ICS 33.040.40
CCS M 32

T/UNP

团　　体　　标　　准

T / UNP XXX—2024

数据中心 计算机网络系统维护管理技术规范

Technical specification for maintenance and management of computer network systems in data centers

2024 — XX — XX 发布　　2024 — XX — XX

发 布

目　　次

前　言

本文件按GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的要求起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由提出。

本文件由xx归口。

本文件主要起草单位：。

本文件主要起草人：。

数据中心　计算机网络系统维护管理技术规范

1　范围

本文件规定了数据中心计算机网络系统维护管理的总体要求、网络管理、设备及软件系统维护管理、机房维护管理和安全维护管理。

本文件适用于数据中心计算机网络系统的维护和管理。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 50052　供配电系统设计规范

GB 50174　数据中心设计规范

3　术语和定义

本文件没有需要界定的术语和定义。

4　符号和缩略语

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

MAC 介质访问控制　Media Access Control

NAT 网络地址转换　Network Address Translation

SNMP 简单网络管理协议　Simple Network Management 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

5　总体要求

5.1　维护管理范围

应包括对数据中心的网络、设备、软件系统、机房的运行维护以及安全要求的维护和管理。

5.2　维护周期

维护周期应保证每24 h对各设备循环检查一次，节假日例行检查。

5.3 应急处理

5.3.1 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。

5.3.2 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。

6 网络维护管理

6.1 网络管理系统

数据中心应建立网络管理系统，对计算机网络所用的设备、链路等进行集中监视。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。

6.2 网络管理接口

6.2.1 网络设备应提供基于 SNMP 协议的网络管理接口。

6.2.2 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。

6.3 网络维护

6.3.1 每月应对核心网络设备运行状态进行评估，包括 CPU/内存使用率、丢包率、时延等关键指标。当发现性能下降或带宽拥塞时，应优化路由策略或扩展带宽资源

6.3.2 应通过服务质量策略，对语音、视频等关键业务流量进行优先级配置。

6.3.3 所有网络配置变更必须提交变更申请，并在实施前进行测试。变更实施后需进行功能验证，

6.3.4 每季度应检查发布的固件和补丁，针对已知安全漏洞进行更新；升级前应在测试环境验证兼容性，不应影响生产网络。

6.4 其他要求

6.4.1 网络管理信息与信息网络设备、运行的实际数据应保持一致。

6.4.2 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 s。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%。

6.4.3 各种日志文件应至少保存 12 个月的事件。

6.4.4 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。

7 设备维护管理

7.1 设备故障处理流程

设备故障处理流程应符合以下要求：

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。

7.2 路由器维护管理

7.2.1 路由器基本配置

路由器基本配置应符合以下要求：

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

7.2.2 路由器系统文件管理

7.2.2.1 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：

7.2.2.2 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。

7.2.3 路由器维护

7.2.3.1 路由器设备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。

7.2.3.2 路由器设备故障维护应包括：

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。

7.3 交换机维护管理

7.3.1 交换机基本配置应包括：

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） 设置交换机设备的管理接口 IP 地址，关闭交换机上不使用的端口。

7.3.2 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。

7.3.3 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。

7.3.4 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。

7.3.5 VLAN 系统维护要求应符合下列要求：

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的链路进行配置和管理。

8 软件维护管理

8.1 服务器及软件系统

8.1.1 服务器

8.1.1.1 服务器应放置在专业机房内，并安装固定在标准机柜中。

8.1.1.2 应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。

8.1.1.3 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。

8.1.2 软件系统

8.1.2.1 应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。

8.1.2.2 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。

8.1.2.3 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。

8.1.2.4 应查看系统运行日志，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。

8.1.2.5 应检查防病毒软件是否告警，病毒库是否更新。

8.1.2.6 应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。

8.2 防火墙

8.2.1 防火墙安全策略应包括：

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。

8.2.2 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。

8.3 IDS 系统

IDS维护应检查以下内容：

a) 系统运行情况，检测误报率、报率；
b) 系统策略状态；
c) 系统资源状态；
d) 运行日志，日志；
e) 备份及分析。

8.4 VPN 系统

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。

8.5 安全审计与监控系统

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。

9 机房维护管理

9.1 机房环境要求

数据中心机房环境应符合以下要求：

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 的要求；
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 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 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；
i) 应保持机房环境卫生，定期打扫，定期清理。

9.2 机房制度要求

9.2.1 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。
9.2.2 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。

9.3 UPS 系统管理维护

UPS系统管理维护应符合下列要求：

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：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。

10 安全要求

10.1 资产安全

10.1.1 应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容
10.1.2 应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施。
10.1.3 应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理

10.2 介质安全

10.2.1 应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点。
10.2.2 应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录。

10.3 设备安全

10.3.1 应对备份和冗余设备等各种设备线路指定专门的部门或人员定期进行维护管理

10.3.2 应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等。
10.3.3 信息处理设备应经过审批才能带离机房或办公地点，含有存储介质的设备带出工作环境时其中重要数据应加密。
10.3.4 含有存储介质的设备在报废或重用前，应进行完全清除或被安全覆盖，保证该设备上的敏感数据和授权软件无法被恢复重用。

10.4 漏洞和风险

10.4.1 应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补。
10.4.2 应定期开展安全测评，形成安全测评报告，采取措施应对发现的安全问题。

10.5 网络和系统安全

10.5.1 应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限。
10.5.2 应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制
10.5.3 应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定。
10.5.4 应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等。
10.5.5 应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容。
10.5.6 应指定专门的部门或人员对日志、监测和报警数据等进行分析、统计，及时发现可疑行为。
10.5.7 应控制变更性运维，经过审批后才可改变连接、安装系统组件或调整配置参数，操作过程中应保留不可更改的审计日志，操作结束后应同步更新配置信息库。
10.5.8 应控制运维工具的使用，经过审批后才可接入进行操作，操作过程中应保留不可更改的审计日志，操作结束后应删除工具中的敏感数据。
10.5.9 应控制远程运维的开通，经过审批后才可开通远程运维接口或通道，操作过程中应保留不可更改的审计日志，操作结束后立即关闭接口或通道。
10.5.10 应保证所有与外部的连接均得到授权和批准，应定期检查违反规定无线上网及其他违反网络安全策略的行为。

10.6 恶意代码防范

10.6.1 应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等。
10.6.2 应定期验证防范恶意代码攻击的技术措施的有效性。

10.7 配置安全

10.7.1 应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等。
10.7.2 应将基本配量信息改变纳入变更范畴，实施对配置信息改变的控制，并及时更新基本配量信息库。

10.8 变更安全

10.8.1 应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施。
10.8.2 应建立变更的申报和审批控制程序，依据程序控制所有的变更，记录变更实施过程。

10.8.3 应建立中止变更并从失败变更中恢复的程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。

10.9 备份安全

10.9.1 应识别需要定期备份的重要业务信息、系统数据及软件系统等
10.9.2 应规定备份信息的备份方式、备份频度、存储介质、保存期等。
10.9.3 应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。

10.10 安全事件处理

10.10.1 应及时向安全管理部门报告所发现的安全点和可事件。
10.10.2 应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等。
10.10.3 应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训。
10.10.4 对造成系统中断和造成信息泄漏的重大安全事件应采用不同的处理程序和报告程序。

10.11 应急预案

10.11.1 应规定统一的应急预案框架，包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容。
10.11.2 应制定重要事件的应急预案，包括应急处理流程、系统复流程等内容。
10.11.3 应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练。
10.11.4 应定期对原有的应急预案重新评估，修订完善。