HJ

中华人民共和国国家环境保护标准

HJ 461－2009

环境信息网络管理维护规范

Specification for environmental information network management and maintenance

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

为规范各级环境保护部门网络管理工作，提高网络管理维护水平，保障各级环境信息网络运行平稳、有效，制定本标准。

本标准附录 A 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、北京思路创新科技有限公司。

本标准环境保护部 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。

环境信息网络管理维护规范

1 适用范围

本标准规定了环境信息网络管理维护的内容，对网络管理、设备维护管理、机房维护管理、安全维护管理等方面作出了具体要求。

本标准适用于各级环境保护部门管理所属的环境信息网络基础设施所进行的维护工作。

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 9361 计算站场地安全要求

GB/T 20269 信息安全技术 信息系统安全管理要求

GB/T 20270 信息安全技术 网络基础安全技术要求

GB/T 20271 信息安全技术 信息系统通用安全技术要求

GB/T 20272 信息安全技术 操作系统安全技术要求

GB/T 20273 信息安全技术 数据库管理系统安全技术要求

GB/T 20282 信息安全技术 信息系统安全工程管理要求

GB/T 21028 信息安全技术 服务器安全技术要求

GB/T 22239 信息安全技术 信息系统安全等级保护基本要求

GB/T 22240 信息安全技术 信息系统安全等级保护实施指南

GB 50052—1995 供配电系统设计规范

GB 50174 电子计算机房设计规范

BMB 5—2000 涉密信息设备使用现场的电磁泄漏发射防护要求.

GA/T 387—2002 计算机信息系统安全等级保护网络技术要求

GA/T 671—2006 信息安全技术 终端计算机系统安全等级技术要求

HJ/T 416—2007 环境信息术语

HJ 460—2009 环境信息网络建设规范

YD/T 1289.2—2003 同步数字体系（SDH）传送网网络管理技术要求 第二部分：网元管理系统（EMS）功能

YD/T 1289.3—2003 同步数字体系（SDH）传送网网络管理技术要求 第三部分：网络管理系统（NMS）功能

ITU-T Q.811 Q 与 X 接口的底层协议框架（Lower layer protocol profiles for the Q and X interfaces）

ITU-T Q.812 Q 与 X 接口的高层协议框架（Upper layer protocol profiles for the Q and X interfaces）

3 术语、定义、符号和缩略语

3.1 术语和定义

HJ/T 416—2007、HJ 460—2009 中确立的术语和定义适用于本标准。

3.2 符号和缩略语

ACL 访问控制列表 Access Control List

CPU 中央处理单元 Central Processing Unit

IDS　入侵检测系统　Intrusion Detection System

IP　互联网协议　Internet Protocol

ITU-T　国际电信联盟远程通信标准化组　International Telecommunication Union Telecommunication Standardization Sector

MAC　介质访问控制　Media Access Control

MSTP　多业务传送平台　Multi-Service Transport Platform

NAT　网络地址转换　Network Address Translation

SDH　同步数字体系　Synchronous Digital Hierarchy

SNMP　简单网络管理协议　Simple Network Management Protocol

TCP　传输控制协议　Transmission Control Protocol

UPS　不间断电源　Uninterruptible Power Supply

VLAN　虚拟局域网　Virtual Local Area Network

VPN　虚拟专用网　Virtual Private Network

4　总体要求

4.1　网络管理维护范围

网络管理维护范围包括对各级环境保护部门所属的网络、设备、软件系统、机房的运行维护以及安全维护管理。网络管理维护对象包括网络设备、服务器设备、终端计算机、机房空调系统、UPS 设备、消防设备、软件系统等。

4.2　运行维护制度

各级环境保护部门应制定并落实网络管理维护制度。

4.3　对维护人员的要求

各级环境保护信息管理部门应配有网络管理维护人员。

4.4　维护周期

维护周期应保证每 24 小时对各设备循环检查一次，节假日例行检查。范例参见附录 A.1。

4.5　软件系统维护

各级环境保护部门应建立软件系统资产清单，记录软件系统维护、备份和升级情况。范例参见附录 A.2。

4.6　备份管理

应明确规定数据及系统备份的频率、备份内容、备份方式，并记录备份工作情况。范例参见附录 A.3。

4.7　线路端口维护

应对线路、端口使用标签标识，规范标签命名，并建立线路端口维护记录。范例参见附录 A.4。

4.8　设备维护

应对各级环境保护部门所属的硬件设备编号，建立设备维护记录。范例参见附录 A.5。

4.9　终端计算机维护

终端计算机维护应由网络管理维护人员填写维护记录。记录内容应包括事件说明、维护方式、时间等。范例参见附录 A.6。

4.10　设备故障处理流程

a）根据故障现象，确定故障范围；

b）查看故障所引起的相关问题；

c）通知相关负责人；

d）查找故障原因；

e）解决故障问题；

f）整理备份资料，以便恢复数据；

g）记录故障日志，并建立故障档案。

4.11 紧急事故处理程序

紧急事故包括：

a）各种通信事故、严重设备故障、严重电路障碍、网络异常等情况；

b）出现危及通信设备、人身安全的问题或出现事故征兆等异常情况；

c）各项工作中发现的严重失、泄密问题；

d）应及时处理的各类紧急通知；

e）上级管理部门要求的其他紧急报告。

应建立紧急事故处理程序，包括事故判别及事故级别、应急预案及处理方法、通信联络制度、监督检查制度以及技术储备与保障等。

4.12 安全管理

各级环境保护部门信息系统在被确定安全等级后，负责部门应依据国家对不同安全等级的信息系统应达到的安全保护能力要求进行安全保护实施和运行维护工作。

4.13 维护文档管理

宜建立维护文档管理数据库系统，记录维护工作、统计维护内容、维护事件、解决方式等，为配置变更、事件处理提供完整的维护记录。

4.14 维护情况综合汇报和分析

应定期编写维护情况综合汇报，并对维护中出现的问题进行分析并提出改进方案，定期评估配置、策略是否优化。

5 网络管理

5.1 网络管理要求

各级环境保护部门应建立网络管理系统，对环境信息网络所用的设备、链路等进行集中监视。国家级环境信息广域网、省级环境信息广域网及环保系统城域网的网络管理系统应满足 HJ 460—2009 中对网络管理平台的要求，其中采用 SDH 技术的网络应满足 YD/T 1289.2—2003 及 YD/T 1289.3—2003 对网络管理功能的要求。网络管理系统应包括以下功能：

a）配置管理：对设备配置和端口配置进行管理；

b）性能管理：对设备的各种性能数据进行采集、存储和分析，并给出分析结果；

c）网络拓扑管理：包括拓扑视图、网络浏览、网络监视和拓扑编辑等功能；

d）故障管理：包括告警的监视与显示、告警过滤、告警信息定位、告警信息存储、告警信息查询统计等功能；

e）业务管理：业务配置信息上报和查询、业务保护倒换状态查询等功能；

f）安全管理：包括用户管理、权限控制和登录日志管理等；

g）报表管理：根据用户需要生成报表，用于分析和保存；

h）备份管理：应提供网络管理数据的备份功能，包括自动和手工备份，需要时可将备份数据恢复；

i）用户管理：应限制未授权操作人员，支持分权分域管理。

5.2 网络管理接口

a）MSTP 设备之间及 MSTP 设备与网络管理系统之间的通信接口采用 ITU-T Q.811 和 Q.812 规定的无连接模式协议栈或 TCP/IP 协议栈；

b）网络设备应提供基于 SNMP 协议的网络管理接口；

c）网络管理系统之间应具备接口，能够根据要求进行网络管理信息的交换，包括配置、故障和性

能数据。该接口可选择开放的国际协议标准，如 Web Service 等标准接口。

5.3 网络管理其他要求

a）网络管理信息与环境信息网络设备、运行的实际数据应保持一致；

b）网络设备运行正常情况下，告警平均响应时间（指从发生告警到显示告警）不大于 20 秒。在系统满负荷情况下，告警响应时间应不大于以上指标的 150%；

c）各种日志文件应至少保存 12 个月的事件；

d）原始告警信息保存时间不小于 1 个月，原始性能信息保存时间不小于 3 个月，处理后的告警数据、性能数据保存时间不小于 3 个月，各类统计分析结果数据保存时间不小于 6 个月。

6 设备及软件系统维护管理

6.1 服务器及软件系统维护管理

6.1.1 服务器监控

宜采用服务器监控管理系统集中监控管理服务器系统。

6.1.2 服务器维护要求

a）服务器应放置在专业机房内，并安装固定在标准机柜中。

b）检查服务器资源利用率是否满足要求，包括 CPU、内存、磁盘空间等。

c）应定期检查服务器硬件状态，查看面板指示灯有无异常和告警，如出现告警，应分析原因，并及时处理解决。

6.1.3 软件系统维护要求

a）检查服务器上运行的操作系统、信息系统、数据库管理系统等软件系统工作是否正常。

b）应按合理的备份策略对软件系统进行数据备份和系统备份。

c）应根据系统情况，及时更新相关业务应用软件和系统软件补丁。

d）查看系统运行日志，是否有异常情况，及时进行分析解决，并备份日志等系统服务记录。

e）检查防病毒软件是否告警，病毒库是否更新。

f）检查所需系统服务是否正常，服务器有无可疑进程，并进行记录分析。

6.2 路由器维护管理

6.2.1 路由器基本配置

a）配置标识网络中路由器的设备名称；

b）配置路由器设备的日志记录信息；

c）配置路由器设备的 enable 口令，应为进入路由器特权模式配置密码；

d）关闭路由器上不使用的端口，将需要应用的端口结合实际应用配置 IP 地址；

e）通过路由器设备的访问控制列表（ACL）的配置和管理，实现对主机和网络的访问限制。

6.2.2 路由器系统文件和配置文件管理

a）路由器的系统文件和配置文件应备份，并进行版本管理和维护；

b）运行维护人员应熟悉路由器系统文件、配置文件的恢复和更新操作。

6.2.3 路由器维护要求

6.2.3.1 路由器设备维护要求

维护应检查以下内容：

a）资源利用率；

b）网络接口带宽利用率；

c）丢包率；

d）接口转发时延；

e）包转发率；

f）系统软件运行情况；

g）路由器的配置文件情况；

h）电源和风扇工作情况；

i）查看并记录安装或升级的新硬件和新软件；

j）监视路由器及相连接网络的性能和状态；

k）收集流量统计的信息。

6.2.3.2 路由器设备故障维护

a）定期查看路由器运行软件的故障日志记录等，及时发现网络中存在的安全问题，并及时更新升级路由器系统软件。

b）当发现网络性能大幅下降时，应检查路由器情况，诊断问题原因；如路由器不能满足正常业务流量要求，可考虑升级路由器设备。

c）当路由器出现故障告警，可根据具体故障信息判断路由器硬件的故障。当路由器故障定位后，应按相关技术处理要求解决故障，详细记录故障日志，并建立故障档案。

d）可利用网络管理工具管理路由器设备，发现及诊断网络中的问题。

e）发生暂时或永久的网络拓扑改变时，应及时调整路由器配置，尽可能优化网络结构和网络性能。

6.3 交换机维护管理

6.3.1 交换机基本配置

a）配置交换机设备名称。

b）配置交换机设备的日志记录信息。

c）设置交换机设备的 enable 口令，应为进入交换机特权模式配置密码。

d）设置交换机设备的管理接口 IP 地址，关闭交换机上不使用的端口。

6.3.2 交换机系统文件和配置文件管理

a）交换机的系统文件和配置文件应备份，并进行版本管理和维护。

b）运行维护人员应熟悉交换机系统文件、配置文件的恢复和更新操作。

6.3.3 交换机维护要求

交换机维护应检查以下内容：

a）资源利用率。

b）网络接口带宽利用率。

c）交换机及相连网络的状态和性能。

d）交换机系统软件运行状态。

6.3.4 VLAN 系统维护要求

a）应根据实际应用，确定广播域的范围，划分和创建相应的 VLAN。

b）VLAN 划分发生变化时，应及时维护交换机上的 VLAN 设置。

c）应根据具体情况对交换机上 Trunk 链路进行配置和管理。

6.4 防火墙维护管理

6.4.1 防火墙安全策略要求

a）使用最小安全原则，即除非明确允许，否则就禁止。

b）包含基于源 IP 地址、目的 IP 地址的访问控制。

c）包含基于源端口、目的端口的访问控制。

d）包含基于协议类型的访问控制。

e）包含基于 MAC 地址的访问控制。

6.4.2 防火墙维护要求

防火墙维护应检查以下内容：

a）监控吞吐量、连接速率和延迟，进行流量统计分析，根据分析对防火墙策略进行调整优化。
b）NAT 列表。
c）端口开放及连接状态。
d）包过滤设置、应用代理设置、内容过滤设置等配置。
e）并发连接数。

6.5 IDS 维护要求

IDS 维护应检查以下内容：
a）系统运行情况，检测误报率、漏报率。
b）系统策略状态。
c）系统资源状态。
d）运行日志，日志备份及分析。

6.6 VPN 系统维护要求

VPN 系统维护应检查以下内容：
a）VPN 系统状态。
b）VPN 策略。
c）VPN 许可用户名单。
d）VPN 连接数。

6.7 安全审计与监控系统维护要求

安全审计与监控系统维护应检查以下内容：
a）软件工作状态。
b）受控端信息采集状态。
c）备份恢复系统工作状态。
d）数据库运行状态。
e）系统数据信息。

7 机房维护管理

7.1 机房环境要求

a）温、湿度：机房内的温度、湿度应符合 GB 50174 指标要求；
b）防尘：机房应具备防尘能力，保证机房内空气含尘浓度应符合 GB 50174 指标要求；
c）噪声、电磁干扰及静电：机房应有良好的噪声控制、防电磁干扰、防静电等措施，应符合 GB 50174 指标要求；
d）供配电：机房用电负荷等级及供电要求应符合 GB 50052—1995 标准；
e）照明：机房照明应有应急备用设备，各种照明设备应有专人负责，定期检修。照明的照度标准应符合 GB 50174 指标要求；
f）接地：机房接地装置的设置应满足人身的安全及计算机正常运行和系统设备的安全要求，符合 GB 50174 指标要求；
g）给水排水：机房给排水条件应符合 GB 50174 要求；
h）机房环境：机房周围环境要保持清洁和安全可靠，机房门前道路应保持畅通无阻；应保持机房环境卫生，定期打扫，定期清理。

7.2 机房制度要求

a）各级环境保护部门应制定并落实机房管理制度，并不断健全完善机房各项规章制度；
b）机房管理制度至少应包括机房出入、值班及交接班、设备维护、消防等方面内容。

7.3 UPS 系统管理维护

a）UPS 使用环境：保持温度湿度在合适的范围，尽量远离具有强磁性的装置；

b）UPS 电池组维护：定期进行充放电；

c）UPS 充电电压、充电电流：保证在额定范围之内；

d）UPS 放电深度：防止深度放电；

e）UPS 负载：保持适当负载，必要时可对 UPS 进行扩容。

7.4 机房空调系统管理维护

a）检查空调的制冷、供热、新风及电气控制等部分，发现问题及时排除，以满足机房对温度、湿度和空气含尘浓度的要求；

b）检查空调设备的能力是否满足要求，保证空调效果。

7.5 机房消防系统管理维护

a）应定期检查维护消防设施和设备，保证消防系统工作正常；

b）严格执行国家关于消防系统管理标准规范中对消防系统维护的相关要求。消防设施和设备符合 GB 50174、GB/T 9361 等标准规范中的相关规定。

7.6 机房监控要求

宜采用机房监控系统监控机房供配电、UPS、空调、消防等相关设施。

8 安全维护管理

8.1 安全维护管理内容

安全维护管理内容包括安全运行维护机构和安全运行维护机制的建立，环境、资产、设备、介质的管理，网络、系统的管理，密码、密钥的管理，运行、变更的管理，安全状态的监控和安全事件的处置，安全审计和安全检查等。

8.2 安全维护过程

安全维护过程包含运行管理和控制、变更管理和控制、安全状态监控、安全事件处置和应急预案、安全检查和持续改进以及监督检查等。各过程具体目标和过程控制要求见 GB/T 22240。

8.3 安全管理制度

各级环境保护部门应按照 GB/T 20269、GB/T 20282、GB/T 22239、GB/T 22240 等标准规范，制定并落实符合本部门安全保护等级要求的安全管理制度。

8.4 安全维护技术要求

8.4.1 设备及软件系统安全维护技术要求

安全维护管理中涉及的网络、信息系统、操作系统、数据库、服务器、终端计算机等管理维护对象的具体维护技术要求，见 GB/T 20270、GB/T 20271、GB/T 20272、GB/T 20273、GB/T 21028、GA/T 387—2002、GA/T 671—2006 等标准规范。

8.4.2 机房安全维护技术要求

a）场地安全要求：各级环境保护部门机房的供配电系统、空调系统、防静电、防雷、消防、防水等方面应符合 GB/T 9361 要求；

b）电磁防护要求：应对机房内设备实施防电磁辐射泄漏、抗电磁干扰及电源保护等保护措施。承载涉密信息系统的设备的电磁泄漏发射防护应依据 BMB 5—2000 进行防护。

附 录 A
（资料性附录）
网络管理维护表格范例

A.1 日常维护检查表范例

日常维护检查表				
检查对象	检查内容	状态	问题说明	备注
服务器				
网络设备				
安全设备				
电力设备				
空调系统				
消防系统				
其他系统				
日期：		运行维护工程师：		
填表说明： 运行维护人员应按上表检查服务器等设备和系统的运行状态。在“状态”列中填写状态说明，在“问题说明”列中填写出现的问题描述和处理办法。				

A.2 软件系统维护表范例

软件系统维护表			
软件系统	维护内容	情况问题说明	备注
服务器操作系统			
业务应用系统			
数据库系统			
地理信息系统			
数据库系统			
防病毒系统			
其他软件系统			
日期：		运行维护工程师：	
填表说明： 运行维护人员应按上表记录软件系统维护情况。在“维护内容”列中填写维护内容，如备份、升级等。在“情况或问题说明”列中填写维护情况或问题及处理办法。			

A.3 备份记录表范例

备份记录表					
系统名称	备份内容	使用工具	备份频率	备份策略	备份目标

A.4 线路端口登记表范例

线路端口登记表					
原始编码	记录编号	对应端口	所属设备编号	对应使用人员	备注

A.5 设备登记表范例

设备登记表				
设备编号	设备名称	购买日期	保修年限	存放位置

A.6 终端计算机日常服务表范例

终端计算机日常服务表					
报修人员：		联系电话：		部门及房间号：	
登记时间：		维护人员：		备注：	
事件信息：					
处理方式：					
登记人：		维护人员签字：		报修人员签字：	

中华人民共和国国家环境保护标准
环境信息网络管理维护规范
HJ 461—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　1
字数　40 千字
统一书号：1380209・247
定价：12.00 元