

附件四：

ICS

HJ

中华人民共和国国家环境保护标准

HJ/T ××××—××××

环境信息网络管理维护规范

Specification for environmental information network management and
maintenance

(征求意见稿)

20□□-□□-□□发布

20□□-□□-□□实施

环 境 保 护 部 发布

目 次

前 言	I
1 适用范围	1
2 规范性引用文件	1
3 术语和定义	1
4 网络管理制度	2
5 链路维护管理	2
6 设备维护管理	4
7 机房维护管理	7
8 安全维护管理	9
附 录 A（资料性附录） 网络管理维护表格	12
附 录 B（规范性附录） 机房专用空调设备的维护周期表	15

前 言

为配合国家环境信息网络建设和维护工作，规范各级环境保护行政主管部门网络管理工作，提高网络管理维护水平，以保证各级环境信息通过国家环境信息网络实时、有效传输，为环境保护管理和决策服务，制定本标准。

本标准规定了建立环境信息网络管理制度的要求及主要内容，以及链路维护管理、设备维护管理、机房维护管理、安全维护管理的技术要求。

本标准附录 A 为资料性附录，附录 B 为规范性附录。

本标准为首次发布。

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、北京思路创新科技有限公司。

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。

环境信息网络管理维护规范

1 适用范围

本标准规定了建立环境信息网络管理制度的要求及主要内容，以及链路维护管理、设备维护管理、机房维护管理、安全维护管理的技术要求。

本标准适用于各级环境保护部门的信息化基础设施运行维护管理活动。

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 9361-1988	计算站场地安全要求
GB/T 18018-1999	路由器安全技术要求
HJ/T 416-2007	环境信息术语
BMB5-2000	涉密信息设备使用现场的电磁泄漏发射防护要求
YD/T 1109-2001	ATM交换机技术规范
YD/T 1097-2001	YD/T 1097-2001 路由器设备技术规范——高端路由器
YD/T 1096-2001	YD/T 1096-2001 路由器设备技术规范——低端路由器

3 术语和定义

HJ/T 416-2007《环境信息术语》中确立的术语和定义以及下列缩略语适用于本标准。

3.1

虚拟局域网 Virtual Local Access Network (VLAN)

通过桥接的局域网内活跃拓扑中工作站的划分，各VLAN使用VID（VLAN标识符）区分。各个VLAN是原桥接的局域网的一个子集。

3.2

域名服务 Domain Name Server (DNS)

一种分层的分布式数据库，它包含对 DNS 域名到各种数据类型的映射，例如，IP 地址。DNS 可以用来按友好用户名称查找计算机和服务的位置，也可以用来发现存储在数据库中的其他信息。

3.3

Web 服务 Web Service

一种服务构件式集成方法，提供了一系列标准化的功能组件，部署到网络中可作为不同的应用系统间的标准接口，用于所有接受这个标准的应用的请求中。

3.4

网络地址转换 Network Address Translation (NAT)

一种IETF(Internet Engineering Task Force, Internet工程任务组)标准。允许一个整体机构以一个公用IP (Internet Protocol) 地址出现在Internet上。

3.5

非军事区 Demilitary Zone (DMZ)

与军事区和信任区相对应。作用是把WEB服务器、邮件服务器等允许外部访问的服务器单独接在该区端口，使整个需要保护的内部网络接在信任区端口后，不允许任何访问，实现内外网分离，达到用户需求。

4 网络管理制度

4.1 运行维护制度管理

各级环境保护行政主管部门应建立维护管理制度。维护管理制度主要规定：

4.1.1 维护范围

维护范围应包括各级网络设备、服务器设备、客户端计算机设备、线路、机房空调系统、UPS 设备、防火设备等。

4.1.2 维护内容

负责环境信息网络中所有设备的维护。

4.1.3 对维护人员的要求

各级环境保护行政主管部门应有专门网络维护人员。

4.1.4 维护时间

维护时间应保证每 24 小时对各级设备循环检查一次，节假日例行检查。范例参见附录 A.1。

4.1.5 备份体系

备份体系根据备份内容不同分为数据备份及系统备份两种。应对备份时间、备份内容、备份方式进行明确规定。要求对备份内容制作统计表单。范例参见附录 A.2。

4.1.6 线路端口维护

应对各级线路、端口明确标签命名记录，建立维护记录。范例参见附录 A.3。

4.1.7 硬件维护

应对所有硬件设备编号，建立设备维护记录。范例参见附录 A.4。

4.1.8 建立客户端维护工作程序

每次客户端维护应填写维护记录。维护人员及接受服务人员负责填写维护记录。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.5。

4.1.9 建立紧急事故处理程序

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内容。

4.1.10 维护综合汇报

应定期编写维护综合汇报，制作周报、月报、季报、年报等。

4.1.11 建立运行安全管理制度

应建立运行安全管理制度，对保密及数据安全、人员管理等进行规定。

4.1.12 建立各种维护手册

维护手册包括客户端办公环境标准安装手册、维护人员日常维护手册、标准服务器安装手册、设备编号统计规则、防病毒客户端配置手册、常用设备操作手册等。

4.2 维护报告管理

应根据维护制度，在每次维护操作后填写记录表单。累计表单要求制作档案。可以建立数据库系统，统计维护内容、维护工作量、维护事件、解决方式等。

5 链路维护管理

5.1 传输骨干网网络管理

5.1.1 网络监控系统管理功能

网络监控系统应满足YD/T 1238-2002、YD/T1289.2-2003、YD/T 1345-2005的要求，应具备以下管理功能：

- a) 配置管理：对传输电路的指配和网络配置管理。电路指配即指电路的建立、修改、查询和删除；
- b) 性能管理：对传输骨干网设备和电路的各种性能数据进行采集、存储和分析，并给出分析结果；
- c) 故障管理：对电路的运行情况进行监视，对电路出现的故障进行处理，包括告警的监视与显示、告警过滤、告警信息定位、告警信息存储等功能；
- d) 资源管理：对传输骨干网电路等资源数据进行管理；
- e) 安全管理：包括用户管理、权限控制和登录日志管理等。

5.1.2 网络监视系统管理功能

若需要，应提供传输骨干网网络监视系统，对传输骨干网所用的特定设备、电路和系统进行集中监视。网络监视系统应满足YD/T 1238-2002、YD/T1289.2-2003、YD/T 1345-2005的要求，应具备以下管理功能：

- a) 告警实时监视、告警收集与显示、告警查询与统计、告警显示过滤和告警同步；
- b) 性能监视、性能数据上报和性能数据查询；
- c) 拓扑视图、网络浏览、网络监视和拓扑编辑；
- d) 业务配置信息上报和查询、业务保护倒换状态查询；
- e) 安全管理，包括用户管理、权限控制和登录日志管理。

5.1.3 网络管理接口

MSTP设备之间及MSTP设备与网管系统之间的通信接口采用国际电信联盟远程通信标准化组（International Telecommunication Union Telecommunication Standardization Sector, ITU-T）建议Q.811和Q.812规定的无连接模式协议栈或TCP/IP协议栈。

5.1.4 网络管理性能要求

网络管理性能要求如下：

- a) 应提供网管数据的备份功能，包括自动和手工备份，需要时可将备份数据恢复；
- b) 应限制未授权操作人员；
- c) 应保证网管与被管网络数据的一致性；
- d) 网络设备运行正常情况下，告警平均响应时间（指从网元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%；
- e) 各种日志文件应至少能保存 12 个月的事件；
- f) 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；
- g) 时间戳的精度为 1 秒。

5.2 业务网络网络管理

5.2.1 网络管理功能

a) 配置管理

包括对路由器、IP-VPN 等 IP 网络设备和业务的配置管理。至少应包括以下内容：

- 1) 根据用户需求查询、修改路由器设备的系统信息、路由信息及接口信息，并对已配置完毕的信息进行备份；
- 2) 查询、修改 IP-VPN 业务信息，并对已配置完毕的信息进行备份。

b) 性能管理

性能管理至少应包括如下内容：

- 1) 性能监控：包括定时/非定时采集线路和路由器的流量、延迟、丢包率、CPU 利用率、内存余量等性能参数，并生成性能报告；
 - 2) 设置性能监视门限值：当性能参数越过一定的门限值时，发出告警通知；
 - 3) 性能分析：对性能数据进行分析、统计，计算性能指标。
- c) 故障管理
- 故障管理至少应包括如下内容：
- 1) 故障信息采集：采集网元设备的告警信息，包括设备故障告警、链路故障告警、各种门限告警、设备/端口/链路状态变化告警等；
 - 2) 故障监视：对网元和网络路由进行监视，出现故障时进行显示；
 - 3) 故障处理过程管理：记录排错行为，包括故障产生、变化、消除过程；
 - 4) 故障信息的查询与统计。

5.2.2 网络管理接口

a) IP 网元网络管理接口

IP 网元应提供基于 SNMP 协议的网络管理接口，应符合 RFC 1213、RFC 1901、RFC 1910、RFC2574、RFC 2578、RFC 3418 等规范。

b) 业务网络管理间的接口

业务网络网络管理系统之间存在接口，能够根据要求进行网管信息的交互，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 CORBA、Web Services 等标准接口。

6 设备维护管理

6.1 网络服务器系统

网络应用服务器是指在环境信息网络中承担各种应用服务的计算机。例如：数据库服务器，邮件服务器，DNS服务器，防病毒服务器等。

6.1.1 网络应用服务器软件系统维护

6.1.1.1 DNS 服务器系统管理维护

- a) 应检查操作系统是否工作正常；
- b) 应检查磁盘空间是否满足系统要求；
- c) 应根据系统情况，及时更新系统补丁；
- d) 应查看系统运行日志，检查运行状况；
- e) 应检查本机防病毒软件是否报警，病毒库更新；
- f) 应检查 DNS 服务是否启动正常；
- g) 应按照维护制度备份 DNS 记录；
- h) 应根据修改要求记录单，编辑 DNS 记录。

6.1.1.2 网络管理服务器系统管理维护

- a) 应检查操作系统是否工作正常；
- b) 应检查磁盘空间是否满足系统要求；
- c) 应根据系统情况，及时更新系统补丁；
- d) 应查看系统运行日志，检查运行状况；
- e) 应检查本机防病毒软件是否报警，病毒库更新；
- f) 应检查网络管理软件是否应用正常；
- g) 应检查相关协议是否正常。

6.1.1.3 防病毒管理中心服务器系统管理维护

- a) 应检查操作系统是否工作正常；
- b) 应检查磁盘空间是否满足系统要求；

- c) 应根据系统情况，及时更新系统补丁；
- d) 应查看系统运行日志，检查运行状况；
- e) 应定时升级防病毒库。建议设定防病毒软件每天定时更新病毒库；
- f) 应共享防病毒客户端安装程序，方便客户端设备安装防病毒程序，建议客户端设定从防病毒服务器更新病毒库；
- g) 应根据维护制度定期检查防病毒客户端状态，查杀病毒；
- h) 应根据维护制度设定客户端防病毒程序扫描周期。

6.1.2 网络应用服务器硬件系统维护

服务器应放置在专业机房内，并安装固定在标准机柜中。

服务器应定期检查服务器硬件状态，如硬盘状态、电源状态等。如出现报警，应按照运行维护制度管理要求进行处理。

6.1.3 服务器故障处理流程

- a) 确定故障范围；
- b) 查看故障所引起的相关问题，如服务中断，数据丢失等；
- 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，方便恢复数据。

6.2 路由器系统

6.2.1 路由器设备运行维护

6.2.1.1 路由器设备运行维护：性能

- a) 应查看资源利用率；
- b) 应查看网络接口带宽利用率；
- c) 应查看丢包率；
- d) 应查看软件运行情况；
- e) 应查看路由器的配置情况；
- f) 应查看交换机配置；
- g) 应查看安装或升级新硬件；
- h) 应查看安装或升级新软件；
- i) 应查看监视路由器及相连接网络的性能和状态；
- j) 应查看流量统计的收集。

6.2.1.2 路由器设备运行维护：告警

- a) 当发现网络性能大幅下降时，应检查路由器的处理器和内存使用情况，并检查网络接口、相连的网络或通信链路的流量和硬件，由此诊断是由于正常业务流量较大，还是网络攻击对网络造成的影响；如路由器不能满足正常业务流量，可考虑升级路由器设备；
- b) 当路由器故障定位后，应详细记录故障日志，并建立故障档案；
- 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；
- d) 在宕机后，无法登录路由器时，可通过控制端口重新启动或重新引导路由器，如无法登录，可采用断电的方式关闭路由器，宜间隔几分钟后，再加电重新启动；
- e) 配置（重新配置）路由器时，应先保存原来的配置文件，然后再开始配置（重新配置）路由器；
- f) 可通过网络工具管理路由器设备，发现及诊断网络中问题，包括拥塞、路由环回、差错 IP 地址、黑洞、包雪崩、主机的错误行为等；
- g) 暂时的或永久的网络拓扑改变，应及时调整路由器配置，尽可能优化网络结构和网络性能；

- h) 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运行软件。

6.2.2 路由器的基本配置

- a) 应配置路由器设备名称，标识网络中路由器的设备名称；
- b) 应配置路由器设备的日志消息，主要用于非授权访问的警告或对设备的说明；
- c) 应配置路由器设备的 **enable** 口令，必须给进入路由器特权模式配置密码；
- d) 应配置路由器设备的接口 **IP** 地址，关闭路由器上不用的端口，将需要应用的端口结合实际应用配置 **IP** 地址；
- e) 应通过路由器设备的访问控制列表 (**ACL**) 的配置和管理，来实现对主机对网络的访问限制；
- f) 应配置路由器设备串行接口的时钟，在对路由器 **DCE** 线缆进行配置时，需要设置时钟，时钟是接收口收发数据的速率。

6.2.3 路由器的配置文件管理

- a) 可使用命令行方式管理路由器的配置文件；
- b) 可使用 **TFTP** 服务器管理路由器的配置文件；
- c) 可使用 **FTP** 服务器管理路由器的配置文件。

6.2.4 路由器的系统文件管理

- a) 路由器的系统文件应备份；
- b) 应熟悉路由器系统文件恢复、更新。

路由器的具体要求见 **YD/T 1097-2001** 和 **YD/T 1096-2001**。

6.3 交换机系统

6.3.1 交换机的基本配置

- a) 应配置交换机设备名称，标识网络中交换机的设备名称；
- b) 应配置交换机设备的日志消息，主要用于非授权访问的警告或对设备的说明；
- c) 应配置交换机设备的 **enable** 口令，必须给进入交换机特权模式配置密码；
- d) 应配置交换机设备的管理接口 **IP** 地址，关闭交换机上不用的端口；
- e) 应配置交换机设备串行接口的时钟，在对交换机 **DCE** 线缆进行配置时，需要设置时钟，时钟是接收口收发数据的速率。

6.3.2 交换机的配置文件管理

- a) 可使用命令行方式管理交换机的配置文件；
- b) 可使用 **TFTP** 服务器管理交换机的配置文件；
- c) 可使用 **FTP** 服务器管理交换机的配置文件。

6.3.3 交换机的系统文件管理

- a) 交换机的系统文件应备份；
- b) 应熟悉交换机系统文件恢复、更新。

6.3.4 交换机的性能监控

- a) 应监控交换机的资源利用率，例如：**CPU**、**Memory** 占用率等；
- b) 应监控交换机网络接口带宽利用率；
- c) 应监控交换机及相连网络的状态和性能；
- d) 应监控交换机系统软件运行状态。

6.3.5 VLAN 系统维护

- a) 应根据实际应用，确定广播域的范围，划分相应的 **VLAN**；
- b) 应在交换机上创建 **VTP** 域，设置 **VTP** 服务器、客户机、透明模式；
- c) 应对交换机上 **Trunk** 链路的配置和管理；
- d) 应对交换机上 **VLAN** 的创建和管理；

- e) 可配置交换机上接口所属 VLAN。

7 机房维护管理

7.1 机房运行管理

7.1.1 机房环境要求

- a) 机房应防尘，门窗要严密，做到地面清洁、设备无尘、排列正规、布线整齐、仪表正常、工具就位、资料齐全、设备有序、使用方便；
- b) 机房内的温度、湿度应符合维护技术指标要求，保持正常通风；
- c) 机房应建立防尘缓冲区，备有工作服和工作鞋；
- d) 机房应有良好的防静电措施；
- e) 机房照明须有应急备用，各种照明设备应有专人负责，定期检修；
- f) 动力机房应设置警示牌和防护栅栏以指示高压区、检修区、禁止合闸区；
- g) 无人值守机房要全封闭，保持机房整洁无尘，应有良好的防火、防盗、防潮、防尘等措施以及相应的远端监测系统；
- h) 无人值守机房的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；
- i) 环境保护部、省环境保护局直属机房的环境卫生由各级信息中心负责落实，定期打扫，定期清理。

7.1.2 机房制度要求

- a) 各中心机房必须统一规范上墙制度，并醒目挂置；
- b) 交流配电机房应上墙悬挂配电图；
- c) 严格执行值班、交接班制度，明确职责，严格纪律，保证制度的进行；
- d) 严格执行安全生产的各项规定，严禁违章操作，确保网络、设备及人身安全；
- e) 严格执行消防安全制度和监督条例，增强机房人员的安全意识，消防设施经常检查，消除隐患；
- f) 严格执行保密法规，对机房人员进行保密教育，增强保密观念，定期进行保密检查，防止泄密失密；
- g) 不断健全完善机房各项规章制度，并组织贯彻实施；
- h) 厂家或集成商或设备厂商在环境保护部、省、市环境保护局机房进行设备安装调测，事先应向环境保护部、省、市环境保护局相关部门提出申请，经批准后方可进行，并做好机房入门登记，环境保护部、省、市环境保护局信息中心应安排专人配合厂家现场工作；
- i) 外单位人员工作性进入环境保护部、省、市环境保护局机房须经环境保护部、省、市环境保护局信息中心同意，安排专人陪同，做好机房入门登记，并佩戴外来人员入室胸牌；
- j) 环境保护部、省、市环境保护局机房进行重大参观活动，须经所在环境保护部、省、市环境保护局领导批准。
- k) 机房安全系统管理维护
 - a) 切实遵守安全制度，认真执行安全操作规定，做好防火、防爆、防盗、防雷、防冻、防潮等工作，确保人身和设备的安全；
 - b) 在维护、测试、磁带更换、装载、故障处理、日常操作以及工程施工等工作中，应采取预防措施，防止造成工伤和通信事故。凡进行危险性较大、操作复杂的工作时，必须事先拟定技术安全措施；
 - c) 各类机房应有可靠避雷装置，配备合适消防器材，安装烟雾告警、高温告警、防盗告警等设备，并制定紧急处理预案；
 - d) 各机房应具备在紧急情况下能与上级部门及时取得联系的手段；机房内有紧急故障处理流程图，人工再启动和再装入流程图，联系人、联系电话等，且相关资料齐全，每个机房维护人

员都能理解、执行；

- e) 雷雨季节要加强对机房内保安设备、地线及防护电路检查；
- f) 加强网络安全管理，确保网络信息不受侵犯，保密信息不被泄露，网络信息不丢失，网络信息正常传递；
- g) 生产核心网络以及与外部因特网存在接口的网络，应特别加强网络安全管理，提高防范措施；
- h) 各种涉及密级的图纸、资料、文件等应严格管理，认真履行使用登记手续；
- i) 加强机房现场钥匙的管理，保证钥匙齐全和完好，由机房值班人员及保安进行分管，并作为交接班的一项内容。

7.2 UPS 系统管理维护

- a) **UPS 开关机顺序：**在使用时应首先给 UPS 供电，使其处于旁路工作状态，然后再逐个打开负载，这样就避免了负载电流对 UPS 的冲击，使 UPS 的使用寿命得以延长。关机顺序可以看做是开机顺序的逆过程，首先逐个关闭负载，再将 UPS 关闭；
- b) **UPS 开机准备：**首先需要确认输入市电连线的极性是否正确，以确保人身安全。注意负载总功率不能大于 UPS 的额定功率。应避免 UPS 工作在过载状态下，以保证 UPS 能够正常工作；
- c) **UPS 使用环境：**UPS 对环境温度的要求通常在 0℃~40℃。UPS 的使用环境要求清洁、少尘、干燥，灰尘和潮湿的环境会引起 UPS 工作不正常。而 UPS 电池组对温度要求则较高，标准使用温度为 25℃，平时最好不要超出 15℃~30℃这个范围。温度过低不但会减小电池组的容量，还会进一步影响 UPS 的使用寿命。另外，UPS 的防磁能力也不是很好。所以不应把强磁性物体放在 UPS 上，否则会导致 UPS 工作不正常或损坏机器；
- d) **UPS 电池组维护：**UPS 的电池组会需要定期进行充放电。如果使用的是免维护的吸收式电解液系统电池，在正常使用时不会产生任何气体，但是如果用户使用不当而造成了电池组过量充电就会产生气体，并出现电池组内压增大的情况，严重时会使电池鼓胀、变形、漏液甚至破裂，如果发现这种现象应立即更换电池组；
- e) **注意人身安全：**由于 UPS 的电池组电压很高，对人体存在一定的电击危险，所以在装卸导电连接条和输出线时应具有安全保障，采用的工具应绝缘，特别是输出接点更应该有防止触电的设置；
- f) **UPS 充电电压：**在 UPS 的充电过程中，如果充电电压过高会导致电池组的过量充电，反之则会造成电池组的充电不足。当充电电压不正常的时候，可能会让电池配置数据产生错误。因此在安装电池组时，一定要注意电池规格和数量的正确性，不同规格、不同品牌的电池应尽量避免混用，外接充电器也最好不要采用低价劣质产品；
- g) **UPS 充电电流：**与 UPS 的电压要求类似，在对 UPS 电池组进行充放电时应尽量避免过大的电流通过。虽然有的时候 UPS 的电池组可以接受一定程度的大电流，但在实际操作中还是应该尽量避免，否则会使电池极板变形，导致电池内阻增大，严重时电池容量将会严重下降，导致电池组寿命大幅缩短；
- h) **UPS 放电深度：**UPS 的放电深度对电池使用寿命的影响也是非常大的，电池放电深度越深，其循环使用次数就越少，因此在使用时应避免电池的深度放电。虽然有些品牌的 UPS 拥有放电保护功能，但是如果 UPS 处于轻载放电或空载放电的情况下，也会让电池深度放电，从而影响电池组的使用寿命；
- i) **UPS 负载大小：**UPS 的负载能力选择 50%~80%的负载为最佳。

7.3 机房空调系统管理维护

7.3.1 制冷部分的维护

- a) 用高、低气压表测试制冷管路的高低压压力，发现问题及时排除；
- b) 经常用手触摸压缩机表面温度，有无过冷过热现象，发现有较大温差时，应查明原因；
- c) 定期观察镜内氟利昂的流动情况，判断有无水份，是否缺液；

- d) 检查冷媒管固定位置有无松动或震动情况；
- e) 检查冷媒管道保温层，发现破损应及时修补；
- f) 制冷管道应畅通，发现堵塞及时排除。

7.3.2 加湿器部分的维修

- a) 保持加湿水盘和加湿罐的清洁，定期清除水垢；
- b) 检查给排水管路，保证畅通，无渗漏、无堵塞现象；
- c) 检查电磁阀的动作，加湿负荷电流和控制器的工作情况，发现问题及时排除；
- d) 检查电极、远红外管，保持其完好无损、无污垢。

7.3.3 冷却系统的维护

- a) 冷却循环管路畅通，无跑、冒，各阀门动作可靠；定期清除冷却水池杂物及清除冷凝器水垢；
- b) 冷却水泵运行正常，无锈蚀，水封严密；
- c) 冷却塔风机运行正常，水流畅通，播洒均匀；
- d) 冷却水池自动补水、水位显示及告警装置完好。

7.3.4 电气控制部分的维护

- a) 定期检查报警器声、光报警是否正常，接触器、熔断器有无松动或损坏，发现问题及时排除；
- b) 检查电加热器的螺丝有无松动，热管有无尘埃，如有松动和尘埃应及时紧固和清洁；
- c) 用钳形电流表测试所有电机的负载电流，测量数据与原始记录不符时，应查出原因，进行排除；
- d) 检查继电器和电子元件有无损坏和变质，发现问题及时更换；
- e) 用测量回风温度，偏差超出标准时，应进行调正；
- f) 测量设备的保护接地线，如果引线接触不良，应及时紧固；
- g) 测量设备绝缘，检查导线有无老化现象。

对空调系统每年应进行一次工况测试，以及时掌握系统各主要设备的性能，并对空调系统设备进行一次有针对性的整修和调整，保证系统运行稳定可靠，不带病工作。机房空调维护周期见附录 B。

7.4 机房消防系统管理维护

- a) 机房设防火负责人、防火安全员等职务，所有机房管理人员纳入消防小组；
- b) 机房内消防器材的使用、灭火方案策略，应做到人人熟知、人人会用；
- c) 任何人不能随意更改消防系统工作状态、设备位置、需要变更消防系统工作状态和设备位置的，必须取得主管领导批准，工作人员更应保护消防设备不被破坏；
- d) 不得随便拉临时电线，高负荷用电，严禁在机房内吸烟和使用明火；
- e) 各种电器设备、防火设备要定期检查、维修，发现问题及时处理；
- f) 当人员离开时，防火安全员要认真检查有无火险隐患。

环境信息网络的各类机房的供配电系统、空调系统、防静电、防雷、消防、防水等方面建设符合 GB/T 9361-1988，并应达到 GB/T 9361-1988 的 A 类或 B 类要求。对电子政务网络中的设备应实施设备的防盗、防毁、防电磁辐射泄漏、抗电磁干扰及电源保护等。承载涉密信息系统的设备的电磁泄漏发射防护应依据 BMB5-2000 进行。

8 安全维护管理

网络安全管理的范围包括网络安全和信息安全两部分。

- a) 网络安全是指生产网络的安全。包括对各级操作密码、远程登陆、内部网与外部网的隔离、网络攻击、计算机病毒防范与杀毒等方面的管理；
- b) 信息安全是指防范有害信息入侵、传播方面的管理。

8.1 防火墙系统维护

8.1.1 防火墙安全策略要求

- a) 防火墙的安全策略应使用最小安全原则，即除非明确允许，否则就禁止；
- b) 防火墙的安全策略应包含基于源 IP 地址、目的 IP 地址的访问控制；
- c) 防火墙的安全策略应包含基于源端口、目的端口的访问控制；
- d) 防火墙的安全策略应包含基于协议类型的访问控制；
- e) 防火墙的安全策略可包含基于 MAC 地址的访问控制。

8.1.2 防火墙日常维护

- a) 应监控网络流量，进行流量统计分析；
- b) 应检查 NAT 列表，根据申请单编辑修改 NAT 列表；
- c) 应检查端口开放及连接状态；
- d) 应检查 VPN 连接状态；
- e) 根据维护制度，应定期修改管理员密码，密码应符合国家密码管理相关规定。

8.2 IDS 系统维护

- a) 应检查系统运行情况；
- b) 应检查系统策略状态；
- c) 应检查系统资源状态；
- d) 应检查运行日志。

8.3 VPN 系统维护

- a) 应检查 VPN 服务器状态；
- b) 应检查 VPN 策略；
- c) 应检查 VPN 许可用户名单；
- d) 应监控 VPN 连接数。

8.4 安全审计与监控系统

- a) 应检查软件工作状态；
- b) 应检查受控端信息采集状态；
- c) 应检查备份恢复系统工作状态；
- d) 应检查数据库运行状态；
- e) 应查看系统数据信息。

8.5 其他安全维护

- a) 根据操作系统情况，应及时更新操作系统补丁程序；
- b) 应对所有计算机设备安装防病毒软件，并及时更新病毒库；
- c) 使用人员密码应符合国家密码管理相关规定。
- d) 可启用密码复杂度策略。复杂性要求，使用数字、大小写字母、特殊符号混合的方式生成口令，并且要定期更改口令；
- e) 可启用最短密码长度策略。最短密码长度普通用户建议为 6 位以上，维护账户密码建议为 13 位以上；
- f) 可启用密码过期策略。密码的最长及最短保存期限应符合国家密码规定；
- g) 可清理不会使用的账户，或是更改账户名称，并启用密码；
- h) 可修改系统自建维护账户信息，改变账户名称；
- i) 可定期检查各级设备使用账户列表；
- j) 可对各个设备运行服务进行统计；
- k) 宜严格控制内部文件共享系统，加强使用管理，关闭系统默认共享。对需要共享的驱动器、目录文件进行严格的访问权限设置。

- l) 宜修改系统日志存储记录大小，能保证存储 7 天以上的日志信息；
- m) 对外发布的 WEB 服务器，可对服务器安装软件防火墙，或是把服务器存放在硬件防火墙 DMZ 区域；
- n) 可对所有应用系统软件，根据使用情况及时安装软件补丁程序。

附 录 A
(资料性附录)
网络管理维护表格

A.1 日常检查表范例

日常维护检查表				
填表说明： 系统管理员每天应按下表检查服务器运行状态。在“状态”列中按说明填写状态说明，在“备注”列中填写出现的问题描述和处理办法。				
服务器	检查内容	状态	备注	说明
Server1	1、系统日志			
	2、邮件系统运行			
	3、操作系统更新			
	4、系统备份			
	5、病毒库更新			
Server2	1、系统日志			
	2、办公系统运行			
	3、操作系统更新			
	4、系统备份			
	5、病毒库更新			
	6、数据库备份			
	7、DNS 服务检查			
其他系统	电力设备检查			
	空调系统检查			
	网络设备检查			
日期：		运维工程师：		
		检查工程师：		

A.4 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.5 客户端日常服务表范例

客户端日常服务表					
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：	

附 录 B
(规范性附录)
机房专用空调设备的维护周期表

维护项目	维护内容	周期
空气处理机	检查、清洁风机转动、皮带和轴承 清洁或更换过滤器 检查及修补跑、冒、滴、漏 清除冷凝沉淀物 检查和清洁蒸发器翅片	月 月 月 季 半年
冷却系统	清洁冷却塔 水泵除垢 水路化清	年 年 年
风冷冷凝器	清洁设备表面 检查清洁冷凝器翅片 检查清洁风扇 检查风扇支座 检查风扇调速状况 检查电机轴承	半月 半月 月 季 季 季
压缩机部分	检查吸气压力和有无过冷、过热现象 检查视镜是否缺液 测试高低压保护装置 检查冷媒管固定情况 检查并修补冷媒管保温层	月 季 年 年 年
加湿器部分	清除水垢 检查电磁阀和加湿器的工作情况 检查给、排水路 检查加湿器电极、远红外管 检查加湿负荷电流和加湿控制运行情况	半月 半月 月 季 半年
电气控制部分	校正温度、湿度传感器 检查低湿报警动作情况 测试回风温度、相对湿度 检查电加热器可靠性 检查所有电机的负载电流 检查所有电器触点和电气元件 检查设备保护接地点 检查设备绝缘状况 校正仪表、仪器	季 半年 半年 年 年 年 年 年 年