 接地装置的选择

- a) 各种接地装置应利用直接埋入地中或水中的自然接地体。交流电气设备的接地，可利用直接埋入地中或水中的自然接地体，可以利用的自然接地体如下：
 - 1) 埋设在地下的金属管道，但不包括有可燃或有爆炸物质的管道；
 - 2) 金属井管；
 - 3) 与大地有可靠连接的建筑物的金属结构。
- b) 交流电气设备的接地线可利用下列自然接地体接地：
 - a) 建筑物的金属结构（梁、柱等）及设计规定的混凝土结构内部的钢筋；
 - b) 配线的钢管。
- c) 人工接地网的敷设应符合以下规定：
 - 1) 人工接地网的外缘应闭合，外缘各角应做成圆弧形，圆弧的半径不宜小于均压带间距的一半；
 - 2) 接地网内应敷设水平均压带，按等间距或不等间距布置。
- d) 除临时接地装置外，接地装置应采用热镀锌钢材，水平敷设的可采用圆钢和扁钢，垂直敷设的可采用角钢和钢管。腐蚀比较严重的地区接地装置，应适当加大截面，或采用阴极保护等措施。不得采用铝导体作为接地体或接地线。
- e) 接地装置的人工导体，导体截面应符合热稳定、均压和机械强度的要求，还应考虑腐蚀的影响，一般不小于表4和表5所列规格：

表4 钢接地体的最小规格

种类、规格及单位		地上		地下	
		室内	室外	交流电流回路	直流电流回路
圆钢直径 (mm)		6	8	10	12
扁钢	截面 (mm ²)	60	100	100	100
	厚度 (mm)	3	4	4	6
角钢厚度 (mm)		2	2.5	4	6

钢管管壁厚度 (mm)	2.5	2.5	3.5	4.5
-------------	-----	-----	-----	-----

表5 铜接地体的最小规格

种类、规格及单位	地上	地下
铜棒直径 (mm)	4	6
铜排截面 (mm ²)	10	30
铜管管壁厚度 (mm)	2	3

- f) 不要求敷设专用接地引下线的电气设备，他的接地线可利用金属构件、普通钢筋混凝土构件的钢筋、穿线的钢管等。利用以上设施作接地线是，应保证其全长为完好的电气通路。
- g) 不得利用蛇皮管、管道保温层的金属外皮或金属网、低压照明网络的导线铅皮以及电缆金属保护层作接地线。蛇皮管两端应采用自固接头或软管接头，且两端应采用软铜线连接。

8.6.6 配电电气装置的接地

- a) 户外配电变压器等电气装置的接地装置，宜在地下敷设成围绕变压器太的闭合环形；
- b) 配电变压器等电气装置安装在有其供电的建筑物内的配电装置室时，其接地装置应与建筑物基础钢筋等相连；
- c) 引入配电装置室的每条架空线路安装的避雷器的接地线，应与配电装置室的接地装置相连，但在入地处应敷设集中接地装置。

8.6.7 建筑物电气装置的接地

- a) 建筑物内的低压系统接地点、电气装置外露导电部分的保护接地（含与功能接地、保护接地共用的安全接地）、总等电位联结的接地极等可与建筑物的雷电保护接地共用同一接地装置。接地装置的接地电阻应符合其中最小值的要求。
- b) 接地装置的安装应符合以下要求：
 - 1) 接地极的形式、埋入深度及接地电阻值应符合设计要求；
 - 2) 穿过墙、地面、楼板等处应有足够坚固的机械保护措施；
 - 3) 接地装置的材质及结构应考虑腐蚀而引起的损伤。必要时采取措施，防止产生电腐蚀。
- c) 电气装置应设置总接地端子或母线，并与接地线、保护线、等电位连接干线和安全、功能共用接地装置的功能性接地线等相连接。
- d) 断开接地线的装置应便于安装和测量。

环境信息网络机房建设应参考 GB 50174《电子计算机机房设计规范》和 GB/T 2887《电子计算机场地通用规范》，技术参数应符合国家标准。

9 全国环境信息网络验收测试标准

9.1 验收测试范围

测试范围包括广域网、城域网链路测试、局域网系统测试、网络设备测试等。

9.2 验收测试方法

9.2.1 局域网系统连通性测试方法

9.2.1.1 测试方法

局域网系统连通性测试结构示意图如图1所示。局域网系统性能测试工具要求参见附录A。

- a) 将测试工具连接到选定的接入层设备的端口，即测试点；
- b) 用测试工具对网络的关键服务器、核心层和汇聚层的关键网络设备（如交换机和路由器），进行 10 次 PING 测试，每次间隔 1s，以测试网络连通性。测试路径要覆盖所有的子网和 VLAN；
- c) 移动测试工具到其它位置测试点，重复步骤 b)，直到遍历所有测试抽样设备。

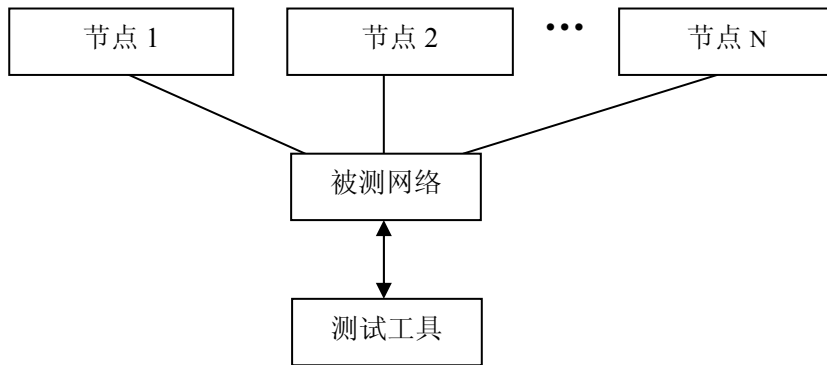


图1 局域网系统连通性测试结构示意图

9.2.1.2 抽样规则

以不低于接入层设备总数的 10% 的比例进行抽样测试，抽样少于 10 台设备的，全部测试；每台抽样设备中至少选择一个端口，即测试点，测试点应能够覆盖不同的子网和 VLAN。

9.2.1.3 合格判据

- a) 单项合格判据：测试点到关键服务器的 PING 测试连通性达到 100% 时，则判定该测试点符合 6.3.1 的要求；
- b) 综合合格判据：所有测试点的连通性都达到 100% 时，则判定局域网系统的连通性符合 6.3.1 的要求；否则判定局域网系统的连通性不符合 6.3.1 的要求。

9.2.2 链路传输速率测试方法

9.2.2.1 测试方法

测试结构示意图如图 2，测试工具 1 产生流量，测试工具 2 接收流量。若发送端口和接收端口位于同一机房，也可用一台具备双端口测试能力的测试工具实现。测试应在空载网络中进行。

- a) 将用于发送和接收的测试工具分别连接到被测网络链路的源和目的交换机端口或末端集线器端口上；
- b) 对于交换机，测试工具 1 在发送端口产生 100% 满线速流量；对于集线器，测试工具 1 发送端口产生 50% 线速流量（建议将帧长度设置为 1518 字节）；
- c) 测试工具 2 在接收端口对收到的流量进行统计，计算其端口利用率。

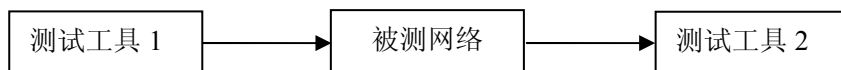


图2 链路传输速率测试结构示意图

9.2.2.2 抽样规则

对核心层的骨干链路，应进行全部测试；对汇聚层到核心层的上联链路，应进行全部测试；对接入层到汇聚层的上联链路，以不低于 10% 的比例进行抽样测试；抽样链路数不足 10 条时，按 10 条进行计算或者全部测试。

9.2.2.3 合格判据

发送端口和接收端口的利用率若符合表 1 要求，则判定局域网系统的传输速率符合 6.3.2 的要求，否则判定局域网系统的传输速率不符合 6.3.2 的要求。

9.2.3 网络吞吐率测试方法

9.2.3.1 测试方法

测试结构示意图如图 3，测试工具 1 产生流量，测试工具 2 接收流量。若发送端口和接收端口位于同一机房，也可用一台具备双端口测试能力的测试工具实现。测试应在空载网络下分段进行，包括接入层到汇聚层链路、汇聚层到核心层链路、核心层间骨干链路、及经过接入层、汇聚层和核心层的用户到用户链路。

- a) 将两台测试工具分别连接到被测网络链路的源和目的交换机端口上；

- b) 先从测试工具 1 向测试工具 2 发送数据包；
- c) 用测试工具 1 按照一定的帧速率，均匀地向被测网络发送一定数量的数据包；
- d) 如果所有的数据包都被测试工具 2 正确接收到，则增加发送的帧速率；否则减少发送的帧速率；
- e) 重复步骤 c)，直到测出被测网络/设备在未丢包的情况下，能够处理的最大帧速率；
- f) 分别按照不同的帧大小（包括：64、128、256、512、1024、1280、1518 字节）重复步骤 b)~d)；
- g) 从测试工具 2 向测试工具 1 发送数据包，重复步骤 c)~f)。



图3 网络吞吐量测试结构示意图

9.2.3.2 抽样规则

对核心层的骨干链路，应进行全部测试；对汇聚层到核心层的上联链路，应进行全部测试；对接入层到汇聚层的上联链路，以不低于 10% 的比例进行抽样测试；抽样链路数不足 10 条时，按 10 条进行计算或者全部测试；对于端到端的链路（即经过接入层、汇聚层和核心层的用户到用户的网络路径），以不低于终端用户数量 5% 比例进行抽测，抽样需要覆盖所有 VLAN 到 VLAN、网段到网段间可能用到的连接。抽样链路数不足 10 条时，按 10 条进行计算或者全部测试。

9.2.3.3 合格判据

若局域网系统在不同帧大小情况下，从两个方向测得的最低吞吐率值都符合表 2 要求时，则判定局域网系统的吞吐率符合 6.3.3 的要求，否则判定局域网系统的吞吐率不符合 6.3.3 的要求。如果所选择的两点间测试通过，那么该两点间所包含的接入层、汇聚层和骨干层部分中间链路可不必测试。

9.2.4 传输时延测试方法

9.2.4.1 测试方法

当被测网络的收发端口位于不同的地理位置，测试结构示意图如图 4a)，需要由两台测试工具来完成测试，测试工具 1 产生流量，测试工具 2 接收流量，并将测试数据流环回。当被测网络的收发端口位于同一机房，测试结构示意图如图 4b)，可由一台具有双端口测试能力测试工具完成，测试工具的一个端口用于产生流量，另一个端口用于接收流量。测试应在空载网络下分段进行，包括接入层到汇聚层链路、汇聚层到核心层链路、核心层间骨干链路、及经过接入层、汇聚层和核心层的用户到用户链路。

- a) 将测试工具（端口）分别连接到被测网络链路的源和目的交换机端口上；
- b) 先从测试工具 1（发送端口）向测试工具 2（接口端口）均匀地发送数据包；
- c) 向被测网络发送一定数目的 1518 字节的数据帧，使网络达到 7.1.3 节中所测得的最大吞吐率；
- d) 在图 4a) 中，由测试工具 1 向被测网络发送特定的测试帧，在数据帧的发送和接收时刻都打上相应的时间标记（Timestamp）；在图 4b) 中，测试工具通过发送端口发出带有时间标记的测试帧，在接收端口接收测试帧；
- e) 测试工具 1 计算发送和接收的时间标记之差，便可得一次结果；
- f) 重复步骤 c)~d) 20 次，传输时延是对 20 次测试结果的平均值；
- g) 在图 4a) 中，从测试工具 2 向测试工具 1 发送数据包，重复步骤 c)~f)，所得到时延是双向往返时延，单向时延可通过除 2 计算获得；在图 4b) 中，交换收发端口，重复步骤 c)~f)，所得到时延是单向时延。

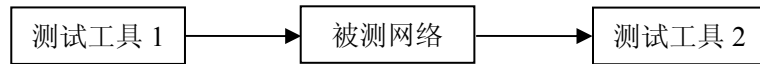


图 4a) 网络传输时延测试结构示意图

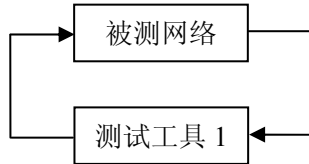


图 4b) 网络传输时延测试结构示意图

图 4 网络传输时延测试结构示意图

9.2.4.2 抽样规则

对核心层的骨干链路，应进行全部测试；对汇聚层到核心层的上联链路，应进行全部测试；对接入层到汇聚层的上联链路，以不低于 10% 的比例进行抽样测试；抽样链路数不足 10 条时，按 10 条进行计算或者全部测试；对于端到端的链路（即经过接入层、汇聚层和骨干层的用户到用户的网络路径），以不低于终端用户数量 5% 比例进行抽测，抽样链路数不足 10 条时，按 10 条进行计算或者全部测试。

9.2.4.3 合格判据

若局域网系统在 1518 字节帧长情况下，从两个方向测得的最大传输时延都小于或等于 1 ms 时，则判定局域网系统的传输时延符合 6.3.4 的要求，否则判定局域网系统的传输时延不符合 6.3.4 的要求。

9.2.5 丢包率测试方法

9.2.5.1 测试方法

测试结构示意图如图 5，测试工具 1 产生流量，测试工具 2 接收流量。若发送端口和接收端口位于同一机房，也可用一台具备双端口测试能力的测试工具实现。测试链路应分段进行，包括接入层到汇聚层链路、汇聚层到核心层链路、核心层间骨干链路、及经过接入层、汇聚层和核心层的用户到用户链路。

- a) 将两台测试工具分别连接到被测网络链路的源和目的交换机端口上；
- b) 测试工具 1 向被测网络加载 70% 的流量负荷，测试工具 2 接收负荷，测试数据帧丢失的比例；
- c) 分别需按照不同的帧大小（包括：64、128、256、512、1024、1280、1518 字节）重复步骤 c)。

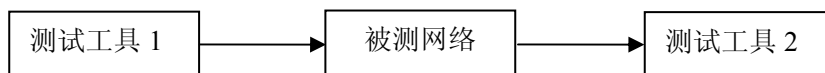


图 5 丢包率测试结构示意图

9.2.5.2 抽样规则

对核心层的骨干链路，应进行全部测试；对汇聚层到核心层的上联链路，应进行全部测试；对接入层到汇聚层的上联链路，以不低于 10% 的比例进行抽样测试；抽样链路数不足 10 条时，按 10 条进行计算或者全部测试；对于端到端的链路（即经过接入层、汇聚层和骨干层的用户到用户的网络路径），以不低于终端用户数量 5% 比例进行抽测，抽样需要覆盖所有 VLAN 到 VLAN、网段到网段间可能用到的连接，抽样链路数不足 10 条时，按 10 条进行计算或者全部测试。

9.2.5.3 合格判据

若局域网系统在不同帧大小情况下测得的丢包率都符合表 3 要求时，则判定局域网系统丢包率符合 6.3.5 的要求，否则判定局域网系统丢包率不符合 6.3.5 的要求，如果所选择的两点间测试通过，那么该两点间所包含的接入层、汇聚层和骨干层部分中间链路可不必测试。

9.2.6 以太网链路层健康状况测试方法

9.2.6.1 测试方法

以太网健康状况示意图如图 6，对于共享式以太网，可将测试工具直接连接在空闲端口上；对于交换式以太网，可将测试工具串接在被监测的以太网链路上（如交换机和主机之间、交换机和路由器之间、

交换机和交换机之间)。如果被测网络链路的设备端口具备 SNMP 流量监测功能,也可以通过直接提取 SNMP 端口来替代测试仪。

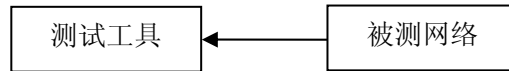


图6 以太网链路层健康状况测试结构示意图

测试链路应分段进行,包括接入层到汇聚层链路、汇聚层到核心层链路、核心层间骨干链路、及经过接入层、汇聚层和核心层的用户到用户链路。

在进行以太网碰撞和出错率时,应保证在至少有 30%的流量下进行。若没有达到该流量,则应人为加载一定的背景流量。

- a) 根据不同的网络类型,按以上方式之一,将测试工具连接到网络中的某一段;
- b) 用测试工具或通过 SNMP 流量监测功能,对被监测的网段进行流量统计(至少测试 5min 以上),测试广播和组播率、错误率、线路利用率、碰撞率等指标;
- c) 移动测试工具到其它网段,重复步骤 b),直到遍历完所有需要测试的网段。

9.2.6.2 抽样规则

对核心层的骨干链路,应进行全部测试;对汇聚层到核心层的上联链路,应进行全部测试;对接入层到汇聚层的上联链路,以不低于 30%的比例进行抽样测试;抽样链路数不足 10 条时,按 10 条进行计算或者全部测试;对于接入层的网段,以 10%的比例进行抽测。抽样网段数不足 10 个时,按 10 个进行计算或者全部测试。

9.2.6.3 合格判据

所有链路的健康状况指标都符合表4要求时,则判定局域网系统的健康状况符合6.3.6的要求,否则判定局域网系统的健康状况不符合6.3.6的要求。

9.3 验收测试项目

9.3.1 传输媒体要求

9.3.1.1 双绞线布线系统

局域网系统的传输媒体一般采用五类、超五类或六类等非屏蔽(屏蔽)双绞线布线系统。双绞线布线系统的传输指标、传输性能和测试方法应符合 GB/T 50311-2007、GB/T 50312-2007、GB/T 18233、IEC 61935:2005 等标准的规定。

9.3.1.2 多模、单模光缆布线系统

根据传输距离的长短,局域网系统可采用多模或单模光缆布线系统。光缆布线系统的传输指标和测试方法应符合 GB/T 50311-2007、GB/T 50312-2007、IEC 61280-4-1:2003、IEC 61280-4-2:1999 等标准的规定。

9.3.2 网络设备要求

9.3.2.1 集线器

集线器的端口密度、数据帧转发功能应达到产品的明示要求。相应的测试方法应符合 RFC2544 的规定。

9.3.2.2 交换机

交换机的端口密度、数据帧转发功能、数据帧过滤功能、数据帧转发及过滤的信息维护功能、运行维护功能、网络管理功能及性能指标应符合 YD/T 1099-2005、YD/T 1255—2003 的规定和产品明示要求。相应的测试方法应符合 YD/T 1141-2001、YD/T 1287-2003 的规定。

9.3.2.3 路由器

路由器设备的接口功能、通信协议功能、数据包转发功能、路由信息维护、管理控制功能、安全功能及性能指标应符合 YD/T 1096-2001、YD/T 1097-2001 的规定及产品明示要求。相应的测试方法应符合 YD/T 1098-2001、YD/T 1156-2001 的规定。

9.3.2.4 防火墙

防火墙设备,则设备的用户数据保护功能、识别和鉴别功能、密码功能、安全审计功能及性能指标

应符合 GB/T 20281-2006 的规定及产品明示要求。相应的测试方法应符合 GA 372-2001 的规定。

9.4 环境信息网络性能验收测试要求

9.4.1 系统连通性

所有联网的终端都应按使用要求全部连通。

9.4.2 链路传输速率

链路传输速率是指设备间通过网络传输数字信息的速率。对于 10M 以太网，单向最大传输速率应达到 10Mbit/s；对于 100M 以太网，单向最大传输速率应能达到 100Mbit/s；对于 1000M 以太网，单向最大传输速率应能达到 1000Mbit/s。发送端口和接收端口的利用率关系应符合表 6 的规定。

表6 发送端口和接收端口的利用率对应关系

网络类型	全双工交换式以太网		共享式以太网/半双工交换式以太网	
	发送端口利用率	接收端口利用率	发送端口利用率	接收端口利用率
10M以太网	100%	≥99%	50%	≥45%
100M以太网	100%	≥99%	50%	≥45%
1000M以太网	100%	≥99%	50%	≥45%

注：链路传输速率=以太网标称速率×接收端利用率

9.4.3 吞吐量

吞吐量是指空载网络在没有丢包的情况下，被测网络链路所能达到的最大数据包转发速率。

吞吐量测试需按照不同的帧长度（包括 64、128、256、512、1024、1280、1518 字节）分别进行测量。系统在不同帧大小情况下，从两个方向测得的最低吞吐量应符合表 7 规定。

表7 局域网系统的吞吐量要求

测试帧长 字节	10M以太网		100M以太网		1000M以太网	
	帧/秒	吞吐量	帧/秒	吞吐量	帧/秒	吞吐量
64	≥14731	99%	≥104166	70%	≥1041667	70%
128	≥8361	99%	≥67567	80%	≥633446	75%
256	≥4483	99%	≥40760	90%	≥362318	80%
512	≥2326	99%	≥23261	99%	≥199718	85%
1024	≥ 1185	99%	≥11853	99%	≥107758	90%

表2（续）

测试帧长 字节	10M以太网		100M以太网		1000M以太网	
	帧/秒	吞吐量	帧/秒	吞吐量	帧/秒	吞吐量
1280	≥ 951	99%	≥9519	99%	≥91345	95%
1518	≥ 804	99%	≥8046	99%	≥80461	99%

9.4.4 传输时延

传输时延是指数据包从发送端口（地址）到目的端口（地址）所需经历的时间。通常传输时延与传输距离、经过的设备和带宽的利用率有关。在网络正常情况下，传输时延应不影响各种业务（如视频点播、基于 IP 的语音/VoIP、高速上网等）的使用。

考虑到发送端测试工具和接收端测试工具实现精确时钟同步的复杂性，传输时延一般通过环回方式进行测量，单向传输时延为往返时延除以 2。局域网系统在 1518 字节帧长情况下，从两个方向测得的

最大传输时延应不超过 1 ms。

9.4.5 丢包率

丢包率是由于网络性能问题造成部分数据包无法被转发的比例。在进行丢包率测试时，需按照不同的帧长度（包括64、128、256、512、1024、1280、1518字节）分别进行测量，测得的丢包率应符合表8的规定。

表8 丢包率要求

测试帧长 字节	10M以太网		100M以太网		1000M以太网	
	流量负荷	丢包率	流量负荷	丢包率	流量负荷	丢包率
64	70%	≤0.1%	70%	≤0.1%	70%	≤0.1%
128	70%	≤0.1%	70%	≤0.1%	70%	≤0.1%
256	70%	≤0.1%	70%	≤0.1%	70%	≤0.1%
512	70%	≤0.1%	70%	≤0.1%	70%	≤0.1%
1024	70%	≤0.1%	70%	≤0.1%	70%	≤0.1%
1280	70%	≤0.1%	70%	≤0.1%	70%	≤0.1%
1518	70%	≤0.1%	70%	≤0.1%	70%	≤0.1%

9.4.6 以太网链路层健康状况指标

9.4.6.1 链路利用率

链路利用率指网络链路上实际传送的数据吞吐率与该链路所能支持的最大物理带宽之比。

链路的利用率包括最大利用率和平均利用率。最大利用率的值同测试统计采样间隔有一定的关系，采样间隔越短，则越能反映出网络流量的突发特性，因此最大利用率的值就越大。对于共享式以太网和交换式以太网，链路的持续平均利用率应符合表9的规定。

9.4.6.2 错误率及各类错误

错误率指网络中所产生的各类错误帧占总数据帧的比率。

常见的以太网错误类型包括长帧、短帧、有 FCS 错误的帧、超长错误帧、欠长帧和帧对齐差错帧，网络的错误率（不包括冲突）应符合表9的规定。

9.4.6.3 广播帧和组播帧

在以太网中，广播帧和组播帧数量应符合表9的要求。

9.4.6.4 冲突（碰撞）率

处于同一网段的两个站点如果同时发送以太网数据帧，就会产生冲突。冲突帧指在数据帧到达目的站点之前与其它数据帧相碰撞，而造成其内容被破坏的帧。共享式以太网和半双工交换式以太网传输模式下，冲突现象是极为普遍的。过多的冲突会造成网络传输效率的严重下降。

冲突帧同发送的总帧数之比，称为冲突（或碰撞）率。一般情况下，局域网系统的碰撞率应符合表9的规定。

表9 链路的健康状况指标要求

测试指标	技术要求	
	共享式以太网 / 半双工交换式以太网	全双工交换式以太网
链路平均利用率（带宽）	≤ 40%	≤ 70%
广播率	≤ 50 帧/秒	≤ 50 帧/秒
组播率	≤ 40 帧/秒	≤ 40 帧/秒
错误率（占总帧数）	≤ 1%	≤ 1%
冲突（碰撞）率（占总帧数）	≤ 5%	0%

9.5 环境信息网络验收测试文档要求

9.5.1 项目概况及建设需求

主要包括项目建设单位、设计单位、实施单位、项目规模，项目功能要求、项目技术指标要求。

9.5.2 设计方案

主要包括用户需求分析、组网方案、设备选型、网络拓扑图、配置功能说明、设计变更记录。

9.5.3 线路接线表和设备布置图

主要包括综合布线系统、局域网系统的设备布置图、线路端接及配线架描述文件、线路端点对应表。

9.5.4 系统参数设定表

主要包括 IP 地址分配表、子网划分表、VLAN 划分表、路由表。

9.5.5 用户操作和维护手册

主要包括系统操作说明，系统安装、恢复和数据备份说明。

9.5.6 自测报告

主要包括综合布线系统的自测报告、局域网系统的自测报告。

9.5.7 第三方测试报告

综合布线系统的第三方验收测试报告、网络设备的第三方抽查测试报告。

9.5.8 试运行报告

主要包括局域网系统试运行期间的运行记录、故障处理情况、硬件和软件系统调整情况。

9.5.9 用户报告

用户方针对局域网系统使用情况而出具的报告。

附 录 A
(规范性附录)
全国环境信息网络系统域名命名规则

A.1 顶级域名全国统一采用cn

A.2 二级域名

A.2.1 环境保护部采用gov

A.2.2 全国省级环境保护部门（包括计划单列市、新疆生产建设兵团，下同）统一采用gov

A.2.3 环境保护部直属单位统一采用org。

A.3 三级域名

环境保护部、省级环境保护部门用部门或单位的汉语拼音缩写，其中，环保局缩写为hb，如辽宁环保局缩写为lnhb；环境保护部直属单位按单位简称的汉语拼音缩写，如环境保护部信息中心缩写为xxzx。如果省级环境保护部门的汉语拼音缩写有重名，以该省简称的汉语拼音缩写为后缀加以区别。详见下表。

全国环境信息网络系统域名命名规则

序号	组织名	三级域名
	环境保护部	Zhb
省级环境保护局		
1	北京市环保局	bjhb
2	天津环保局	tjhb
3	上海环保局	shhb
4	重庆环保局	cqhb
5	河北环保局	hehb
6	山西环保局	sxhb
7	内蒙古环保局	nmghb
8	辽宁环保局	lnhb
9	吉林环保局	jlhb
10	黑龙江环保局	hljhb
11	江苏环保局	jshb
12	浙江环保局	zjhb
13	安徽环保局	ahhb
14	福建环保局	fjhb
15	江西环保局	jxhb
16	山东环保局	sdhb
17	河南环保局	hahb
18	湖北环保局	hbhb
19	湖南环保局	hnhb
20	广东环保局	gdhb
21	广西环保局	gxhb
22	海南环保局	hihb
23	四川环保局	schb
24	贵州环保局	gzhb
25	云南环保局	ynhb
26	西藏环保局	xzhb

27	陕西环保局	snhb
28	甘肃环保局	gshb
29	青海环保局	qhnb
30	宁夏环保局	nxhb
31	新疆环保局	xjhb
	新疆生产建设兵团环保局	xjbthb
计划单列市环境保护局		
1	青岛市环保局	qdhb
2	宁波市环保局	nbhb
3	厦门市环保局	xmhb
4	深圳市环保局	szhb
5	大连市环保局	dlhb
环境保护部直属单位		
1	环境保护部信息中心	xxzx
2	环境保护部宣传教育中心	xjzx
3	中国环境监测总站	jczz

A.4 四级和四级以下域名由省级环境保护管理部门自行规划

附 录 B
(规范性附录)
全国环境信息网络 IP 地址规划表

序号	单位名称	局域网络 IP 地址	备用网络 IP 地址	网络设备 IP 地址
1	总局	10.10.0.0/16	10.101-104.0.0/16	10.1-9.10.0/24
2	北京市	10.11.0.0/16	10.105-108.0.0/16	10.1-9.11.0/24
3	天津市	10.12.0.0/16	10.109-112.0.0/16	10.1-9.12.0/24
4	上海市	10.31.0.0/16	10.113-116.0.0/16	10.1-9.31.0/24
5	重庆市	10.50.0.0/16	10.117-120.0.0/16	10.1-9.50.0/24
6	河北省	10.13.0.0/16	10.121-124.0.0/16	10.1-9.13.0/24
7	山西省	10.14.0.0/16	10.125-128.0.0/16	10.1-9.14.0/24
8	内蒙古	10.15.0.0/16	10.129-132.0.0/16	10.1-9.15.0/24
9	辽宁省	10.21.0.0/16	10.133-136.0.0/16	10.1-9.21.0/24
10	吉林省	10.22.0.0/16	10.137-140.0.0/16	10.1-9.22.0/24
11	黑龙江	10.23.0.0/16	10.141-144.0.0/16	10.1-9.23.0/24
12	江苏省	10.32.0.0/16	10.145-148.0.0/16	10.1-9.32.0/24
13	浙江省	10.33.0.0/16	10.149-152.0.0/16	10.1-9.33.0/24
14	安徽省	10.34.0.0/16	10.153-156.0.0/16	10.1-9.34.0/24
15	福建省	10.35.0.0/16	10.157-160.0.0/16	10.1-9.35.0/24
16	江西省	10.36.0.0/16	10.161-164.0.0/16	10.1-9.36.0/24
17	山东省	10.37.0.0/16	10.165-168.0.0/16	10.1-9.37.0/24
18	河南省	10.41.0.0/16	10.169-172.0.0/16	10.1-9.41.0/24
19	湖北省	10.42.0.0/16	10.173-176.0.0/16	10.1-9.42.0/24
20	湖南省	10.43.0.0/16	10.177-180.0.0/16	10.1-9.43.0/24
21	广东省	10.44.0.0/16	10.181-184.0.0/16	10.1-9.44.0/24
22	广西省	10.45.0.0/16	10.185-188.0.0/16	10.1-9.45.0/24
23	海南省	10.46.0.0/16	10.189-192.0.0/16	10.1-9.46.0/24
24	四川省	10.51.0.0/16	10.193-196.0.0/16	10.1-9.51.0/24
25	贵州省	10.52.0.0/16	10.197-200.0.0/16	10.1-9.52.0/24
26	云南省	10.53.0.0/16	10.201-204.0.0/16	10.1-9.53.0/24
27	西藏区	10.54.0.0/16	10.205-208.0.0/16	10.1-9.54.0/24
28	陕西省	10.61.0.0/16	10.209-212.0.0/16	10.1-9.61.0/24
29	甘肃省	10.62.0.0/16	10.213-216.0.0/16	10.1-9.62.0/24
30	青海省	10.63.0.0/16	10.217-220.0.0/16	10.1-9.63.0/24
31	宁夏区	10.64.0.0/16	10.221-224.0.0/16	10.1-9.64.0/24
32	新疆区	10.65.0.0/16	10.225-228.0.0/16	10.1-9.65.0/24
33	新疆兵团	10.66.0.0/16	10.229-232.0.0/16	10.1-9.66.0/24
34	大连	10.24.0.0/16		10.1-9.24.0/24
35	青岛	10.38.0.0/16		10.1-9.38.0/24
36	宁波	10.39.0.0/16		10.1-9.39.0/24
37	深圳	10.47.0.0/16		10.1-9.47.0/24
38	厦门	10.40.0.0/16		10.1-9.40.0/24

路由器地址广域网地址段为：10.1.0.0/16，防火墙地址广域网地址段为：10.2.0.0/16

例如：以北京市环保局为例：总局核心路由器对应北京市环保局路由器地址为：10.1.11.254/24，北京市环保局对应总局的路由器地址为：10.1.11.253/24，北京市环保局路由器连接防火墙的端口地址为：10.2.11.254/24，防火墙连接路由器的地址为：10.2.11.253/24，防火墙连接内部局域网的端口为：10.11.1.254/24，北京市环保局局域网IP地址段为：10.11.0.0/16。

附录 C
(资料性附录)
路由器性能指标

性能名称 种类	高端路由器	中端路由器	低端路由器
吞吐量	≥30Mpps		
丢包率	轻载条件下（端吞吐量10%）丢包率<0.05% 重载条件下（端吞吐量80%）丢包率<0.1%		轻载条件下（端吞吐量10%）丢包率<0.1% 重载条件下（端吞吐量80%）丢包率<0.3%
容量	≥700Gbps		
接口转发时延	在最坏情况下，1518字节长度及以下的IP包时延均应<1ms		64字节IP包，时延<1ms 512字节IP包，时延<15ms 1815字节IP包，时延<350ms
路由表容量	支持至少250000条路由，平均每个目的地址至少提供2个路径 支持至少50个BGP对等 支持至少50个IGP邻居		
可靠性和可用性要求	系统必须达到或超过99.999%的可用性 系统无故障工作时间>40万小时 系统故障恢复时间<30分钟 支持热插拔功能		

附 录 D
(规范性附录)
防火墙安全等级划分

D.1 一级防火墙功能要求细目

功能分类	功能项目要求
包过滤	支持默认禁止原则
	支持基于 IP 地址的访问控制
	支持基于端口的访问控制
	支持基于协议类型的访问控制
应用代理	支持应用层协议代理
NAT	支持双向 NAT
流量统计	支持根据 IP 地址、协议、时间等参数对流量进行统计
	支持统计结果的报表形式输出
安全审计	支持记录来自外部网络的被安全策略允许的访问请求
	支持记录来自内部网络和 DMZ 的被安全策略允许的访问请求
	支持记录任何试图穿越或到达防火墙的违反安全策略的访问请求
	支持记录防火墙管理行为
	审计记录内容
	支持日志的访问授权
	支持日志的管理
提供日志管理工具	
管理	支持对授权管理员的口令鉴别方式
	支持对授权管理员、可信主机、主机和用户进行身份鉴别
	支持本地和远程管理
	支持设置和修改安全管理相关的数据参数
	支持设置、查询和修改安全策略
	支持管理审计日志

D.2 二级防火墙增加的功能要求细目

二级防火墙除需满足一级防火墙的功能要求外，还需增加如附录C-2所示的功能要求。

功能分类	功能项目要求
包过滤	支持基于 MAC 地址的访问控制
	支持基于时间的访问控制
	支持基于用户自定义安全策略的访问控制
状态检测	支持基于状态检测技术的访问控制
深度包检测	支持基于 URL 的访问控制
	支持基于电子邮件信头的访问控制
应用代理	支持应用层协议代理
NAT	支持动态 NAT
IP/MAC 地址绑定	支持 IP/MAC 地址绑定
	支持检测 IP 地址盗用
动态开放端口	支持 FTP 的动态端口开放
策略路由	支持根据数据包信息来设置路由策略
	支持设置多个路由表
带宽管理	支持客户端占用带宽大小限制
	支持物理设备状态检测

双机热备	支持 VRRP 和 STP 协议
负载均衡	支持将网络负载均衡到多台服务器
流量统计	支持根据 IP 地址、协议、时间等参数对流量进行统计
	支持统计结果的报表形式输出
安全审计	支持记录对防火墙系统自身的操作
	支持记录在防火墙管理端口上的认证请求
	支持对日志记录存储和备份的安全
	支持日志记录存储和备份的安全
	支持日志管理工具管理日志
	支持日志的统计分析和报表生成
管理	支持日志的集中管理
	支持智能卡、USB 钥匙等身份鉴别信息载体
	支持鉴别失败处理
	支持授权管理员、可信主机、主机和用户的唯一安全属性
功能分类	功能项目要求
管理	支持远程管理安全
管理	支持防火墙状态和网络数据流状态监控

D.3 二级防火墙增加的功能要求细目

三级产品除需满足一、二级产品的功能要求外，还需增加如附录C-3所示的功能要求。

功能分类	功能项目要求
深度包过滤	支持基于文件类型的访问控制
	支持基于用户的访问控制
	支持基于关键字的访问控制
	支持基于电子邮件信头的访问控制
应用代理	支持透明应用代理
动态开放端口	支持以 H.323 协议建立视频会议
	支持 SQL*NET 数据库协议
	支持 VLAN
带宽管理	支持动态客户端带宽管理
双机热备	支持链路状态检测的双机热备
负载均衡	支持集群工作模式的负载均衡
VPN	支持 IPSec 协议
	支持建立“防火墙至防火墙”和“防火墙至客户机”两种形式的 VPN
	支持 VPN 认证
	加密算法和验证算法符合国家密码管理的有关规定
协同联动	支持与其他安全产品的协同联动
	支持联动安全产品的身份鉴别
安全审计	支持记录协同联动响应行为事件
	支持日志存储耗尽处理机制
管理	支持生物特征鉴别方式
	支持管理员权限划分

附 录 E
(资料性附录)
防火墙性能指标

性能名称 种类	十兆防火墙	百兆防火墙	千兆及千兆以上防火墙
吞 吐 量	防火墙在只有一条允许规则和不丢包的情况下，应达到的吞吐量指标：		
	对 64 字节短包，应不小于线速的 20%，	对 64 字节短包，应不小于线速的 20%，	对 64 字节短包，应不小于线速的 35%，
	对 512 字节中长包，应不小于线速的 70%，	对 512 字节中长包，应不小于线速的 70%，	对 512 字节中长包，应不小于线速的 80%，
	对 1518 字节长包，应不小于线速的 90%，	对 1518 字节长包，应不小于线速的 90%，	对 1518 字节长包，应不小于线速的 95%，
	在添加大数量访问控制规则（不同的 200 余条）的情况下，防火墙的吞吐量下降应不大于原吞吐量的 3%		
延 迟	最大延迟不应超过 1ms	最大延迟不应超过 500 μ s	最大延迟不应超过 90 μ s
	在添加大数量访问控制规则（不同的 200 余条）的情况下，防火墙延迟所受的影响应不大于原吞吐量的 3%		
最大并发连接数	最大并发连接数应不小于 1000 个	最大并发连接数应不小于 10000 个	最大并发连接数应不小于 100000 个
最大连接速率	最大连接速率应不小于每秒 500 个	最大连接速率应不小于每秒 1500 个	最大连接速率应不小于每秒 5000 个

附 录 F
(规范性附录)
对不同高度房间的火灾探测器的选择

房间高度 h (m)	感烟探测器	感温探测器			火焰探测器
		一级	二级	三级	
$12 < H \leq 20$	不适合	不适合	不适合	不适合	适合
$8 < H \leq 12$	适合	不适合	不适合	不适合	适合
$6 < H \leq 8$	适合	适合	不适合	不适合	适合
$4 < H \leq 6$	适合	适合	适合	不适合	适合
$H \leq 4$	适合	适合	适合	适合	适合

附 录 G
(资料性附录)
感烟、感温探测器的保护面积和保护半径

火灾探测器的种类	地面面积 S(m ²)	房间高度 h(m)	探测器的保护面积 A 和保护半径 R					
			屋顶坡度 θ					
			$\theta \leq 15^\circ$		$15^\circ < \theta \leq 30^\circ$		$\theta > 30^\circ$	
			A(m ²)	R(m)	A(m ²)	R(m)	A(m ²)	R(m)
感烟探测器	$S \leq 80$	$h \leq 12$	80	6.7	80	7.2	80	9.0
	$S > 80$	$6 < h \leq 12$	80	6.7	100	8.0	120	9.9
		$h \leq 6$	60	5.8	80	7.2	100	9.0
感温探测器	$S \leq 30$	$h \leq 8$	30	4.4	30	4.9	30	5.5
	$S > 30$	$H \leq 8$	20	3.6	30	4.9	40	6.3

