

MH

中华人民共和国民用航空行业标准

MH / T 401 8. 2—2004

民用航空空中交通管理 管理信息系统技术规范 第2部分：系统与网络安全

Technical standards air air traffic management
of civil aviation management information system—
Part 2: System and network security

2004—12—20发布

2005-04-01实施

中国民用航空总局 发布

目次

前言	
1 范围	1
2规范性引用文件	1
3术语和定义	1
4物理安全	1
4. 1环境安全	1
4. 2设备安全	2
4. 3记录介质安全	2
4. 4安全管理中心的安全	2
5 网络安全	2
5. 1网络安全建设	2
5. 2网络安全基本要求	4
5. 3网络基本安全技术	4
5. 4详细技术要求	5
6操作系统安全	5
6. 1技术要求	5
6. 2使用	6
6. 3检查测试	6
7数据库管理系统安全	6
7. 1基本要求	6
7. 2身份鉴别	6
7. 3标记与访问控制	6
7. 4数据完整性	6
7. 5数据库安全审计	6
7. 6客体重用	6
7. 7数据库可信恢复	6
7. 8隐蔽信道分析	6
7. 9可信路径	7
7. 10推理控制	7
8应用系统安全	7
8. 1输入数据的确认	7
8. 2内部处理控制	7
8. 3信息验证	7
8. 4输出数据的确认	7
8. 5开发和支持过程的安全	7
8. 6计算机病毒的预防	7

前 言

MH / T 4018《民用航空空中交通管理信息系统技术规范》分为三个部分：

——第1部分：系统数据与接口；

——第2部分：系统与网络安全；

——第3部分：系统网络与接入。

本部分为MH / T 4018的第2部分。

本部分由中国民用航空总局空中交通管理局提出并负责解释。

本部分由中国民用航空总局航空安全技术中心归口。

本部分由中国民用航空总局空中交通管理局负责起草，中国民用航空东北地区管理局空中交通管理局参加起草。

本部分主要起草人：吕小平、李朝阳、齐鸣、李作明、赵凡、闫鹏、郑雪松、唐朝达、邱镭。

民用航空空中交通管理管理信息系统技术规范

第2部分：系统与网络安全

1 范围

MH / T 4018的本部分规定了民用航空空中交通管理(以下简称空管)管理信息系统与网络安全的技术规范。

本部分适用于空管管理信息系统的设计与建设。

2 规范性引用文件

下列文件中的条款通过MH / T 4018的本部分的引用而成为本部分的条款。凡是注日期的引用文件，其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本部分，然而，鼓励根据本部分达成协议的各方研究是否可使用这些文件的最新版本。凡是不注明日期的引用文件，其最新版本适用于本部分。

GB / T 2887—2000电子计算机场地通用规范

GB / T 9387. 2—1995信息处理系统 开放系统互连基本参考模型 第2部分：安全体系结构(idt ISO 7498—2:1989)

GB 17859—1999计算机信息系统安全保护等级划分准则

GB 50174 1993 电子计算机机房设计规范

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 388—2002计算机信息系统安全等级保护操作系统技术要求

GA / T 389—2002 计算机信息系统安全等级保护数据库管理系统技术要求

GA / T 390—2002计算机信息系统安全等级保护通用技术要求

ISO 9001:1994质量系统设计研制、生产、装配和维修的质量认证规范

3 术语和定义

GB 17859—1999、GA / T 387~390—2002、GB / T 2887—2000所确立的术语和定义均适用于MH / T 4018的本部分。

4 物理安全

4.1 环境安全

4.1.1 中心机房的安全保护

4.1.1.1 机房场地的选择应符合GB 50174—1993中2.1的要求。

4.1.1.2 机房内部安全防护应符合GB 50174—1993中4.2的要求。

4.1.1.3 机房防火应符合GB 50174—1993中4.3的要求。

4.1.1.4 机房供电、配电应符合GB 50174—1993中6.1的要求。

4.1.1.5 机房空调、降温应符合GB 50174—1993中第3章的要求。

4.1.1.6 机房防水、防潮应符合GB 50174—1993中第7章的要求。

4.1.1.7 机房防静电应符合GB 50174—1993中6.3的要求。

4.1.1.8 机房接地与防雷击应符合GB 50174—1993中6.4的要求。

4.1.1.9 机房电磁干扰防护应符合GB 50174—1993中3.2的要求。

4. 1. 2通信线路的安全防护

4. 1. 2. 1 应采用有效措施,预防线路截获,使线路截获设备无法工作。

4. 1. 2. 2应设置线路截获探测装置,及时发现线路截获事件并报警。

4. 1. 2. 3应设置线路截获定位装置,及时发现线路截获、窃取设备的准确位置。

4. 1. 2. 4 应定期测试信号强度,检查是否有非法装置接入线路。

4. 1. 2. 5应定期检查接线盒及其他易被人接近的线路部位。

4. 1. 2. 6应定期检查传输线路各线段及接点,更换老化变质的电缆。

4. 1. 2. 7传输线路应采用屏蔽电缆并有露天保护或埋于地下,远离强电线路或强电磁场发射源,以减少由于干扰引起的数据错误。

4. 1. 2. 8铺设室外电缆应采用金属铠装、屏蔽电缆或加装金属套管,以减少各种监控辐射对线路的干扰。

4. 1. 2. 9调制解调器应放置在受监视的区域,以防止外来连接的企图。应定期检查调制解调器的连接是否有篡改行为。

4. 1. 3信息传输安全

4. 1. 3. 1 密级信息到达终点之前,不应呈现明文状态。

4. 1. 3. 2传输密级信息时应进行网络加密,如链路加密、节点加密和用户加密等。

4. 1. 3. 3为保证密级数据的安全传递,应有备份的网络节点机。

4. 1. 3. 4不传送信息时接口应阻断。

4. 1. 3. 5应具有辨认正当通信伙伴的功能。

4. 1. 3. 6用拨号线能接触网络时,拨号码应予以保护、同时保密信息不宜存放在节点机内。

4. 2设备安全

4. 2. 1 设备的防盗和防毁

4. 2. 1. 1计算机系统的设备和部件应有明显标记。

4. 2. 1. 2计算机中心应利用光、电、无源红外等技术设置机房报警系统,并有专人值守。

4. 2. 1. 3机房应采用特殊门锁。

4. 2. 1. 4机房外部的网络设备应采取加固防护等措施。

4. 2. 2设备的安全可用

4. 2. 2. 1 支持计算机信息系统运行的所有设备,包括计算机主机、外部设备、网络设备以及其他辅助设备均应安全可用。

4. 2. 2. 2应提供可靠的运行支持,并有故障容错和故障恢复能力。

4. 3记录介质安全

4. 3. 1 应采取措施,防止存放有用数据的各类记录介质被盗、被毁和受损。

4. 3. 2系统中有很高使用价值或很高机密程度的重要数据,应采取加密等方法进行保护。

4. 3. 3应采取措施,防止删除和销毁的数据被非法拷贝。

4. 4安全管理中心的安全

4. 4. 1 安全管理中心应符合GB / T 2887—2000中4. 9的要求。

4. 4. 2安全管理中心应设置在中心机房,以各种方式与计算机信息系统的各类安全机制相连接。

4. 4. 3安全管理中心除了按照一般的机房建设要求进行建设外,还应设置关卡,必要时可安装闭路摄像监视系统。

5 网络安全

5. 1 网络安全建设

5. 1. 1应确定所设计、实现的网络设备、网络协议、网络软件及网络环境。

5. 1. 2应分析网络设备、网络协议、网络软件及网络环境的安全要求,分析其可能存在的薄弱环节以及

这些环节可能造成的危害和由此产生的后果。

- 5. 1. 3应确定网络设备、网络协议、网络软件及网络环境的安全策略,根据安全需求分析的结果,确定应控制的危害因素及控制程度、应保护的资源和保护程度。
- 5. 1. 4应确定网络设备、网络协议、网络软件及网络环境应达到的安全等级。
- 5. 1. 5应根据GB / T 9387. 2 1995确定网络设备、网络协议、网络软件及网络环境在ISO / OSI开放系统互联参考模型中所处的网络层次。
- 5. 1. 6应确定安全等级及网络层次,网络安全等级和网络各层次所对应的安全要素见表1。
- 5. 1. 7应根据5. 4的要求,使网络设备、网络协议、网络软件及网络环境达到预期的安全需求、安全等级。

表 1 网络安全等级、安全要素与各层的相互关系

安全等级 及 网络层次		安全要素										
		自主访问控制	强制访问控制	标记	用户身份鉴别	客体重用	安全审计	数据完整性	隐蔽信道分析	可信路径	可信恢复	抗抵赖
用户自主保护级	物理层							★				
	链路层	★			★			★				
	网络层	★			★			★				
	传输层	★			★			★				
	会话层	★			★			★				
	表示层	★			★			★				
	应用层	★			★			★				
系统审计保护级	物理层							★				
	链路层	★			★	★		★				
	网络层	★			★	★	★	★				
	传输层	★			★	★	★	★				
	会话层	★			★	★	★	★				
	表示层	★			★	★	★	★				
	应用层	★			★	★	★	★				★
安全标记保护级	物理层							★				
	链路层	★	★	★	★	★		★				
	网络层	★	★	★	★	★	★	★				★
	传输层	★	★	★	★	★	★	★				★
	会话层	★	★	★	★	★	★	★				★
	表示层	★	★	★	★	★	★	★				★
	应用层	★	★	★	★	★	★	★				★

表 1（续）

安全等级 及 网络层次		安全要素										
		自主访问控制	强制访问控制	标记	用户身份鉴别	客体重用	安全审计	数据完整性	隐蔽信道分析	可信路径	可信恢复	抗抵赖
结构化保护级	物理层							★				
	链路层	★	★	★	★	★		★				
	网络层	★	★	★	★	★	★	★	★	★		★
	传输层	★	★	★	★	★	★	★	★	★		★
	会话层	★	★	★	★	★	★	★	★	★		★
	表示层	★	★	★	★	★	★	★	★	★		★
	应用层	★	★	★	★	★	★	★	★	★		★
访问验证保护级	物理层							★				
	链路层	★	★	★	★	★		★				
	网络层	★	★	★	★	★	★	★	★	★	★	★
	传输层	★	★	★	★	★	★	★	★	★	★	★
	会话层	★	★	★	★	★	★	★	★	★	★	★
	表示层	★	★	★	★	★	★	★	★	★	★	★
	应用层	★	★	★	★	★	★	★	★	★	★	★
注：“★”表示应具有该项技术要求。												

5. 2网络安全基本要求
5. 2. 1 网络应具有对全网网络拓扑、网络配置及网络参数的统一管理、监督与控制功能。

5. 2. 2应采取安全措施，确保网络实体的环境安全、防电磁干扰和辐射干扰。

5. 2. 3应采取安全措施，确保网络数据传输、交换、存储处理及通信控制的安全。

5. 2. 4 网络应具有计算机病毒的预防措施。

5. 2. 5对灾难性事件应有应急措施。

5. 2. 6网络应具有必要的冗余度和降级处理能力。

5. 2. 7网络安全设施的接口设备应方便用户并实现透明操作。

5. 2. 8 网络应具有承受允许的最严重错误的能力。

5. 2. 9在确保安全的前提下应充分发挥资源共享的效能。

5. 2. 10网络应采取多重安全控制手段。每个安全控制手段均能产生充分的证据，以表明所完成操作的正确性。

5. 2. 11 网络应记载用户进入网络的各种活动，以提供事后检查。

5. 2. 12存取控制应逐级授权。网络在为授权用户提供合法服务的同时，应具有拒绝非法访问的功能。

5. 2. 13 网络应具有监视和控制网络负载状态的功能，以防止其崩溃和瘫痪。

5. 2. 14 局域网(LAN)与局域网之间、局域网与广域网(WAN)之间互连，应采用防火墙、入侵检测等安全保护措施。

5. 2. 15网络互联网不应影响互联双方原有的安全性。
5. 3网络基本安全技术
- 网络基本安全技术应包括对以下安全要素的保护：
- 自主访问控制；

——强制访问控制；

- 标记;
 - 用户身份鉴别;
 - 客体重用;
 - 安全审计;
 - 数据完整性;
 - 隐蔽信道分析;
 - 可信路径;
 - 可信恢复;
 - 抗抵赖。
5. 4详细技术要求
5. 4. 1 自主访问控制应符合GA / T 387 2002中6. 1的要求。
5. 4. 2强制访问控制应符合GA / T 387—2002中6. 2的要求。
5. 4. 3标记应符合GA / T 387—2002中6. 3的要求。
5. 4. 4身份鉴别应符合GA / T 387 2002中6. 4的要求。
5. 4. 5客体重用应符合GA / T 387—2002中6. 5的要求。
5. 4. 6审计应符合GA / T 387—2002中6. 6的要求。
5. 4. 7数据完整性应符合GA / T 387 2002中6. 7的要求。
5. 4. 8 隐蔽信道分析应符合GA / T 387—2002中6. 8的要求。
5. 4. 9可信路径应符合GA / T 387—2002中6. 9的要求。
5. 4. 10可信恢复应符合GA / T 387—2002中6. 10的要求。
5. 4. 11 抗抵赖应符合GA / T 387—2002中6. 11的要求。

6操作系统安全

6. 1 技术要求

计算机操作系统应满足表2所列出的安全功能技术等级要求。

表 2 安全功能技术等级

安全保证技术要求	安全保护等级				
	用户自主保护级	系统审计保护级	安全标记保护级	结构化保护级	访问验证保护级
自主访问控制	★	★	★	★	★
强制访问控制			★	★	★
标记			★	★	★
用户身份鉴别	★	★	★	★	★
客体重用		★	★	★	★
安全审计		★	★	★	★
数据完整性	★		★	★	★
隐蔽信道分析				★	★
可信路径				★	★
可信恢复					★
注：“★”表示应具有该项技术要求。					

6.2 使用

6.2.1 应使用成熟的操作系统(OS)。

6.2.2 在首次使用操作系统时,应对操作系统进行配置管理控制、网络访问控制、口令管理控制以及屏幕加锁控制。

6.2.3 应及时下载操作系统供应商实时发布的OS安全防范补丁,更新系统,减少OS在安全方面的漏洞,对原有的操作系统进行加固。

6.2.4 应及时安装系统和在用程序的补丁包,定期检查帐户和审计文件。

6.3 检查测试

应通过对当前系统配置的分析,查找可能使用户或闯入者获得未认证访问的配置,并对以下内容进行检测:

- 配置文件;
- 软件版本;
- 文件宿主和允许;
- SUID / SGID文件;
- 不规则文件;
- 用户账户;
- 工作组设置;
- 口令;
- 系统受损;
- 系统更改;
- 文件基线受损;
- 账户设置修改。

7 数据库管理系统安全

7.1 基本要求

数据库管理系统的安全性由可信的IT数据库产品自身来保证,并应具备以下特性:

- 保密性:保护存储在数据库中的数据不被泄露和未授权获取;
- 完整性:保护存储在数据库中的数据不被破坏和删除;
- 一致性:确保存储在数据库中的数据满足实体完整性、参照完整性和拥护定义完整性要求;
- 可用性:确保存储在数据库中的数据不因人为的和自然的原因对授权用户不可用。

7.2 身份鉴别

应符合GA / T 389—2002中4.1的要求。

7.3 标记与访问控制

应符合GA / T 389—2002中4.2的要求。

7.4 数据完整性

应符合GA / T 389—2002中4.3的要求。

7.5 数据库安全审计

应符合GA / T 389—2002中4.4的要求。

7.6 客体重用

应符合GA / T 389—2002中4.5的要求。

7.7 数据库可信恢复

应符合GA / T 389—2002中4.6的要求。

7.8 隐蔽信道分析

应符合GA / T 389—2002中4. 7的要求。

7. 9可信路径

应符合GA / T 389—2002中4. 8的要求。

7. 10推理控制

应符合GA / T 389 2002中4. 9的要求。

8应用系统安全

8. 1输入数据的确认

系统应具备输入数据的确认功能,以确保输入数据的正确性和适用性。

8. 2内部处理控制

系统应具备确认检查功能,以检查数据处理过程中的错误。

8. 3信息验证

在有安全措施要求的地方,应进行应用信息验证以保护信息内容的完整性。

8. 4输出数据的确认

从应用系统中输出的数据应经过确认,以确保存储信息相对于各种情况的处理正确而适当。

8. 5开发和支持过程的安全

系统在开发过程中应遵循ISO 9001:1994的要求,在支持过程中应按正式的更改控制程序进行更改控制。

8. 6计算机病毒的预防

系统应配置专用的计算机防病毒软件系统,并定期升级更新。同时应建立有效的防病毒管理机制。

中华人民共和国民用航空
行 业 标 准
民用航空空中交通管理
管理信息系统技术规范
第2部分：系统与网络安全
MH / T 4018. 2 2004

*

中国民航出版社出版发行
(北京市朝阳区光熙门北里甲31号楼)
— 邮政编码: 100028 —
北京华正印刷厂印刷
版权专有不得翻印

*

开本880X1230 1 / 16印张0. 75字数13千字
2005年5月第1版2005年5月第1次印刷 印数1—500册
统一书号: 1580110 • 247 定价: 10. 00元

MH

中华人民共和国民用航空行业标准

MH / T 401 8. 3—2004

民用航空空中交通管理 管理信息系统技术规范 第3部分：系统网络与接入

Technical standards for air traffic management
of civil aviation management information system—
Part 3: System network and access

2004-12-20发布

2005-04-01实施

中国民用航空总局 发布

目次

前言	
1 范围	1
2规范性引用文件	1
3术语和定义	2
4系统网络总体要求	3
4.1 网络结构	3
4.2传输协议	3
4.3 IP地址规划	3
4.4 IP地址分配	3
4.5广域网建设	3
5局域网设计	5
5.1 总体要求	5
5.2有线局域网	5
5.3无线局域网	5
5.4远程访问	5
6互 联	5
7总体网络安全	5

前 言

MH / T 4018《民用航空空中交通管理信息系统技术规范》分为三个部分：

- 第1部分：系统数据与接口；
- 第2部分：系统与网络安全；
- 第3部分：系统网络与接入。

本部分为MH / T 4018的第3部分。

本部分由中国民用航空总局空中交通管理局提出。

本部分由中国民用航空总局航空安全技术中心归口。

本部分由中国民用航空总局空中交通管理局负责起草，中国民用航空西北地区管理局空中交通管理局参加起草。

本部分主要起草人：吕小平、李朝阳、齐鸣、向宏武、胡兴宇、傅竑、丁蓉、陈鸿波、邱镭。

民用航空空中交通管理管理信息系统技术规范

第3部分：系统网络与接入

1 范围

MH / T 4018的本部分规定了民用航空空中交通管理(以下简称空管)管理信息系统网络与接入的技术规范。

本部分适用于空管管理信息系统的设计与建设。

2 规范性引用文件

下列文件中的条款通过MH / T 4018的本部分的引用而成为本部分的条款。凡是注日期的引用文件，其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本部分，然而，鼓励根据本部分达成协议的各方研究是否可使用这些文件的最新版本。凡是不注明日期的引用文件，其最新版本适用于本部分。

GB / T 13993. 2—2002通信光缆系列 第2部分：核心网用室外光缆

GB / T 13993. 3—2001 通信光缆系列 第3部分：综合布线用室内光缆

MH / T 4018. 1—2004 民用航空空中交通管理管理信息系统技术规范第1部分：系统数据与接口

MH / T 4018. 2—2004 民用航空空中交通管理管理信息系统技术规范第2部分：系统与网络安全

RFC 1918私有网络地址分配

EIA / TIA-232 DTE(数据终端设备)和DCE(数据电路端接设备)连接接口标准

EIA / TIA-232 RS422 EIA-232标准的扩充

EIA / TIA-232 RS449 EIA-232标准的扩充

EIA / TIA-568商业建筑物电信布线标准第1部分：通用要求—附录5—电信外围场地的电信布线

IEEE 802系列

IEEE 802. 1D信息技术—系统间的通信和信息交换—局域网和城域网共同规范第3部分：媒介接入控制桥

IEEE 802. 1P定义了优先级和GARP(Generic Attribute Registration Protoc01)

IEEE 802. 1Q虚拟桥局域网

IEEE 802. 1X局域和都市区域网络—网络通路控制

IEEE 802. 3AB信息技术—电信和系统间的信息交换—局域网和城域网—特殊要求—CSMA / CD及物理层规范的补充：物理层参数和1 000MB / S操作规范

IEEE 802. 3U快速以太网100BASE-T、100BASE-TX(用于五类UTP电缆)、100BASE-FX(用于光纤)符合OSI七层网络结构中物理层规范支持的物理介质

IEEE 802. 3z千兆以太网1 000BASE-SX、1 000BASE-LX(光纤、铜缆)标准

IEEE 802. 11B特殊要求第11部分：无线局域网媒体访问控制(MAC)和物理层(PHY)规范扩展到2. 4 GHz带宽的高速物理层勘误1

ITU-T G系列

ITU-T G. 652单模光纤光缆的特性

ITU-T G. 65X(X为0~5)

ITU-T G. 703 系列数字接口的物理 / 电特性

ITU-T G. 704用于1 544、6 312、2 048、8 448和44 736 kbit / s速率系列级的同步帧结构

ITU-T G. 707 同步数字系列(SDH)的网络节点接口

ITU-T G. 957 与同步数字体系有关的设备和系统的光接口

ITU-T G. 992. 1 不对称数字用户线(ADSL)的收发信机

ITU-T G. 992. 2 用在TCM-ISDN串音环境下的重叠PSD掩码实例

ITU-T I系列

ITU-T I. 361 B-ISDN ATM层规范

ITU-T I. 365. 5 SAR、CPCS子层

ITU-T I. 370 ISDN帧中继承载业务的拥塞管理

ITU-T I. 432. 2 B-ISDN用户—网络接口—物理层规范:155 520 kbit / s和622 080 kbit / s的操作

ITU-T Q. 704信令网功能和消息

ITU-T Q. 922 帧方式承载业务的ISDN数据链路层规程

ITU-T Q. 933 1号数字用户信令系统(DSS1)— 帧方式交换、永久虚连接控制及状态监控的信令规程

ITU-T Q. 2110 B-ISDN ATM适配层—业务规定的面向连接的规程(SSCOP)

ITU-T Q. 2130 B-ISDN信令ATM适配层支持用户网络接口信令的业务规定的协调功能(在UNI的SSCF)

ITU-T Q. 2140 B-ISDN信令ATM适配层—网络节点接口的信令的业务规定的协调功能(在NNI的SSCF)

ITU-T Q. 2761 NO. 7信令系统的B-ISUP的功能描述

ITU-T Q. 2762 NO. 7信令系统的B-ISUP的消息和信号的总功能

ITU-T Q. 2762(1999) 国际应急首选方案的支持

ITU-T Q. 2763 NO. 7信令系统的B-ISUP—格式编码

ITU-T Q. 2764 NO. 7信令系统的B-ISDN用户部分(B-ISUP)— 基本呼叫规程

ITU-T Q. 2931 宽带综合业务数字网(B-ISDN)— NO. 2数字用户信令系统—用于基本呼叫 / 连接控制的用户网络接口第三层规范

ITU-T Q. 2971 宽带综合业务数字网((B-ISDN)—NO. 2数字用户信令系统—用于点到多点呼叫 / 连接控制的第三层用户网络接口层规程

ITU-T V系列

ITU-T V. 24数据终端设备(DTE)和数据电路终接设备(DCE)之间的交换电路定义表

ITU-T V. 28 非平衡双流接口电路的电特性

ITU-T V. 34公用电话交换网和点对点二线租用电话型电路上使用、以高达33 600 bit / s数据传信速率操作的调制解调器

ITU-T V. 35使用60 kHz~108 kHz群带电路速率为48 kbit / s的数据传输

ITU-T V. 90 在PSTN中使用的数据信号速率下行速率达到56 000 bit / s,上行达到33 600 bit / s的数字调制解调器和模拟调制解调器对

ITU-T V. 92用于纠错程序的新交互作用设备

ITU-T X系列

ITU-T X. 21BIS X. 25中采用的物理层协议

3 术语和定义

MH / T 4018. 1—2004确立的以及下列术语和定义适用于MH / T 4018的本部分。

3. 1

空管管理信息系统网络 management information system network of air traffic managment
为了整合空管信息而建设的全国性的企业内部网。

4系统网络总体要求

4. 1 网络结构

应采用Intranet / Internet形式。

4. 2传输协议

应采用TCP / IP IPv4或IPv6协议。

4. 3 IP地址规划

系统网络域名及IP地址规划见表1,各地区空管部门可在自己的IP范围内统一规划,自由使用,域名解析由各地区空管部门自行解析。

表 1 IP 地址规划表

单位名称	IP 地址	子网掩码	域 名
中国民用航空总局空中交通管理局	10. 0. 0. 0	255. 248. 0. 0	www. atmb. gov
			www. atmb. net
中国民用航空华北地区管理局空中交通管理局	10. 4. 0. 0	255. 248. 0. 0	www. bj. atmb. gov
			www. bj. atmb. net
中国民用航空东北地区管理局空中交通管理局	10. 18. 0. 0	255. 248. 0. 0	www. sy. atmb. gov
			www. sy. atmb. net
中国民用航空华东地区管理局空中交通管理局	10. 12. 0. 0	255. 248. 0. 0	www. sh. atmb. gov
			www. sh. atmb. net
中国民用航空中南地区管理局空中交通管理局	10. 16. 0. 0	255. 248. 0. 0	www. gz. atmb. gov
			www. gz. atmb. net
中国民用航空西南地区管理局空中交通管理局	10. 20. 0. 0	255. 248. 0. 0	www. cd. atmb. gov
			www. cd. atmb. net
中国民用航空西北地区管理局空中交通管理局	10. 24. 0. 0	255. 248. 0. 0	www. xa. atmb. gov
			www. xa. atmb. net
中国民用航空新疆管理局空中交通管理局	10. 28. 0. 0	255. 248. 0. 0	www. wl. atmb. gov
			www. wl. atmb. net

4. 4 IP地址分配

4. 4. 1 IP地址分配应采用VLSM(可变长子网掩码)技术。

4. 4. 2系统网络地址按RFC 1918中规定的A类保留地址段10. 0. 0. 0进行分配。

4. 4. 3各地区空管部门应按照所分配的地址段,制定本地的IP地址分配规划。在分配规划中,应遵循以下原则:

- 以子网掩码长度为24位进行分配,为节省IP地址资源,可根据需要增加网络掩码的长度;
- 同一地区和单位分配地址时,采用连续地址段,并留出一段备用地址;
- 各地区空管部门内部网络互联时路由器端到端连接的接口地址由上级单位提供,同级单位互联时双方通过协商,由一方提供连接地址,点对点的连接可采用32位子网掩码。

4. 5广域网建设

4. 5. 1 拓朴结构

系统网络的拓朴结构采用部分网状的星形结构,中心结点为民航空管主管部门,各地区空管部门的中心结点为地区空管部门信息中心。

4. 5. 2传输协议

民航空管主管部门和地区空管部门、各地区空管部门之间的局域网互相连接时应选用下列协议：静态路由、动态路由、OSPF、RIP、RIP II、BGP、IGRP、EIGRP、IGMP、PIM DM、PIM SM、DHCP Relay、VRRP协议。

4. 5. 3传输路由

空管管理信息系统网络应基于空管ATM数据网，对不具备空管ATM数据网链路的地区应采用光纤、微波、帧中继等。

4. 5. 4传输带宽

空管管理信息网所分配的带宽不应低于1M，备份线路所分配的带宽不应低于128K。

4. 5. 5通信接口

4. 5. 5. 1 ATM接口

不同速率的ATM接口应分别符合以下标准：

- 155. 52Mbps UNI接口符合ITU-T I. 432. 2；
- 155. 52Mbps NNI接口符合ITU-T G. 707；
- 155. 52Mbps光接口符合ITU-T G. 957；
- ATM层UNI / NNI接口符合ITU-T I. 361；
- SAR、CPCS子层符合ITU-T I. 365. 5；
- SSCOP子层符合ITU-T Q. 2110；
- E1接口及帧结构标准符合ITU-T G. 703或ITU-T G. 704；
- SSCF关于UNI / NNI子层符合ITU-T Q. 2130或ITU-T Q. 2140；
- UNI接口信令符合ITU-T Q. 2931、ITU-T Q. 2971；
- NNI接口信令符合ITU-T Q. 704、ITU-T Q. 2761~2764。

4. 5. 5. 2帧中继接口

帧中继物理层的接口特性应符合ITU-T X、ITU-T V、ITU-T G或ITU-T I系列接口标准。

帧中继数据链路层应符合ITU-T Q. 922附件A的相关规定。

帧中继PVC管理规程应符合ITU-T Q. 933附件A的相关规定。

帧中继SVC信令应符合ITU-T Q. 933的相关规定。

帧中继拥塞控制应具有ITU-T I. 370及ITU-T Q. 922附件A中规定的相关功能。

4. 5. 5. 3光纤接口

主干用光纤宜使用ITU-T G. 652所推荐的单模光纤，光纤及其终端设备应符合ITU-T G. 65x的规定；其他光纤及其终端设备应符合GB / T 13993. 2—2002、GB / T 13993. 3—2001的规定。

至少预留四芯做为备份。

4. 5. 5. 4 卫星接口

应符合ITU-T V. 24、ITU-T V. 35的规定。

4. 5. 5. 5微波接口

应符合ITU-T G. 703的规定。

4. 5. 5. 6 XDSL接口

应符合ITU-T G. 992. 1或者ITU-T G. 992. 2的规定。

4. 5. 5. 7 PSIN接口

应符合ITU-T V. 90、ITU-T V. 92或ITU-T V. 34的规定。

4. 5. 5. 8 同步串口、异步串口

应符合EIA / TIA-232、EIA / TIA-232RS422或EIA / TIA-232 RS449、ITU-T V. 35、ITU-T V. 24、ITU-T V. 28、ITU-T X. 21BIS的规定。

5 局域网设计

5.1 总体要求

5.1.1 建设局域网时应采用以太网(Ethernet)技术连接方式。

5.1.2 网络协议应支持TCP / IP、VLAN、STP。

5.1.3 局域网应符合IEEE 802.3U或IEEE 802.3z的规定。

5.1.4 局域网网络边界的路由器应支持RIP I、RIP II协议,并统一命名规则。

5.1.5 路由器命名为:地名四字代码路由器编号。

5.2 有线局域网

5.2.1 综合布线物理介质应采用双绞线、光纤,智能综合布线规则应符合EIA / TIA—568标准。

5.2.2 综合布线系统应采用超五类以上的布线系统,工作区应根据实际情况设置信息插座,信息插座应具有话音点和数据点。

5.2.3 物理线路应符合IEEE 808.3U、IEEE 808.3AB或IEEE 802.3Z接口标准,其接口特性应符合IEEE.802系列标准中对应的标准。

5.2.4 局域网内的交换机应具备以下功能:

- 支持二层线速转发;
- 支持IEEE 802.1Q的虚拟局域网(VLAN)划分能力;
- 支持IEEE 802.1D的生成树(Spaning Tree)容错能力;
- 支持物理地址与IP地址绑定能力;
- 支持IEEE 802.1P的链路层服务质量(QoS)控制能力;
- 支持组播协议。

5.3 无线局域网

应符合IEEE 802.11B、IEEE 802.1X的规定。

5.4 远程访问

应设置拨号访问服务器,通过电话拨号连接到授权的用户组。

6 互联

6.1 总局空管局与各地区空管局之间、各地区空管局之间、各地区空管局与地区空管中心(站)之间的网络应互联;专业数据网与管理信息系统网之间的网络应互联。

6.2 网关路由器或三层交换机应用技术指标如下:

- 如使用三层交换机,应能实现第二、三层线速转发;
- 支持IEEE 802.1Q的虚拟局域网(VLAN)划分能力;
- 支持IEEE 802.1D的生成树(Spaning Tree)容错能力;
- 支持IEEE 802.1P的链路层服务质量(QoS)控制能力;
- 支持动态路由协议(RIP)、最短路径优先(OSPF)路由协议;
- 支持第四层访问控制能力、访问控制列表(Access Control List)等支持UDP转发能力(UDP forwarding);
- 支持物理地址与IP地址绑定能力。

7 总体网络安全

见MH / T 4018.2—2004。

中华人民共和国民用航空
行 业 标 准
民用航空空中交通管理
管理信息系统技术规范
第3部分：系统网络与接入

MH / T 401 8. 3—2004

*

中国民航出版社出版发行
(北京市朝阳区光熙门北里甲31号楼)
— 邮政编码：100028 —
北京华正印刷厂印刷

版权专有不得翻印

*

开本880X1230 1 / 16印张0. 75字数9千字
2005年5月第1版2005年5月第1次印刷印数1--500册
统一书号：1580110 • 248定价：10. 00元