# **成都市公共卫生临床医疗中心**

# **医院网络运维服务内容及需求**

# 一、维保服务要求和内容

**1.服务方式**

1.1备件服务：提供7×24小时备件，备机支持服务；

1.2远程服务：通过VPN网络接入我院进行远程协助的方式处理维保问题；

1.3现场服务：通过现场的方式直接进行故障的解决处理；

1.4在故障的处理过程中，优先选择最快速恢复业务的服务方式，及时对事件做出响应，缩短故障的解决时间；若远程方式无法有效解决故障，需及时通过现场服务方式进行故障的解决。

**2.服务时间**

2.1提供7×24小时服务台支持

2.2提供7×24小时备件，备机支持

2.3提供7×24小时现场支持

**3.服务指标**

报名单位须提供我院所有“产品清单”（详见本节“9.产品清单”）的备件支持（7×24小时），在我院现场放置部分常用及重要备件，并针对业务提供高级别的支持。

**4.具体服务分类**

|  |  |  |
| --- | --- | --- |
| 序号 | 分类 | 具体服务内容 |
| 4**.**1 | 远程问题诊断与支持服务 | 我院可通过指定电话、邮件、网站提出服务请求，报名单位远程服务工程师需及时与我院沟通，通过电话支持/远程接入等远程方式对服务范围内的设备进行诊断及技术支持。 |
| 4**.**2 | 现场支持服务 | 对于没有条件进行远程支持、或未能通过远程支持诊断解决的问题，报名单位服务工程师在SLA约定时间内到客户现场进行问题的诊断、并负责硬件相关问题的排除。 |
| 4**.**3 | 备件支持服务 | 根据远程或现场诊断结果，如需更换备件来修复硬件问题，报名单位在合同规定的服务时效内将备件送至现场并使用备件恢复业务。提供7\*24小时备件，备机支持服务。 |
| 4**.**4 | 紧急故障恢复服务 | 由于客观原因无法及时判断、定位故障的情况下，报名单位服务工程师将在征求我院的意见后，提供紧急故障恢复服务，利用应急预案或经我院许可的技术方案进行应急处置，优先恢复业务。 |
| 4.5 | 辅助故障定位服务 | 在客户端如出现系统故障难以迅速准确定位的情况，报名单位服务工程师提供辅助故障定位服务，通过协调、配合相关软硬件服务厂商共同对系统故障进行排查定位，避免因多方推委造成我院业务的损失。 |

**5.运维服务**

5.1要求报名单位提供从监控/巡检、预防性检查、日常运维到服务请求和事件响应、系统优化的全面支持。通过运维服务，为我院基础架构的扩展提供实施和必要的支持工作。

5.2同时通过专业的技术服务团队通过专业的可以落实的服务方案，高效规范的管理模式、管理流程和管理工具提升我院的运维服务水平。

**6.服务方式**

运维服务的形式采用按需响应式支持服务，主要采用以下两种方式提供：

6.1远程服务：通过VPN等手段进行远程监控和故障的解决处理；

6.2现场服务：通过现场的方式直接进行故障的解决处理；

**7.网络运维服务**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 类别 | 位置 | 服务内容 |
| 7**.**1 | 网络监控 | 远程 | 7×24小时对网络设备（含网络安全设备）及网络整体的运行状态，各项硬件资源开销和容量，链路的健康状态等信息进行监控。 |
| 7**.**2 | 设备上下架 | 现场 | 根据变更请求，对网络硬件设备（含网络安全硬件设备）实施上架、系统初始化及下架等操作 |
| 7**.**3 | 设备巡检 | 现场 | 定期对网络设备（含网络安全设备）进行现场巡检，定期对设备进行清洁 |
| 7**.**4 | 故障排查 | 远程/现场 | 分析并处理网络设备（含网络安全设备）及网络链路发生的故障和终端设备断网故障 |
| 7**.**5 | 配置调整 | 远程/现场 | 根据变更请求，对网络设备（含网络安全设备）的配置（IP、VLAN、路由及端口等）进行调整，优化，版本升级 |
| 7**.**6 | 配置管理 | 远程/现场 | 对机柜位置、网络拓扑、VLAN、IP资源及网络设备的配置（含网络安全设备）进行管理 |
| 7**.**7 | WAN管理 | 远程/现场 | 协助客户、其他供应商进行专线、VPN的接入及配置；协助其他供应商进行网络测试、扩容 |
| 7**.**8 | 优化建议 | 远程 | 参与到数据中心网络建设项目中并对数据中心网络建设，网络安全和日常运维优化提出建议 |
| 7**.**9 | 线路调整 | 现场 | 机房内所有线路，若存在不规范的布线的，给出实施方案并完成规范化布线 |
| 7.10 | 防病毒管理 | 远程/现场 | 部署、配置终端操作系统防病毒，配置及检查防病毒更新情况 |
| 7.11 | 新增网络布线 | 现场 | （1）网络线路铺设具体要求：线缆需全程套管，明线部分需走线槽，使用医院铺设好的桥架走线，未铺设桥架部分走线需经信息部审核（2）标签制作：铺设的网络线缆，要求制作标签。标签按照医院现有的编号规则，使用标签打印机打印，标签要求整洁，清晰（3）网络测试：要求所有的线缆（八芯）都能够测试通过，传输速度能够达到1000M |
| 7.12 | 网络线路维修 | 现场 | 根据我院的要求对网络点位进行移点、找点和线路维修 |
| 7.13 | 系统升级 | 远程/现场 | 配置、检查设备系统补丁，根据系统安全进行系统及补丁升级管理 |
| 7.14 | 日志分析 | 远程/现场 | 定期对网络设备（含网络安全设备）的日志进行分析，发现安全问题及时上报及处理。 |
| 7.15 | 现场保障 | 现场 | 用户遇到重大检查时，派服务工程师到现场保障 |
| 7**.**16 | 其它要求 | 远程/现场 | 我院在后期会加入路由器、负载均衡、IDS、IPS，上网行为管理等设备，要求报名单位具备全设备调试，故障恢复能力 |

**8.维保服务内容**

（1）基础设施管理

* 确保用户信息系统网络通信传输畅通。
* 负责网络布线架的管理，确保配线的合理有序。
* 掌握用户端设备接入网络情况，以便发现问题可迅速定位。
* 采取技术措施，对网络内经常出现的用户需要变更位置和部门的情况进行管理。
* 掌握与外部的链接配置，监督网络通信状况，发现问题后与有关机构及时联系。
* 实时监控局域网络的运行和网络通信情况。

（2）操作系统管理

* 在网络操作系统配置完成并投入正常运行后，为了确保网络操作系统工作正常，首先利用系统提供的各种管理工具软件，实时监督系统的运转情况，及时发现故障征兆并进行处理。
* 在网络运行过程中，随时掌握系统配置情况及配置参数变更情况，对配置参数进行备份更新。随时做到系统环境变化、业务发展需要和用户需求，动态调整系统配置参数，优化系统。

（3）应用系统管理

* 确保各种网络应用服务运行的不间断性和工作性能的良好性。出现故障时应将造成的损失和影响控制在最小范围。
* 对于要求不可中断的关键型网络应用系统，除了在软件手段上要掌握，备份系统参数和定期备份系统、业务数据外，必要时在硬件手段上要建立和配置系统的热备份。

（4）局域网环境检查

* 测试网络连通性。
* 查看所有路由、交换机端口以及状态灯的工作状态，保证设备工作正常。
* 检查网关设备（防火墙、路由）工作状态，确保外网连接正常。
* 检查网络线缆，确保网络线缆完好无损。

（5）终端环境检查

* 检查终端计算机系统是否摆放整齐，检查机箱及显示器是否干净整洁。
* 检查终端计算机系统运行是否正常，磁盘空间是否满足工作需求。
* 检查安装的软件工作是否正常，保证网络环境没有病毒传播问题。一旦发现必须及时做有效性处理。
* 定期对客户机进行抽查，删除无用文件，对储存于工作无关文件的客户机进行删除清理。
* 对于计算机常用外置配件（键盘、鼠标、耳机）进行日常测试维护。
* 计算机的硬件维修、维护及更换。包括计算机无法启动、蓝屏、系统无法登陆等维护。

（6）其他内容

* 网络设备定期清洁、除尘。
* 网络设备标志标记修复。
* 重大检查时派服务工程师到现场保障。
* 网络的调试、网络故障的排除、网络设备的检修、布线系统的故障检修及故障排除等。

**9.产品清单**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **产品描述** | **产品数量** | **单位** |
| 9.1 | 核心数据交互平台(含2块核心防火墙板卡、4块48口千兆电口板卡、2块24口千兆光口板卡、2块无线控制器板卡、4块万兆引擎板卡、4个电源、4个风扇) | 2 | 套 |
| 9.2 | 24口接入数据交互平台 | 8 | 套 |
| 9.3 | 48口接入数据交互平台 | 13 | 套 |
| 9.4 | 出口安全网关 | 3 | 套 |
| 9.5 | 业务支撑系统 | 4 | 套 |
| 9.6 | 通信控制系统 | 2 | 套 |
| 9.8 | 视频会议系统 | 2 | 套 |
| 9.8 | 会议室多业务网关（带wifi功能） | 1 | 套 |
| 9.9 | 核心数据交互平台(含2块引擎、1块24口千兆电口板卡、2块24口千兆光口板卡) | 2 | 套 |
| 9.10 | 无线控制器 | 2 | 套 |
| 9.11 | 视频监控接入数据交互平台 | 1 | 套 |
| 9.12 | 核心数据交互平台(含2块引擎、1块24口千兆电口板卡、1块24口千兆光口板卡) | 1 | 套 |
| 9.13 | 核心数据交互平台(含2块引擎、1块24口千兆光口板卡) | 1 | 套 |
| 9.14 | 接入数据交互平台 | 29 | 套 |
| 9.15 | 网络线缆改造 | 1 | 套 |

# 三、技术要求

由于我院部分硬件设备比较陈旧，在网运行时间过长，性能低下，安全策略级别较低，基本依赖于医院的高速交换网络以及稳固的网络安全设备、安全策略提供高速数据转发和安全防御。网络以及网络安全是我院生产运行的主干枢纽和重要安全保障，因此报名单位须提供部分重要设备的备品备件，备品备件须满足下列技术要求：

**1.数据交换设备备品备件：**

1.1配置冗余引擎后，业务接口的插槽≥3。

1.2整机交换容量≥19 Tbps，包转发率≥2850 Mpps。

1.3支持将多台物理设备虚拟化为一台逻辑设备，虚拟组内可以实现一致的转发表项，统一的管理，跨物理设备的链路聚合。

1.4支持将一台物理交换机虚拟化成N台逻辑交换机，交换机间硬件独立且相互隔离。

 1.5支持将核心/汇聚和接入设备通过纵向虚拟化技术形成一台纵向逻辑虚拟设备，相当于把接入设备作为一块远程接口板加入核心设备，提供工信部测试报告复印件。

 1.6支持FCOE功能，支持TRILL功能，可实现存储网络和园区网络的融合，简化数据中心部署，提供工信部测试报告复印件。

 1.7支持SDN OPENFLOW，提供工信部测试报告复印件。

1.8支持EVB (Edge Virtual Bridging)，符合IEEE802.1qbg标准。可由硬件交换机提供虚拟机内部流量交换和流量监管；可感知虚拟机迁移并提供网络配置跟随。

 1.9支持CPU防护攻击能力，保障CPU工作安全，提供工信部测试报告复印件。

1.10可以配置EPON接口模块，作为OLT设备使用。

 1.11支持40G和100G扩展，单槽位最大支持24个40G端口，提供官网证明材料复印件。

1.12所配置设备需提供流量监测功能（含分析报表软件），以对网络中的通信量和资源使用情况进行分类和统计，并生成报表。投标所配置各业务板卡需配标准分析功能，即IP Fix（RFC 3917）或（RFC 3954）或（RFC 3176），不接受比选申请人采用私有协议的产品。

1.13支持AC板卡，POE，POE+，基于新一代园区网POE+供电需求（11ac）。

**2.安全网关备品备件：**

 2.1采用多核AMP+架构安全硬件架构，网络接口≥6个10/100/1000M自适应电口，标准2U机箱，≥1个扩展槽（非SFP或COMBO接口），支持液晶屏，网络处理能力≥10Gbps，并发连接数≥260万，新建连接速率≥18万/秒（提供面板截图证明材料复印件）。

2.2产品支持路由、透明、交换以及混合模式接入，满足复杂应用环境的接入需求，支持旁路模式。

2.3支持物理子接口技术，可以虚拟多个逻辑接口（不依靠vlan区分），命令行实现。

2.4 802.3ad方式支持3种负载算法：根据源目的mac组合、根据mac和ip组合、根据ip和TCP/UDP端口组合。

2.5支持IPv6地址配置，支持NAT64和DNS64，支持IPV6手动及自动的IP/MAC探测及绑定，支持IPV6下静态路由及策略路由，支持IPV6下的IPS、AV、URL、内容过滤、QoS及行为管控，支持IPv6安全策略。

 2.6支持会话限制功能，可以根据IP地址、安全域（入、出、双向）、应用设定限制策略，支持按源目的IP、源目的接口、用户、地理区域及应用进行流量排名，并显示流量统计（提供截图证明材料复印件）；

 2.7可以通过与入侵防护策略、防弱口令扫描、情报分析、终端防病毒系统的联动，生成动态策略信息，根据用户在基本配置中配置的动态策略动作，命中动态策略的数据将会被阻断或者记录日志要求支持IPv6内容过滤，包括：http过滤、FTP过滤、DNS过滤、邮件过滤（提供截图证明材料复印件）。