HJ

中华人民共和国国家环境保护标准

HJ 460－2009

环境信息网络建设规范

Specification for environmental information network building

2009-03-20 发布　　2009-06-01 实施

环　境　保　护　部　发布

中华人民共和国环境保护部
公　告

2009 年　第 13 号

为贯彻《中华人民共和国环境保护法》，促进环境信息化建设，现批准《环境信息网络建设规范》等两项标准为国家环境保护标准，并予发布。

标准名称、编号如下：

一、环境信息网络建设规范（HJ 460—2009）

二、环境信息网络管理维护规范（HJ 461—2009）

以上标准自 2009 年 6 月 1 日起实施，由中国环境科学出版社出版，标准内容可在环境保护部网站（www.mep.gov.cn）查询。

特此公告。

2009 年 3 月 20 日

目　　次

前　言

为加强和规范全国环境信息网络的统一建设、管理，实现全国环境保护部门网络互连互通，保障环境业务数据的实时、有效传输，为环境保护管理和决策提供信息服务，制定本标准。

本标准规定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 地址和域名规划，机房建设等技术要求。

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

本标准由环境保护部科技标准司组织制订。

本标准起草单位：环境保护部信息中心。

本标准由环境保护部 2009 年 3 月 20 日批准。

本标准自 2009 年 6 月 1 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，以及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 地址和域名规划，机房建设等技术要求。

本标准适用于环境保护部、各省、自治区、直辖市环境保护厅（局）、新疆生产建设兵团环境保护局（以下简称省级环境保护厅（局））和地市级环境保护局环境信息网络建设工作。区、县级环境保护局及各级环境保护部门直属单位、派出机构亦可参照执行。

2 规范性引用文件

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

GB/T 1988—1998 信息技术 信息交换用七位编码字符集

GB/T 2260 中华人民共和国行政区划代码

GB/T 2887 电子计算机场地通用规范

GB 18030—2005 信息技术 中文编码字符集

GB/T 18233—2008 信息技术 用户建筑群的通用布缆

GB/T 19668 信息化工程监理规范

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 20281—2006 信息安全技术 防火墙技术要求和测试评价方法

GB/T 21671—2008 基于以太网技术的局域网系统验收测评规范

GB 50057—1994 建筑物防雷设计规范

GB 50174 电子计算机机房设计规范

GB/T 50311—2007 建筑与建筑群综合布线系统工程设计规范

GB/T 50312—2007 综合部线系统工程验收规范

GA 372—2001 防火墙产品的安全功能检测

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 1098—2001 路由器测试规范——低端路由器

YD/T 1099—2005 千兆比以太网交换机设备技术规范

YD/T 1141—2001 千兆比以太网交换机测试方法

YD/T 1156—2001 路由器测试规范——高端路由器

YD/T 1170—2001 IP 网络技术要求——网络总体

YD/T 1255—2003 具有路由功能的以太网交换机技术要求

YD/T 1287—2003 具有路由功能的以太网交换机测试方法

IEC 61935：2005 按照 GB/T 18233/ISO/IEC 11801 的平衡通信布缆测试 第 1 部分：已安装布缆

IEC 61280-4-1：2003 纤维光学通信子系统试验程序 第 4-1 部分：光缆设备及链接 多模光缆设备的衰减测量

IEC 61280-4-2：1999　光纤通信子系统基本试验程序　第 4-2 部分：光缆设施　单模光缆设施衰减

RFC 2544　网络互联设备基准测试方法

3　术语和定义

下列术语和定义适用于本标准。

3.1　环保系统骨干网及核心节点

全国环境信息网络分为三级骨干网：

一级骨干网：环境保护部至各省级环境保护厅（局）的网络互连。

二级骨干网：省级环境保护厅（局）至其所属地市级（含计划单列城市和副省级城市）环境保护局的网络互连，以及直辖市环境保护局至其区、县级环境保护局的网络互连。

三级骨干网：各地市级（含计划单列城市和副省级城市）环境保护局至其所属县、区级环境保护局的网络互连。

全国环境信息网络分为四级节点：

环境保护部为一级节点，各省级环境保护厅（局）为二级节点，各地市级（含计划单列城市和副省级城市）环境保护局为三级节点，区、县级环境保护局为四级节点。

3.2　环保系统电子政务内网

环境保护部及全国各省级、计划单列城市和副省级城市环境保护厅（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，须与互联网和电子政务外网物理隔离。

3.3　环保系统电子政务外网

环境保护部及全国各级环境保护厅（局）内部局域网通过专线互连，用于污染源监测数据传输、环境保护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，须与互联网安全隔离。

3.4　环保系统城域网

环境保护部连接其在京直属单位所形成的网络；省级环境保护厅（局）连接其同城直属单位所形成的网络；地市级环境保护局连接其同城直属单位所形成的网络。

3.5　国家级环境信息广域网

指环境保护部通过专线连接各省级环境保护厅（局）所形成的广域网。

3.6　省级环境信息广域网

指省级环境保护厅（局）通过专线连接其管辖范围内各地市级（含计划单列城市和副省级城市）环境保护局所形成的广域网。

3.7　缩略语

DMZ	非军事区	Demilitary Zone
DNS	域名解析系统	Domain Name System
FTP	文件传输协议	File Transfer Protocol
HTTP	超文本传输协议	Hypertext Transfer Protocol
IDS	入侵检测系统	Intrusion Detection System
IP	互联网协议	Internet Protocol
NAT	网络地址转换器	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
VLAN	虚拟局域网	Virtual Local Area Network
VPN	虚拟专用网	Virtual Private Network

4 全国环境信息网络建设原则和基本流程

4.1 网络建设原则

网络建设依据以下主要原则：

a）满足各级环境保护部门的业务应用系统的要求；

b）利用已有的网络资源，与已有的专用政务网络兼容；

c）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；

d）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；

e）应是安全可靠、可管理、可控制和可扩展的网络，具有服务分类和服务质量保障能力。

4.2 网络建设基本流程

4.2.1 立项阶段

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

4.2.2 确定监理机构

电子政务项目实行工程监理制。项目建设单位应按照信息系统工程监理的有关规定，委托具有信息系统工程相应监理资质的工程监理单位，对项目建设进行工程监理。有关规定见 GB/T 19668。

4.2.3 招标投标阶段

环境信息网络建设工程、建设项目招标投标活动应满足以下要求：

a）遵守《工程建设项目施工招标投标办法》的规定；

b）遵守《计算机信息系统集成资质管理办法》的规定；

c）工程建设项目属于《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，须通过招标选择施工单位，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》的单位来承建涉密系统；

e）遵守其他相关技术标准的规定。

4.2.4 工程设计阶段

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合同的要求。

4.2.5 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。

4.2.6 工程验收阶段

重大项目的竣工验收，必须有各级环境保护信息部门参与评审；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、县各级环境保护信息部门参加。环境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，符合网络建设工程招标合同的要求，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。

4.2.7 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做好相应的安排。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。

5 全国环境信息骨干网网际互连

5.1 网络结构及拓扑

全国环境信息网络结构可分为三级骨干网，四级节点。

5.1.1 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境保护部门连接国际互联网的出口。局域网（外网）为星型拓扑结构。

5.1.2 广域网网络结构及拓扑

全国环境信息广域网络主要包括：一、二、三级骨干网。广域网为星型拓扑结构。

5.1.3 环保系统城域网网络结构及拓扑

环保系统城域网是全国各级环境保护部门至同城直属单位的网络互连，为星型拓扑结构。

5.2 链路和带宽

5.2.1 互联网链路和带宽

互联网的链路由运营商提供。互联网的带宽根据业务需求确定，以下为带宽升级的参考标准：

a）当一条链路具有高的利用率，如果优先级高的流量还可以被正常路由，业务应用质量尚可，Ping 测试时所经历的延迟也不显著，可不升级带宽；

b）如果优先级高的流量的可用带宽接近带宽的极限，宜升级带宽；

c）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，应升级互联网带宽。

5.2.2 城域网链路和带宽

环境保护部与在京直属单位的网络互连应采用专线连接，带宽不低于 2 M，环境保护部连接环境保护部信息中心数据中心带宽不低于 100 M。

省级环境保护厅（局）与其同城直属单位的网络互连可采用专线连接，带宽不低于 2 M。

地市级环境保护局与其同城直属单位的网络互连可采用专线连接，带宽不低于 2 M。

5.2.3 广域网链路和带宽

一级骨干网采用专线连接，带宽不低于 6 M。

二级骨干网采用专线连接，带宽不低于 2 M。

三级骨干网可采用专线连接，带宽不低于 2 M，也可采用 VPN 技术，带宽不低于 512 K。

5.3 网络接入设备

5.3.1 接入设备类型

5.3.1.1 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。

5.3.1.2 城域网接入设备

环保系统城域网接入设备等级主要由设备所在节点角色功能决定。环境保护部与在京直属单位的网络互连，采用高端路由器，各在京直属单位可采用低端路由器。各省级环境保护厅（局）与同城直属单位的网络互连，采用中高端路由器，各同城直属单位可采用低端路由器。各地市级环境保护局与同城直属单位的网络互连，采用中低端路由器，各同城直属单位可采用低端路由器。

5.3.1.3 广域网接入设备

全国环境信息广域网一级骨干网络中，环境保护部为一级节点，应采用高端路由器。二级骨干网络中，各省级环境保护厅（局）为二级节点，采用中高端路由器；各地市级环境保护局采用中低端路由器。

5.3.2 接入设备要求

5.3.2.1 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。

a）高端路由器功能主要包括：

1）路由器的功能特性；

2）通信规程；

3）协议要求；

4）路由协议；

5）接口类型；

6）网管协议等。

b）高端路由器性能指标主要包括：

1）吞吐量；

2）丢包率；

3）包转发率；

4）可靠性和安全性；

5）路由表容量；

6）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。路由器性能指标参见附录 C。

5.3.2.2 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络与二级网络的路由器。

a）低端路由器功能主要包括：

1）路由器的功能特性；

2）通信规程；

3）协议要求；

4）路由协议；

5）接口类型；

6）网管协议等。

b）低端路由器性能指标主要包括：

1）接口转发时延；

2）丢包率；

3）包转发率；

4）内存容量等。

有关低端核心路由器的详细要求见 YD/T 1096—2001。路由器性能指标参见附录 C。

5.4 网络安全设备

5.4.1 安全设备类型

5.4.1.1 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。

5.4.1.2 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、省级环境保护厅（局）、地市级环境保护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、县级环境保护局可以采用软件防火墙。

5.4.2 防火墙设备

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。

a）防火墙设备主要功能：

1）包过滤；
2）应用代理；
3）内容过滤；
4）NAT；
5）动态开放端口；
6）VPN；
7）安全审计；
8）安全管理等。

b）防火墙设备主要性能指标：
1）吞吐量；
2）延迟；
3）最大并发连接数；
4）最大连接速率。

c）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：
1）抗渗透；
2）恶意代码防御；
3）系统应构建于安全增强的操作系统之上。

d）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：
1）管理配置；
2）交付与操作；
3）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。

有关防火墙设备要求详见 GB/T 20281—2006。

5.4.3 入侵检测设备

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。

a）入侵检测设备主要功能：
1）数据探测；
2）入侵分析；
3）入侵响应；
4）管理控制；
5）检测结果处理；
6）安全审计。

b）入侵检测设备主要性能指标：
1）误报率；
2）漏报率。

有关入侵检测系统要求详见 GB/T 20275—2006。

5.4.4 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：

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：

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 和 GB/T 20280—2006。

5.5 网络管理平台

5.5.1 网络管理软件系统平台主要功能要求

5.5.1.1 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。

5.5.1.2 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、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。

5.5.1.3 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，可以清楚地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，可以准确地标识出 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。

5.5.1.4 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。这种分权管理能力，可以充分保证全国环境信息网络管理分布式管理的需要，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。

5.6 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。

5.6.1 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：通信协议采用超文本传送协议（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。

5.6.2 E-mail

a）基本技术：利用电子邮件技术；

b）协议及标准：通信协议采用简单邮件传输协议（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。

5.6.3 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：通信协议采用 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。

5.6.4 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：

1）点对点隧道协议：点到点隧道协议（PPTP）；

2）第二层隧道协议：第 2 层隧道协议（L2TP）；

3）第三层隧道协议：通用路由协议 GRE（参见 RFC 1071/1072）；

4）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。

5.6.5 多媒体会议业务

a）基本技术。基于 TCP/IP 的会议业务。由于 LAN 上得不到稳定的业务质量，因而需要图像编码和语音编码的尺度均可伸缩。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。为了进一步保证质量，要有一定的信道带宽预约机制。

b）协议和标准：

1）通信协议：H.323、H.225、RTP、UDP、HTTP；

2）服务质量协议：RSVP、Diffserv；

3）语音编码协议：G.723.1、G.729；

4）图像编码协议：H.263；

5）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。

5.7 全国环保系统IP地址规划

5.7.1 原则

a）全国环保系统网络地址统一规划，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。

5.7.2 全国环保系统网络地址

全国环保系统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全国环境信息网络所需使用的地址，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。此地址作为全国环境信息网络内部地址专用，不使用于互联网；

b）互联共享地址，是指全国环境信息网络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。

5.8 全国环保系统域名管理

5.8.1 原则

a）全国环保系统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）全国环保系统电子政务内网域名系统采用三级域名管理，全国环保系统电子政务外网域名系统可采用多级域名管理。

5.8.2 中文域名

5.8.2.1 使用原则

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

b）不应使用其他国家或地区名称、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。

5.8.2.2 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、字母或

数字开始，以汉字、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 中规定的字符。

5.8.3 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。

5.8.4 英文域名

英文域名使用原则同中文域名使用原则，见 5.8.2.1。

全国环保系统在全国环境信息网络中使用的域名均可从各级环境保护部门环境信息主管部门申请。次一级域名为各省级环境保护厅（局）名，再下一级域名由分配到次一级域名的各省自定，各下级单位域名由上级部门统一管理。全国环境信息网络系统域名命名规则见附录 A。

6 全国环境信息局域网网络建设

6.1 环保系统电子政务内网局域网网络建设

6.1.1 网络平台

6.1.1.1 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 1 000 Mbit/s，到桌面的传输速率不低于 100 Mbit/s。

6.1.1.2 网络接口设备

核心网络设备网络接口速率不低于 1 000 Mbit/s；网络设备网络接口速率不低于 100 Mbit/s；为客户端提供接入服务的交换设备接口速率不低于 100 Mbit/s。

核心应用服务器端均应配备速率不低于 1 000 Mbit/s 的网络接口卡；普通应用服务器端均应配备速率不低于 100 Mbit/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 100 Mbit/s。

6.1.1.3 网络交换设备

网络交换设备主要应用于局域网网络建设，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。

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，其主要功能包括：

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。

除实现数据帧转发功能外，第 3 层交换设备还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端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。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。其主要功能包括：

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。

6.1.1.4 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；服务器应具有高度的可靠性、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：根据国家环境数据中心、环境数据共享服务平台等建设要求，从目前和发展的角度考虑各种软硬件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。

6.1.2 网络存储设备

存储设备可根据实际需求选用容量合适的存储设备，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、备份软件等。

6.1.3 网络综合布线

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至少能满足未来 5～10 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。关于网络综合布线标准详见 GB/T 18233—2008、GB/T 50311—2007、GB/T 50312—2007。

6.1.4 安全平台

6.1.4.1 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。

a）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。这个监控中心应具备以下功能：

1）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。

2）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。

3）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。

4）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。

5）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。

6）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。

7）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。

8）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。

b）网络防病毒系统客户端基本功能：

1）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。

2）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。

3）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尚未更新时，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，使尚未入侵的病毒无法入侵，使已经入侵的病毒无法扩散。

4）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。

5）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。

6）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。

c）单机版防病毒软件可以参照 b）网络防病毒系统客户端基本功能。

6.1.4.2 网络安全域逻辑划分

环保系统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区域。

在环保系统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。

6.1.5 用户平台

6.1.5.1 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。

6.1.5.2 用户操作系统

计算机需安装具有较强网络功能的操作系统。系统应操作便捷，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。

6.1.5.3 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。

6.2 环保系统电子政务外网局域网网络建设

6.2.1 网络平台

6.2.1.1 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 地址应使用私有内部地址，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 1 000 Mbit/s，到桌面的传输速率不低于 100 Mbit/s。

6.2.1.2 网络传输设备

核心应用服务器端均应配备速率不低于 1 000 Mbit/s 的网络接口卡；普通应用服务器端均应配备速率不低于 100 Mbit/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 100 Mbit/s。

6.2.1.3 网络交换设备

见 6.1.1.3。

6.2.1.4 网络服务器

见 6.1.1.4。

6.2.2 网络存储设备

见 6.1.2。

6.2.3 网络综合布线

见 6.1.3。

6.2.4 安全平台

6.2.4.1 网络防病毒系统

见 6.1.4.1。

6.2.4.2 网络安全域逻辑划分

环保系统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、共享域（DMZ 区域）和内部域，安全等级从低到高，内容如下：

a）外部域主要是指各级环境保护部门连接的外部网络。

b）共享域（DMZ 区域）主要指各级环境保护部门与外部接入部分和对外提供服务的逻辑边界部分，如各级环境保护部门对外提供访问的 Web 服务器、MAIL 服务器等。

c）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。

7 全国环境信息网络机房建设

7.1 机房建设的基本要求

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。

7.2 机房环境

机房环境应符合 GB 50174 和 GB/T 2887 的规定。

7.3 不间断电源（UPS）

7.3.1 UPS额定输出容量

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。

7.3.2 UPS机型

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，用户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：用户应为它的交流旁路市电输入的相线和中线配置可单相承担 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：用户应将 UPS 输出端的负载不平衡度控制在不超过 30%～40%范围内。

7.3.3 UPS容错冗余供电系统

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）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，当主机 UPS 出故障时，改由从机 UPS 带载。由于这种冗余工作方式没有“扩容”功能和可能出现 4 ms（毫秒）的供电中断，而使其应用范围有限。

b）“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，当其中一台 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无故障工作时间 MTBF 是单机 UPS 的 7～8 倍，从而大大提高系统的可靠性。

c）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。

7.3.4 UPS运行环境

a）应将 UPS 用蓄电池组置于 20～25℃的环境下运行，无论 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。

7.3.5 UPS供电系统中的中线截面积

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。

7.3.6 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。

7.4 机房空气调节系统

机房空气调节系统应符合 GB 50174 的规定。

7.5 机房消防

机房消防应符合 GB 50174 的规定。

7.6 防雷、接地保护系统

机房防雷、接地保护系统应符合 GB 50057、GB 50169、GB/T 2887 的规定。

8 全国环境信息网络验收测试

8.1 验收测试范围

测试范围包括广域网和城域网链路测试、局域网系统测试、网络设备测试等。

8.2 验收测试方法

验收测试方法应符合 GB/T 21671—2008 的规定。

8.3 验收测试项目

8.3.1 传输媒体要求

8.3.1.1 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。

8.3.1.2 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。

8.3.2 网络设备要求

8.3.2.1 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 RFC 2544 的规定。

8.3.2.2 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。

8.3.2.3 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。

8.3.2.4 防火墙

防火墙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。

8.4 局域网络性能验收测试要求

局域网络性能验收测试方法应符合 GB/T 21671—2008 的规定。

8.5 环境信息网络验收测试文档要求

8.5.1 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。

8.5.2 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。

8.5.3 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。

8.5.4 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。

8.5.5 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。

8.5.6 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。

8.5.7 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。

8.5.8 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。

8.5.9 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
（资料性附录）
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zhb

A.2 二级域名

环境保护部、省级环境保护厅（局）用部门或单位的汉语拼音缩写，其中，环境保护厅（局）缩写为 hb，如辽宁省环境保护局缩写为 lnhb，域名中省、直辖市、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。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。详见表 A.1。

各市、县级环境保护局域名可由上级单位统一规划制定。

表 A.1 环境信息网络系统二级域名表

序号	组织名	二级域名
1	环境保护部	zhb
省级环境保护部门		
1	北京市	bjhb
2	天津市	tjhb
3	河北省	hehb
4	山西省	sxhb
5	内蒙古自治区	nmghb
6	辽宁省	lnhb
7	吉林省	jlhb
8	黑龙江省	hljhb
9	上海市	shhb
10	江苏省	jshb
11	浙江省	zjhb
12	安徽省	ahhb
13	福建省	fjhb
14	江西省	jxhb
15	山东省	sdhb
16	河南省	hahb
17	湖北省	hbhb
18	湖南省	hnhb
19	广东省	gdhb
20	广西壮族自治区	gxhb
21	海南省	hihb
22	重庆市	cqhb
23	四川省	schb
24	贵州省	gzhb
25	云南省	ynhb
26	西藏自治区	xzhb
27	陕西省	snhb
28	甘肃省	gshb
29	青海省	qhhb
30	宁夏回族自治区	nxhb

续表

序号	组织名	二级域名
31	新疆维吾尔自治区	xjhb
32	新疆生产建设兵团	xjbthb
计划单列市环境保护局		
1	大连市环境保护局	dlhb
2	宁波市环境保护局	nbhb
3	厦门市环境保护局	xmhb
4	青岛市环境保护局	qdhb
5	深圳市环境保护局	szhb
环境保护部直属单位、派出机构		
1	环境保护部应急与事故调查中心	yjsgdczx
2	中国环境科学研究院	zghjkxy
3	中国环境监测总站	zghjjczz
4	中日友好环境保护中心	zryhhjbhzx
5	中国环境报社	zghjbs
6	中国环境科学出版社	zghjkxcbs
7	环境保护部核安全中心	haqzx
8	环境保护部环境保护对外合作中心	hjbhdwhzzx
9	环境保护部南京环境科学研究所	njhjkxyjs
10	环境保护部华南环境科学研究所	hnhjkxyjs
11	环境保护部环境规划院	hjghy
12	环境保护部环境工程评估中心	hjgcpgzx
13	环境保护部华北环境保护督查中心	hbhjbhdczx
14	环境保护部华东环境保护督查中心	hdhjbhdczx
15	环境保护部华南环境保护督查中心	hnhjbhdczx
16	环境保护部东北环境保护督查中心	dbhjbhdczx
17	环境保护部西北环境保护督查中心	xbhjbhdczx
18	环境保护部西南环境保护督查中心	xnhjbhdczx
19	环境保护部北方核安全监督站	bfhaqjdz
20	环境保护部上海核安全监督站	shhaqjdz
21	环境保护部广东核安全监督站	gdhaqjdz
22	环境保护部四川核安全监督站	schaqjdz
23	环境保护部东北核与辐射安全监督站	dbhfsaqjdz
24	环境保护部西北核与辐射安全监督站	xbhfsaqjdz
25	中国环境科学学会	zghjkxxh
26	中国环境保护产业协会	zghjbhcyxh
27	中华环境保护基金会	zhhjbhjjh
28	中国环境文化促进会	zghjwhcjh
29	中国环境新闻工作者协会	zghjxwgzzxh
30	中华环保联合会	zhhblhh
31	环境保护部北京会议与培训基地	bjhypxjd
32	环境保护部北戴河技术交流中心	bdhjsjlzx
33	环境保护部兴城环境管理研究中心	xchjglyjzx

A.3 三级和三级以下域名

三级和三级以下域名由省级环境保护管理部门自行规划。

本标准中的域名作为全国环境信息网络专有域名。各单位可参考制定互联网域名命名规则，未注册部门或单位可参照本标准注册域名，已注册并正在应用的域名不要求注销。

附 录 B
（规范性附录）
全国环境信息网络 IP 地址规划表

全国环境信息网络 IP 地址规划表，包括各局域网络 IP 地址、备用网络 IP 地址、网络设备 IP 地址，见表 B.1。

表 B.1 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	环境保护部	10.10.0.0/16	10.101-104.0.0/16	10.1-9.10.0/24
省级环境保护部门				
1	北京市	10.11.0.0/16	10.105-108.0.0/16	10.1-9.11.0/24
2	天津市	10.12.0.0/16	10.109-112.0.0/16	10.1-9.12.0/24
3	河北省	10.13.0.0/16	10.121-124.0.0/16	10.1-9.13.0/24
4	山西省	10.14.0.0/16	10.125-128.0.0/16	10.1-9.14.0/24
5	内蒙古	10.15.0.0/16	10.129-132.0.0/16	10.1-9.15.0/24
6	辽宁省	10.21.0.0/16	10.133-136.0.0/16	10.1-9.21.0/24
7	吉林省	10.22.0.0/16	10.137-140.0.0/16	10.1-9.22.0/24
8	黑龙江省	10.23.0.0/16	10.141-144.0.0/16	10.1-9.23.0/24
9	上海市	10.31.0.0/16	10.113-116.0.0/16	10.1-9.31.0/24
10	江苏省	10.32.0.0/16	10.145-148.0.0/16	10.1-9.32.0/24
11	浙江省	10.33.0.0/16	10.149-152.0.0/16	10.1-9.33.0/24
12	安徽省	10.34.0.0/16	10.153-156.0.0/16	10.1-9.34.0/24
13	福建省	10.35.0.0/16	10.157-160.0.0/16	10.1-9.35.0/24
14	江西省	10.36.0.0/16	10.161-164.0.0/16	10.1-9.36.0/24
15	山东省	10.37.0.0/16	10.165-168.0.0/16	10.1-9.37.0/24
16	河南省	10.41.0.0/16	10.169-172.0.0/16	10.1-9.41.0/24
17	湖北省	10.42.0.0/16	10.173-176.0.0/16	10.1-9.42.0/24
18	湖南省	10.43.0.0/16	10.177-180.0.0/16	10.1-9.43.0/24
19	广东省	10.44.0.0/16	10.181-184.0.0/16	10.1-9.44.0/24
20	广西壮族自治区	10.45.0.0/16	10.185-188.0.0/16	10.1-9.45.0/24
21	海南省	10.46.0.0/16	10.189-192.0.0/16	10.1-9.46.0/24
22	重庆市	10.50.0.0/16	10.117-120.0.0/16	10.1-9.50.0/24
23	四川省	10.51.0.0/16	10.193-196.0.0/16	10.1-9.51.0/24
24	贵州省	10.52.0.0/16	10.197-200.0.0/16	10.1-9.52.0/24
25	云南省	10.53.0.0/16	10.201-204.0.0/16	10.1-9.53.0/24
26	西藏自治区	10.54.0.0/16	10.205-208.0.0/16	10.1-9.54.0/24
27	陕西省	10.61.0.0/16	10.209-212.0.0/16	10.1-9.61.0/24
28	甘肃省	10.62.0.0/16	10.213-216.0.0/16	10.1-9.62.0/24
29	青海省	10.63.0.0/16	10.217-220.0.0/16	10.1-9.63.0/24
30	宁夏回族自治区	10.64.0.0/16	10.221-224.0.0/16	10.1-9.64.0/24
31	新疆维吾尔自治区	10.65.0.0/16	10.225-228.0.0/16	10.1-9.65.0/24
32	新疆生产建设兵团	10.66.0.0/16	10.229-232.0.0/16	10.1-9.66.0/24

续表

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
计划单列市环境保护局				
1	大连市环境保护局	10.24.0.0/16		10.1-9.24.0/24
2	宁波市环境保护局	10.38.0.0/16		10.1-9.38.0/24
3	厦门市环境保护局	10.39.0.0/16		10.1-9.39.0/24
4	青岛市环境保护局	10.40.0.0/16		10.1-9.40.0/24
5	深圳市环境保护局	10.47.0.0/16		10.1-9.47.0/24

环境保护部直属单位和派出机构网络 IP 地址规划见表 B.2。

表 B.2　环境保护部直属单位、派出机构网络 IP 地址规划表

序号	单位名称	局域网络 IP 地址	网络设备 IP 地址
环境保护部直属单位、派出机构			
1	环境保护部应急与事故调查中心	10.87.0.0/16	10.1-9.87.0/24
2	中国环境科学研究院	10.71.0.0/16	10.1-9.71.0/24
3	中国环境监测总站	10.72.0.0/16	10.1-9.72.0/24
4	中日友好环境保护中心	10.73.0.0/16	10.1-9.73.0/24
5	中国环境报社	10.74.0.0/16	10.1-9.74.0/24
6	中国环境科学出版社	10.75.0.0/16	10.1-9.75.0/24
7	环境保护部核安全中心	10.76.0.0/16	10.1-9.76.0/24
8	环境保护部环境保护对外合作中心	10.77.0.0/16	10.1-9.77.0/24
9	环境保护部南京环境科学研究所	10.93.0.0/16	10.1-9.93.0/24
10	环境保护部华南环境科学研究所	10.94.0.0/16	10.1-9.94.0/24
11	环境保护部环境规划院	10.78.0.0/16	10.1-9.78.0/24
12	环境保护部环境工程评估中心	10.79.0.0/16	10.1-9.79.0/24
13	环境保护部华北环境保护督查中心	10.80.0.0/16	10.1-9.80.0/24
14	环境保护部华东环境保护督查中心	10.95.0.0/16	10.1-9.95.0/24
15	环境保护部华南环境保护督查中心	10.96.0.0/16	10.1-9.96.0/24
16	环境保护部东北环境保护督查中心	10.97.0.0/16	10.1-9.97.0/24
17	环境保护部西北环境保护督查中心	10.98.0.0/16	10.1-9.98.0/24
18	环境保护部西南环境保护督查中心	10.99.0.0/16	10.1-9.99.0/24
19	环境保护部北方核安全监督站	10.81.0.0/16	10.1-9.81.0/24
20	环境保护部上海核安全监督站	10.233.0.0/16	10.1-9.233.0/24
21	环境保护部广东核安全监督站	10.234.0.0/16	10.1-9.234.0/24
22	环境保护部四川核安全监督站	10.235.0.0/16	10.1-9.235.0/24
23	环境保护部东北核与辐射安全监督站	10.236.0.0/16	10.1-9.236.0/24
24	环境保护部西北核与辐射安全监督站	10.237.0.0/16	10.1-9.237.0/24
25	中国环境科学学会	10.82.0.0/16	10.1-9.82.0/24
26	中国环境保护产业协会	10.83.0.0/16	10.1-9.83.0/24
27	中华环境保护基金会	10.84.0.0/16	10.1-9.84.0/24
28	中国环境文化促进会	10.85.0.0/16	10.1-9.85.0/24
29	中国环境新闻工作者协会	10.86.0.0/16	10.1-9.86.0/24
30	中华环保联合会	10.88.0.0/16	10.1-9.88.0/24
31	环境保护部北京会议与培训基地	10.89.0.0/16	10.1-9.89.0/24
32	环境保护部北戴河技术交流中心	10.238.0.0/16	10.1-9.238.0/24
33	环境保护部兴城环境管理研究中心	10.239.0.0/16	10.1-9.239.0/24

10.1-9.0.0/16 段地址为各单位与环境保护部网络互连的网络设备地址，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。

省级环境保护厅（局）地址规划设计以表 B.1 中浙江省为例进行说明。

11	浙江省	10.33.0.0/16	10.149-152.0.0/16	10.1-9.33.0/24

以下地址主要为办公网络的地址规划，对于设备互联地址和 IP 地址严格按照以上原则规划，即分别采用 30 位、32 位地址。

表 B.3　浙江省网络 IP 地址规划表

地市	区县	业务 IP 地址	局域网及预留地址
省环境保护局	省中心	10.33.0.0/18	10.149.0.0/16
杭州（10.33.64.0/19）	市局	10.33.64.0/22	10.149.150.0/19（市局）
	余杭	10.33.68.0/23	10.149.152.0/24
	富阳	10.33.70.0/23	10.149.154.0/24
	临安	10.33.72.0/23	10.149.156.0/24
	萧山	10.33.74.0/23	10.149.158.0/24
	淳安	10.33.76.0/23	10.149.160.0/24
	桐庐	10.33.80.0/23	10.149.162.0/24
	建德	10.33.82.0/23	10.149.164.0/24
湖州（10.33.96.0/20）	市局	10.33.96.0/23	10.149.166.0/19
	德清	10.33.98.0/24	10.149.167.0/24
	长兴	10.33.99.0/24	10.149.168.0/24
	安吉	10.33.100.0/24	10.149.169.0/24
嘉兴（10.33.112.0/20）	市局	10.33.112.0/23	10.149.170.0/17
	平湖	10.33.114.0/24	10.149.172.0/24
	海宁	10.33.115.0/24	10.149.174.0/24
	桐乡	10.33.116.0/24	10.149.175.0/24
	海盐	10.33.117.0/24	10.149.176.0/24
	嘉善	10.33.118.0/24	10.149.177.0/24
绍兴（10.33.128.0/20）	市局	10.33.128.0/23	10.149.178.0/17
	绍兴局	10.33.130.0/24	10.149.180.0/24
	诸暨	10.33.131.0/24	10.149.181.0/24
	上虞	10.33.132.0/24	10.149.182.0/24
	嵊州	10.33.133.0/24	10.149.183.0/24
	新昌	10.33.134.0/24	10.149.184.0/24
台州（10.33.144.0/20）	市局	10.33.144.0/23	10.149.186.0/17
	临海	10.33.146.0/24	10.149.188.0/24
	温岭	10.33.147.0/24	10.149.189.0/24
	玉环	10.33.148.0/24	10.149.190.0/24
	天台	10.33.149.0/24	10.149.191.0/24
	仙居	10.33.150.0/24	10.149.192.0/24
	三门	10.33.151.0/24	10.149.193.0/24
	路桥	10.33.152.0/24	10.149.194.0/24
	黄岩	10.33.153.0/24	10.149.195.0/24
	椒江	10.33.154.0/24	10.149.196.0/24

续表

地市	区县	业务 IP 地址	局域网及预留地址
温州（10.33.160.0/20）	市局	10.33.160.0/23	10.149.198.0/17
	乐清	10.33.162.0/24	10.149.200.0/24
	仓南	10.33.164.0/24	10.149.202.0/24
	永嘉	10.33.165.0/24	10.149.203.0/24
	瑞安	10.33.166.0/24	10.149.204.0/24
	平阳	10.33.167.0/24	10.149.205.0/24
	文成	10.33.168.0/24	10.149.206.0/24
	洞头	10.33.169.0/24	10.149.207.0/24
	泰顺	10.33.170.0/24	10.149.208.0/24
丽水（10.33.176.0/20）	市局	10.33.176.0/23	10.149.209.0/17
	青田	10.33.178.0/24	10.149.210.0/24
	松阳	10.33.179.0/24	10.149.211.0/24
	景宁	10.33.180.0/24	10.149.212.0/24
	庆元	10.33.181.0/24	10.149.213.0/24
	缙云	10.33.182.0/24	10.149.214.0/24
	龙泉	10.33.183.0/24	10.149.215.0/24
	遂昌	10.33.184.0/24	10.149.216.0/24
	云和	10.33.185.0/24	10.149.217.0/24
金华（10.33.192.0/20）	市局	10.33.192.0/23	10.149.216.0/17
	武义	10.33.194.0/24	10.149.218.0/24
	磐安	10.33.195.0/24	10.149.219.0/24
	兰溪	10.33.196.0/24	10.149.220.0/24
	东阳	10.33.197.0/24	10.149.221.0/24
	义乌	10.33.198.0/24	10.149.222.0/24
	永康	10.33.199.0/24	10.149.223.0/24
舟山（10.33.208.0/20）	市局	10.33.208.0/23	10.149.225.0/17
	岱山	10.33.209.0/23	10.149.226.0/24
	嵊泗	10.33.210.0/23	10.149.227.0/24
衢州（10.33.224.0/20）	市局	10.33.224.0/23	10.149.228.0/17
	龙游	10.33.226.0/23	10.149.230.0/24
	江山	10.33.227.0/24	10.149.231.0/24
	常山	10.33.228.0/24	10.149.232.0/24
	开化	10.33.229.0/24	10.149.233.0/24

以上地址主要为办公网络的地址规划，对于设备互联地址和 IP 地址严格按照以上原则规划，即分别采用 30 位、32 位地址。

附 录 C
（资料性附录）
路由器性能指标

种 类 性能名称	高端路由器	中端路由器	低端路由器
包转发率	≥80 Mpps（兆脉冲数/秒）	≥10 Mpps（兆脉冲数/秒）	≥300 kpps（兆脉冲数/秒）
交换容量	≥128 Gbit/s	≥64 Gbit/s	
路由表容量	≥60 万条	≥60 万条	≥10 万条
可靠性和可用性要求	系统必须达到或超过 99.999%的可用性 各组件均支持热插拔功能	支持接口模块的热插拔	
安全性	支持用户分级管理和口令保护 支持标准和扩展 ACL，可以对报文进行过滤，防止网络攻击	支持标准和扩展 ACL	支持标准 ACL

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，还需增加如下的功能要求：

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
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

续表

功能分类	功能项目要求
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
双机热备	支持物理设备状态检测
	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
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
	支持日志的集中管理
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
	支持远程管理安全
	支持防火墙状态和网络数据流状态监控

D.3 三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，还需增加如下的功能要求：

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

种 类 性能名称	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 1 ms	最大延迟不应超过 500 μs	最大延迟不应超过 90 μs
	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 1 000 个	最大并发连接数应不小于 10 000 个	最大并发连接数应不小于 100 000 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 1 500 个	最大连接速率应不小于每秒 5 000 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

主机房、基板工作间内的温、湿度必须满足计算机设备要求；计算机机房内温、湿度应满足下列要求：

a）开机时计算机机房内的温、湿度符合表 F.1 的规定；

b）关机时计算机机房内的温、湿度符合表 F.2 的规定。

表 F.1 开机时计算机机房内的温、湿度

级 别 / 项 目	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 F.2 关机时计算机机房内的温、湿度

级 别 / 项 目	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。

附 录 G
（资料性附录）
机房面积公式

计算机机房最小使用面积不得小于 50 m^2，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：

$$A=k\sum S \qquad (1)$$

式中：A——计算机主机房使用面积，m^2；

k——系数，取值为 5～7；

S——计算机系统及辅助设备的投影面积，m^2；

$\sum S$——机房内所有设备占地面积的总和，m^2。

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：

$$A=KN \qquad (2)$$

式中：A——计算机主机房内使用面积，m^2；

K——单台设备占用面积，可取 4.5～5.5，m^2/台；

N——计算机主机房内所有设备的总台数，台。

附 录 H
（资料性附录）
局域网系统性能测试工具要求

H.1 用于局域网系统性能测试的测试工具，宜具备以下基本功能：

a）应具备直接网络流量监听功能，能够对网络利用率、单播帧、广播帧、多播帧、碰撞、各种类型的出错帧进行统计；

b）应能统计网络中产生业务量最多的节点、出错最多的节点、产生广播帧和多播帧最多的节点；

c）应具备网络协议分析功能，能对网络中的协议进行解码和流量分布统计；

d）应具备自动网络节点和拓扑发现功能，能自动生成网络节点列表，包括节点的 MAC 地址、IP/IPX 地址和名称的对应；

e）应具备网络流量仿真功能，可指定数据包的内容（如 MAC 地址、IP 地址）和数据包长度，并可指定所产生流量的大小；

f）应具备 RFC2544 网络性能测试功能，包括吞吐率、传输时延和丢包率测试；

g）应具备 PING 和 TraceRoute 测试功能；

h）应具备从网络设备上获取 SNMP 数据的功能；

i）应具备测试结果分析及图表打印输出的功能；

j）宜具备基本网络业务仿真测试功能（如：DHCP、DNS、Web、E-mail、文件服务等）。

H.2 用于局域网系统性能测试的工具，应具备以下性能和精度要求：

a）应支持在 10/100/1 000 M 以太网接口上的 100%满线速流量产生功能（包括所有的帧大小，如：64、128、256、512、1 024、1 280、1 518 字节）；

b）应支持在 10/100/1 000 M 以太网接口（包括全双工链路）上的 100%满线速流量统计功能；

c）时间标签精度应优于 10 μs。

HJ 460—2009

中华人民共和国国家环境保护标准

环境信息网络建设规范

HJ 460—2009

*

中国环境科学出版社出版发行

（100062　北京崇文区广渠门内大街 16 号）

网址：http：//www.cesp.cn

电话：010-67112738

北京市联华印刷厂印刷

*

2009 年 6 月第　1　版　　开本　880×1230　1/16

2009 年 6 月第 1 次印刷　　印张　2.5

字数　80 千字

统一书号：1380209・248

定价：30.00 元