## 医院网络核心设备升级改造项目

## 项目需求分析

医院目前机房核心交换机设备（H3C 10512）于2014上线启用运行至今，已超使用年限。很难保证它提供的局域网链路的持续可用性，有可能导致整个网络中断，而网络中断则意味着整个医院信息系统的瘫痪。

## 业务现状分析

我院目前的整体网络现状如下：两个机房各有一台核心交换机10512，两台做互联；办公网环境中，楼层接入交换机都上行千兆连接到核心交换机的板卡上，楼层交换机分布在每个楼层的弱电间里，并未占用机房位置，下行到桌面端的应该大多在千兆；内网数据中心的服务器也分布在两个机房中，信息设备总数量在五十台左右，目前大多是千兆电口网卡，两个机房各有一台S5820交换机做服务器的接入，然后上连到核心交换机中；一些采用千兆光口和万兆光口网卡的服务器直接连到核心交换机上。

## 网络现状拓扑



本次计划将整网中核心交换机部分做一个整体替换，参数如下：

|  |  |
| --- | --- |
| **功能及技术指标** | **参数要求** |
| 产品品牌 | 国内知名品牌 |
| 性能指标 | 交换容量≥645Tbps，转发能力≥230000Mpps，以官网所列最低参数为准 |
| 板卡要求 | 主控引擎模块≥2，满足1+1冗余，主控槽位与交换网板槽位宽度相同的全宽槽位，提供更好的扩展性和可靠性，业务插槽数≥8，支持交换网模块≥6 |
| 电源冗余 | 电源模块N+M冗余 |
| 风扇框冗余 | 支持风扇冗余，风扇框数量≥2 |
| 关键部件热插拔 | 主控交换卡、电源、接口模块、风扇、网板等关键部件可热插拔 |
| 接口要求 | 支持高密 10GE、40GE 和 100GE 以太网端口,单槽位万兆端口密度≥48，单槽位40G端口密度≥36，单槽位100G端口密度≥18 |
| 链路聚合 | 支持设备链路聚合 |
| Mac | MAC表≥256K,学习速率≥120K/S |
| 路由表 | IPv4 FIB表项≥4M，IPv6 FIB表项≥2M |
| ARP | ARP表项≥256K  |
| 虚拟化 | 多虚一技术(N:1)，支持一虚多技术（1:N），支持多虚一技术和一虚多技术的配合使用,支持纵向虚拟化，支持远程端口扩展，作为控制设备实现对端口扩展模块的集中控制,支持有线无线的纵向虚拟化技术，实现有线无线设备的统一管理 |
| SDN/OPENFLOW | 支持OPENFLOW 交换机支持SDN平台管控，实现网络及SDN方案一体化部署，简化组网，简化运维 |
| 可视化 | 提供Telemetry流量可视化功能 |
| VxLAN | 支持VxLAN 网关支持EVPN,与非VXLAN网络互通支持VXLAN ARP广播抑制支持组播 over VXLAN支持Service Chain |
| 认证功能 | 支持802.1x认证，支持mac认证，支持Portal认证 |
| 配置要求 | 配置冗余电源，数量≥8，以太网交换机风扇模块≥2，满配主控板，配置交换网板≥3，配置≥36个40G以太网光接口，配置≥144个万兆以太网光口，配置40G模块数量≥16。 |

|  |  |
| --- | --- |
|  |  |

核心交换机

汇聚交换机

|  |  |
| --- | --- |
| **功能及技术要求** | **参数要求** |
| 基本性能 | 交换容量≥2.56Tbps，包转发率≥720Mpps，扩展插槽≥2，以官网所列最低参数为准 |
| 电源 | 模块化双电源 |
| 风扇 | 模块化双风扇，前/后通风，风道可调;  |
| 性能指标 | MAC地址表>=128K |
| 路由表容量>=64K |
| ARP：64K |
| ACL>=2K |
| 接口类型 | 端口形态：24个1G/10G SFP+端口，2个QSFP28端口，支持2个Slot |
| VxLAN | 支持VxLAN二层网关 |
| 支持VxLAN三层网关 |
| 支持EVPN |
| ERPS | 要求支持ERPS功能，并且收敛时间小于50ms |
| CPU保护 | 实现CPU保护功能，包括ARP报文攻击 |
| VLAN特性 | 支持基于端口的VLAN，支持基于协议的VLAN；支持基于MAC的VLAN； |
| 最大VLAN数(不是VLAN ID)>=4094 |
| 链路聚合 | 支持链路聚合基本功能及聚合零丢包 |
| 镜像功能 | 支持本地端口镜像和远程端口镜像、支持流镜像  |
| 访问控制策略 | 支持基于第二层、第三层和第四层的ACL； |
| 支持基于端口和VLAN的 ACL； |
| 支持IPv6 ACL； |
| 支持出方向ACL，以便于灵活实现数据包过滤； |
| 支持802.1x认证，支持集中式MAC地址认证； |
| Macsec | 支持802.1ae Macsec安全加密，实现MAC层安全加密，包括用户数据加密、数据帧完整性检查及数据源真实性校验。无需软件授权 |
| 管理 | 支持网管系统、支持WEB网管特性 |
| 实际配置 | 配置冗余风扇，冗余电源，堆叠线缆 |

服务器汇聚交换机参数如下：

| 功能及技术指标 | 详细技术参数 |
| --- | --- |
| 基本性能 | 交换容量≥4.8Tbps，包转发率≥2000Mpps，以官网所列最低参数为准 |
| 电源 | 模块化电源 |
| 风扇 | 模块化双风扇，前/后通风，风道可调;  |
| 性能指标 | MAC地址表>=128K |
| 路由表容量>=64K |
| ARP：64K |
| ACL>=2K |
| 接口类型 | 端口形态：48个1G/10G SFP+端口，6个QSFP28端口 |
| VxLAN | 支持VxLAN二层网关 |
| 支持VxLAN三层网关 |
| 支持EVPN |
| VLAN特性 | 支持基于端口的VLAN，支持基于协议的VLAN；支持基于MAC的VLAN； |
| 最大VLAN数(不是VLAN ID)>=4094 |
| 链路聚合 | 支持链路聚合基本功能及聚合零丢包 |
| 镜像功能 | 支持本地端口镜像和远程端口镜像、支持流镜像  |
| 访问控制策略 | 支持基于第二层、第三层和第四层的ACL； |
| 支持基于端口和VLAN的 ACL； |
| 支持IPv6 ACL； |
| 支持出方向ACL，以便于灵活实现数据包过滤； |
| 支持802.1x认证，支持集中式MAC地址认证； |
| Macsec | 支持802.1ae Macsec安全加密，实现MAC层安全加密，包括用户数据加密、数据帧完整性检查及数据源真实性校验。无需软件授权 |

## 项目改造目标

本次改造完成后可形成整网的核心网络层架构，核心采用双机冗余，院区所有网络区域均可通过核心层进行互联，两台核心交换机可以维持全院区网络转发。

整网骨干链路升级改造为40G链路，即所有汇聚节点上行40G到核心交换机，下行万兆到接入交换机，所有数据中心服务器通过万兆链路接入整网。

* 1. 兼容性：在有线网络设备选取上，选取在全国医疗行业成熟应用的设备，具备优秀的兼容性和高性能，在网络设计过程中采用国际标准协议兼容现有网络。
	2. 架构明晰：建立有效网络分区，隔离内外网设备，提升安全管控能力。遵从医疗行业相关规范，对网络分区进行合理规划设计，从网络分区的安全性、容量体系上进行设计，引入网络成熟新技术，提高自身的安全管控和技术支撑能力。同时进一步规范网络运维管理，提升网络服务水平。
	3. 高可靠：采用高可靠的产品和技术，充分考虑系统的应变能力、容错能力和纠错能力，确保整个网络基础设施运行稳定、可靠，例如整网采用双链路部署方式，减少单点故障带来的风险。
	4. 高安全：网络基础设计的安全性，涉及到业务的核心数据安全。按照端到端访问安全、网络L2-L7层安全两个维度对安全体系进行设计规划，从局部安全、全局安全到智能安全，将安全理念渗透到整个数据中心网络中。
	5. 先进性：本网络将长期支撑医院的业务发展，而网络又是信息化业务的基础支撑平台，因此本项目的建设需要考虑后续的机会成本，采用主流的、先进的技术和产品，保证基础支撑平台3~5年内不会被淘汰，从而实现投资的保护。
	6. 易扩展：未来我院的业务范围会更多更广，业务系统频繁调整与扩展再所难免，因此网络平台需适应业务系统的频繁调整，同时在性能上应至少能够满足未来3~5年的业务发展。对于网络设备的选择和协议的部署，遵循业界标准，保证良好的互通性和互操作性，支持业务的快速部署。

## 售后服务

提供设备的专业培训服务，保证设备的有效运行。

提供7×24 小时技术支持，包括远程支持和现场支持；当故障不能使用有效的远程支持方式进行解决时，提供派遣工程师赶往现场，进行现场故障诊断及现场故障排除，故障响应时间2个小时以内。

五年质保，每年至少两次上门巡检，对设备的运行状况进行回访、巡查，消除网络故障隐患，及时排除网络故障，以保障项目网络长期稳定运行。

建立了应急保障机制，提高对突发事件的组织指挥能力和应急处置能力，满足突发情况下，网络保障和网络恢复工作的需要。当该项目网络设施遭受异常破坏、异常流量或其他特殊故障情况下，使用应急保障流程恢复该项目重要的网络部件，确保该项目平稳运行。

重要时刻专人值守服务，医院认为可能对其业务运营产生重大影响的时刻，提供专人现场值守支持，保证重要时刻设备稳定运行。