



中华人民共和国粮食行业标准

LS/T 1806—2017

粮食信息系统网络设计规范

Network specification for grain information system

2017-03-10 发布

2017-06-01 实施

国家粮食局 发布

目 次

前言	I
1 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 网络结构	3
6 拓扑结构	3
7 设备要求	3
8 域名和 IP 管理	3
9 机房建设	4
10 服务质量	4
11 网络安全	5
12 信息安全	5
13 网络管理	5
参考文献	6

前 言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由国家粮食局提出。

本标准由全国粮油标准化技术委员会(SAC/TC 270)归口。

本标准起草单位：国家信息中心、国家粮油信息中心、国贸工程设计院、河南工业大学、江苏省粮食局、航天信息股份有限公司。

本标准主要起草人：徐枫、宦茂盛、李素云、王子亮、侯璐、魏慧军、徐锦萍、彭守根、王涛、甄彤、高巍、臧传真。

粮食信息系统网络设计规范

1 范围

本标准规定了粮食行业各级行政管理部门间、粮食行政管理部门与粮食企业间进行信息交换与共享时,所涉及的信息系统传输网络的基本设计要求,包括网络结构、拓扑结构、设备要求、域名和 IP 管理要求、机房建设要求、服务质量要求、网络安全要求和信息安全要求。

本标准适用于粮食行业信息系统网络的总体规划、设计、开发、应用、培训和运行维护,以及粮食行业信息交换与共享,支持粮食行业信息系统互联互通。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

- GB/T 2887—2011 计算机场地通用规范
- GB/T 5271.1—2000 信息技术 词汇 第 1 部分:基本术语
- GB/T 5271.9—2001 信息技术 词汇 第 9 部分:数据通信
- GB/T 7260.1—2008 不间断电源设备 第 1-1 部分:操作人员触及区使用的 UPS 的一般规定和安全要求
- GB/T 7260.2—2009 不间断电源设备(UPS) 第 2 部分:电磁兼容性(EMC)要求
- GB/T 7260.3—2003 不间断电源设备(UPS) 第 3 部分:确定性能的方法和试验要求
- GB/T 7260.4—2008 不间断电源设备 第 1-2 部分:限制触及区使用的 UPS 的一般规定和安全要求
- GB/T 18018—2007 信息安全技术 路由器安全技术要求
- GB/T 18903—2002 信息技术 服务质量:框架
- GB/T 20270—2006 信息安全技术 网络基础安全技术要求
- GB/T 20281—2015 信息安全技术 防火墙安全技术要求和测试评价方法
- GB/T 21050—2007 信息安全技术 网络交换机安全技术要求(评估保证级 3)
- GB/T 21061—2007 国家电子政务网络技术和运行管理规范
- GB/T 22239—2008 信息安全技术 信息系统安全等级保护基本要求
- GB 50174—2008 电子信息系统机房设计规范
- LS/T 1807—2017 粮食信息安全技术规范
- YD/T 1190—2002 基于网络的虚拟 IP 专用网(IP-VPN)框架
- YD/T 5227—2015 云计算资源池系统设备安装工程设计规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

国家电子政务外网 national e-government extranet

满足各级政务部门社会管理、公共服务等面向社会服务需要的专门网络。国家电子政务外网由中央政务外网和地方政务外网组成,与互联网逻辑隔离。

3.2

国家电子政务内网 national e-government intranet

主要满足各级政务部门内部办公、管理、协调、监督和决策的需要,同时满足副省级以上政务部门的特殊办公需要的专门网络,由党委、人大、政府、政协、法院、检察院的业务网络互联互通形成,与互联网物理隔离。

3.3

互联网 internet

广域网、局域网及单机按照一定的通讯协议组成的国际计算机网络。

3.4

局域网 local area network (LAN)

一种位于有限地理区域的用户宅院内的计算机网络。

注:局域网内的通信不服从外部的规则;但是,跨越网域边界的通信可能要服从某种形式的规则。

[GB/T 5271.1—2000,定义 01.01.46]

3.5

虚拟专用网络 virtual private network (VPN)

在共享网络中,通过多种技术(如隧道、加密等)实现原有专用网络的能力,并在保证网络的安全性、可靠性、可管理性的同时提供更强的扩展性和灵活性。

[YD/T 1190—2002,定义 3.1.12]

3.6

城域网 metropolitant network

连接位于同一城市区域内的几个局域网的一种网络。

[GB/T 5271.9—2001,定义 09.07.10]

3.7

广域网 wide area network (WAN)

一种网络,它对一个比局域网或城域网更大的地理区域提供各种通信服务。

[GB/T 5271.9—2001,定义 09.07.11]

3.8

网络交换机 network switch

网络中连接各个节点或其他网络设备的设备,提供了开放式系统互联模型二层的逻辑路径,基于数据链路层信息转发数据包,能够基于目的地址过滤。

[GB/T 21050—2007,定义 3.1.5]

3.9

节点 node

计算机网络系统中可以对信息进行存储或转发的设备。

[GB/T 21050—2007,定义 3.1.6]

3.10

路由器 router

主要的网络节点设备,工作在网络层,通过路由选择算法决定流经数据的存储转发,并具备访问控制和安全扩展功能。

[GB/T 18018—2007,定义 3.1.1]

4 缩略语

下列缩略语适用于本文件。

IP: 网际协议(Internet Protocol)

QoS: 服务质量(Quality of Service)

UPS: 不间断电源(Uninterruptible Power System /Uninterruptible Power Supply)

5 网络结构

粮食信息系统网络包括互联网、国家电子政务外网、国家电子政务内网、业务专网等。其中,国家电子政务外网与互联网逻辑隔离,国家电子政务内网、业务专网与互联网物理隔离。

粮食行业信息系统交换与共享网络互联互通,包括各级粮食行政管理部门业务系统之间、粮食行政管理部门业务系统与粮食企业业务系统之间进行信息交换与共享,网络节点包括但不限于:

- a) 国家粮食局业务信息系统;
- b) 省级粮食行政管理部门业务信息系统;
- c) 市级粮食行政管理部门业务信息系统;
- d) 县级粮食行政管理部门业务信息系统;
- e) 粮食企业业务信息系统。

6 拓扑结构

粮食行业各信息系统网络节点在网络接入区的网络拓扑结构应表示成星型、环型或者总线型,同时满足以下要求:

- a) 应规范星型、环型及总线型拓扑结构,最小化网络设备间的连接故障,同时确保网络设备便于增加或减少;
- b) 星型、环型及总线型拓扑应具有可扩展性和灵活性;
- c) 宜采用以太网标准支持星型局域网设计,采用点对点连接和结构化布线拓扑;
- d) 网络接入层、汇聚层和核心层应针对不同的接入网络,提供各自独立的接入端。

7 设备要求

7.1 路由器

接入路由器应符合 GB/T 18018—2017 的相关要求,其中国家级和省级信息系统网络接入区的接入路由器宜按照等级保护三级安全要求进行配置,省级以下信息系统、企业业务信息系统的接入路由器宜按照等级保护二级安全要求进行配置。

7.2 网络交换机

网络交换机应符合 GB/T 21050—2007 中第 5 章~第 7 章的相关要求。

7.3 防火墙

防火墙应符合 GB/T 20281—2015 中第 6 章的相关要求。

8 域名和 IP 管理

8.1 域名要求

域名管理应符合 GB/T 21061—2007 中 9.2 的相关要求。

粮食信息系统网络域名的命名应遵循以下原则：

- a) 各级网络的子域名由英文字母(大小写等价)、数字(0~9)和连接符(-)组合而成；
- b) 域名的命名应符合以下要求：
 - 名称长度不应超过 25 个字符；
 - 域名的主体不应使用含有“CHINA”“CHINESE”“CN”“NATIONAL”等字样的名称；
 - 不应使用公众知晓的其他国家或地区名称、外国地名、国际组织名称；
 - 不应使用行业名称或商品的通用名称；
 - 不应使用他人已在中国注册过的企业名称或者商标名称；
 - 不应使用对国家、社会或者公共利益有损害的名称。

8.2 IP 地址要求

IP 地址的划分应符合 GB/T 21061—2007 中 9.1 的相关要求。

9 机房建设

9.1 基本要求

机房建设应符合 GB/T 2887—2011 中第 4 章、GB 50174—2008 中第 3 章和 LS/T 1807—2017 中 8.1.1 的相关要求。其中，国家级、省级机房应按照国家标准 B 级机房进行建设，省级以下机房宜按照 B 级机房进行建设；系统通过云平台进行搭建的，应参照云计算服务机房建设标准 YD/T 5227—2015 中 9.1 进行建设。

9.2 选址要求

按 GB 50174—2008 中 4.1 执行。政务机构各类机房应建在建筑物可控范围内，不宜与其他设备共享空间。

9.3 UPS 要求

UPS 系统应符合 GB/T 7260 系列标准的相关要求。

9.4 接地要求

接地保护系统应符合 GB/T 2887—2011 中 4.4 的相关要求，以及 GB 50174—2008 中 8.3 和 8.4 的相关要求。

9.5 消防要求

机房消防设施建设应符合 GB 50174—2008 中第 13 章的要求。

9.6 电磁屏蔽要求

涉密机房建设应符合 GB 50174—2008 中第 9 章的要求。

10 服务质量

粮食信息系统网络服务质量应符合 GB/T 18903—2002 中第 6 章规定的要求，同时还应符合下列要求：

- a) 粮食信息系统网络广域网 QoS 各指标应达到以下要求：

- 平均时间延迟 <0.2 s;
- 延迟抖动 <0.01 s;
- 吞吐量 >128 M/s;
- 丢包率 $<0.05\%$;
- 可用性 $>99.9\%$;
- 可靠性 ≥ 365 d。

b) 粮食信息系统网络城域网 QoS 各指标应达到以下要求:

- 平均时间延迟 <0.2 s;
- 延迟抖动 <0.01 s;
- 吞吐量 >128 M/s;
- 丢包率 $<0.05\%$;
- 可用性 $>99.9\%$;
- 可靠性 ≥ 365 d。

11 网络安全

粮食信息系统网络接入区的网络安全应符合 GB/T 22239—2008 中 7.1.2 和 7.2.5.6 的要求。

12 信息安全

信息安全技术应符合 GB/T 20270—2006 和 LS/T 1807—2017 中 8.4 的相关要求。信息传输应根据传输数据的涉密程度,选择不同的网络进行传输,主要包括以下几种方式:

- a) 涉密信息应通过国家电子政务内网进行传输;
- b) 非涉密的敏感信息应通过国家电子政务外网进行传输;
- c) 公开的粮食行业信息和为社会公众提供的公共服务,可通过互联网进行传输;
- d) 传输信息有保密规定的,按国家保密管理部门和公安部有关规定执行。

13 网络管理

具备条件的粮食信息系统网络接入区的网络管理,应实现网络拓扑结构的可视化,便于及时进行故障处理,提高网络管理效率。

参 考 文 献

- [1] GB/T 17859—1999 计算机信息系统安全保护等级划分准则
 - [2] GB/T 30850.3—2014 电子政务标准化指南 第3部分:网络建设
 - [3] GAT 669.8—2008 城市监控报警联网系统 技术标准 第8部分:传输网络技术要求
 - [4] GW0101 2014 国家电子政务外网信息安全标准体系框架
 - [5] GW0102 2014 国家电子政务外网信息安全标准化工作规范
 - [6] GW0103 2011 国家电子政务外网安全等级保护基本要求
 - [7] GW0104 2014 国家电子政务外网安全等级保护实施指南
 - [8] GW0201 2011 国家电子政务外网 IPSec VPN 安全接入技术要求与实施指南
 - [9] GW0202 2014 国家电子政务外网安全接入平台技术规范
 - [10] GW0203 2014 国家电子政务外网安全监测体系技术规范与实施指南
 - [11] GW0204 2014 国家电子政务外网安全管理系统技术要求与接口规范
 - [12] GW0205 2014 国家电子政务外网跨网数据安全交换技术要求与实施指南
 - [13] GW0206 2014 接入政务外网的局域网安全技术规范
 - [14] GW0206 2015 国家电子政务外网 IPv4 地址规划
 - [15] 国家电子文件管理“十三五”规划
 - [16] 国家信息化领导小组关于我国电子政务建设指导意见(中办发[2002]17号)
 - [17] 国家信息化领导小组关于推进国家电子政务网络建设的意见(中办发[2006]18号)
 - [18] 国家信息化领导小组关于加强信息安全保障工作的意见(中办发[2003]27号)
 - [19] 国家电子政务总体框架(国信[2006]2号)
-