小型医院网络建设

1. 设计目标
2. 设计需求
3. 用需求分析
4. 网络拓扑图
5. IP 地址规划
6. 核心层设计
7. 汇聚层设计
8. 接入层设计
9. 数据中心设计

10.互联网接入设计

11.冗余与负载均衡设计

12.路由设计

13.网络安全设计

14.网络管理与维护设计

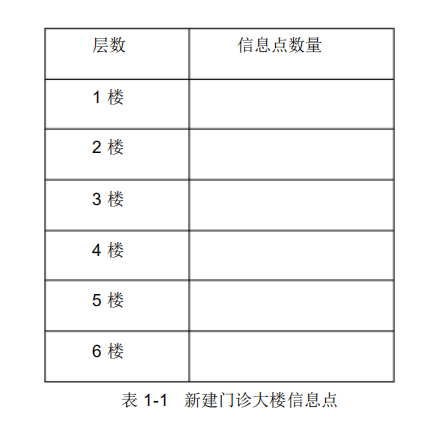
15.虚拟专用网 VPN

16.在网络中部署 QOS

1. 设计目标

本次院方新建了一栋6层的门诊大楼，使之达到如今医疗系统对网络的普遍要求，网络整体高速稳定的运行，易于管理且安全可靠、实现了海量数据的高速传输以及可扩展性等。

信息点分布



2.设计需求（1）各楼层直接与？楼的中心机房经过万兆膜光纤互联，要求实现万兆骨干，千兆到桌面的全网设计 ；

（2）网络核心 ，要求考虑采用双核心架构，万兆互联，充分考虑网络的稳定性与冗余，以及灾难恢复 。

（3）数据中心 ，位于门诊楼？楼，拥有各类型的服务器？台，要求配置一台专门的高端核心交换机 / 数据中心交换机，且双万兆链路与核心互联。

（4）网络出口设计需要考虑四条出口，一是社保局的VPN 出口，二是医保 VPN 出口，三是银行机构 VPN 出口 、四是干保 VPN 出口，且各条VPN出口均是独立的电信或者联通线路。出口设计要求安全、可控 。

3.用户需求分析

（1）网络系统稳定性需求：能够保证整个网络的稳定 、可靠 保证在单点故障的情况下不会对整个网络造成冲击，保证核心、骨干设备在出问题的时候能够无缝的恢复或切换 。

（2）网络传输性能需求： 能够通过有效的网络带宽控制技术和服务质量保证技术，来满足医院对于不同数据传输的需要。

（3）网络系统安全性需求：能够保证整个系统的保密性、完整性、可用性、可审核性。关键设备必须有备份系统且能够通过有效的手段控制和防御网络病毒的攻击。

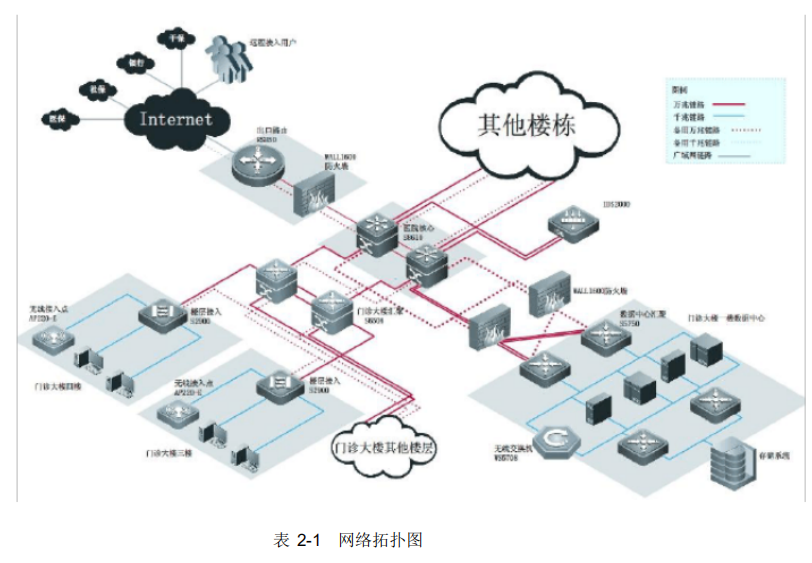
（4）网络系统管理维护需求：能够及时有效的发现网络中的异常流量，有效的控制网络设备，及时的对异常网络设备进行远程控制且操作简单、方便管理与维护。

（5）远程接入需求 ：能够为医院外部特殊用户提供安全保密的信息，实现高速安全的广域网数据传输。

1. 网络拓扑图

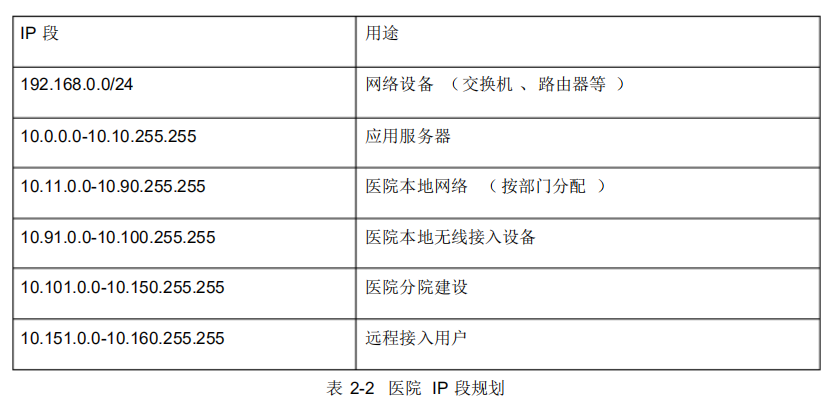
网络设计依照 “万兆核心、千兆支干、千兆交换桌面”的要求采用三层结构，重要部分双链路冗余 ，双设备冗余 ，核心层采用两台RG-S8610 系列交换机 ，门诊大楼汇聚层采用两台 RG-S6506 系列交换机 ，门诊大楼各层接入层采用RG-S2900 系列可堆叠交换机，在数据中心部分采用两台RG-S5750 系列交换机 ，除接入层到终端使用千兆以太网链路外，其他全部使用万兆光纤链路。除接入层到终端不进行冗余外， 其他部分均有冗余。汇聚层、核心层互联均使用双万兆光纤聚合，数据中心到核心层链路也使用双万兆光纤聚合，整个网络使用锐捷SAM 进行身份认证，Star-View 进行网络设备管理。核心层旁部署

RG-IDS2000 用于审计整个网络，为各种事件提供证据。其数据也作为当前网络运行状况与后续网络扩充的参考

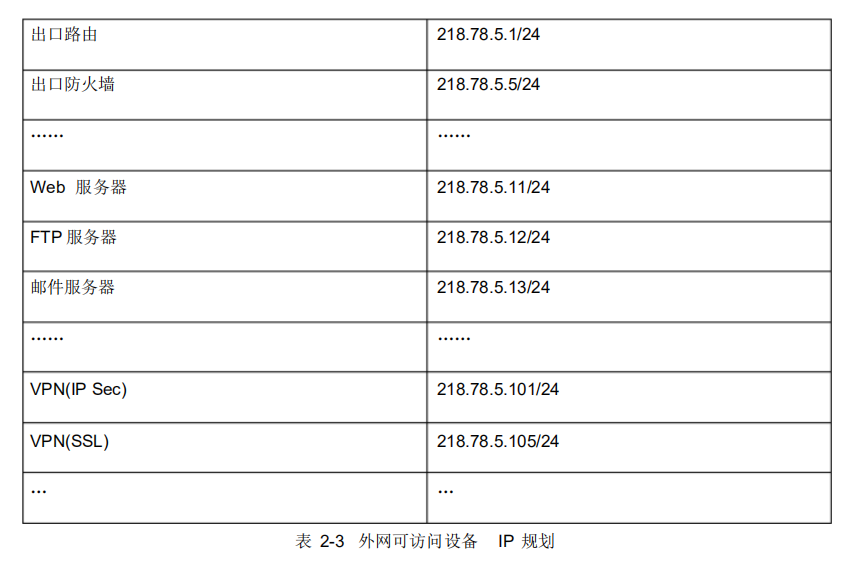


5.IP 地址规划

在网络 IP 规划中，网络设备 （交换机 、路由器等 ）使用 192.168.0.0/24 这个地址块，医 院 使 用 整 个10.0.0.0/8私有地址块 ，应 用 服 务 器 ，验 证 和 管 理 系 统 使 用10.0.0.0-10.10.255.255 这个网络块，IP 地址池10.11.0.0-10.90.255.255 均用于本地网络，按部门分配使用，多余部分保留，IP 地址池10.91.0.0-10.100.255.255用于无线网络 ，对于可能的分院建设 ，预留 10.101.0.0-10.150.255.255用于分院的IP，分院IP 和总院IP 统一编址，可实现通过 VPN 的站点到站点完全互访，即分院与总院在逻辑上就是一个大的整体网络。对于远程接入用户 ，使用 10.151.0.0-10.160.255.255网段。总体如下表所示 ：



在汇聚层交换机上建立IP 池，开启 DHCP Server，根据终IP。对于需要静态 IP 的设备 ，由管理员根据 IP 规划表手动配置。对于数据中心中需要被外部访问的设备的IP 划分 ，需要被其他系统访问的设备均使用唯一的外网 IP，在出口处不添加这些IP 的路由 ，这样外网无法访问到这些设备，对于 VPN连接进入的用户和站点到站点的VPN 额外添加路由，使这些设备能被访问。医院拥有218.78.5.0/24 这个外网IP块。按如下表单分配IP 地址。



6.核心层设计

大型医院网络的核心网主要完成整个医院内部不同部门之间的高速数据路由转发，以及维护全网路由的计算。鉴于大型医院的用户数量众多，业务复杂 ，QOS 要求较高 、以及的这些特点。本方案中核心部分采用两台RG-S8610 交换机 ，通过两条万兆光纤互联， 与楼栋汇聚层 、数据中心 、 出口 、IDS 均采用万兆光纤互联且有冗余链路 ， 保证了网络的高速与稳定。IDS 采用RG-IDS2000S ，RG-IDS2000S 以旁路的方式在网络中部署，实时监测网络运

行状况与网络安全。

1. 汇聚层设计

汇聚层网络主要完成医院内各部门内接入交换机的汇聚及数据交换和VLAN 终结以及实施与安全 、流量负载和路由相关的策略，在本方案中汇聚层采用两台

RG-S6506 交换机 ，各楼层接入层交换机都通过万兆光纤分别与这两台交换机相

，实现冗余 。汇聚层交换机同时与核心层两台交换机万兆光纤互联。实现高速。

1. 接入层设计

接入层网络主要完成为局域网接入广域网或者终端用户访问网络提供接入

，在本方案中采用 RG-S2900 交换机。根据不同楼层可能的信息点增加情况

，按该楼层整体接入点的10%-30% 进行接口预留 ，用于扩充 ，若进行更大规模的信息点增加，则需购置新的模块或设备。接入层交换机同时与一楼两台汇聚层交换机通过万兆光纤相连。实现高速、稳定。

9.数据中心设计

门诊大楼数据中心汇聚在RG-S5750 ，外连 RG-WALL1600 后到网络核心层 ，数据中心流量较大 ，因此通过双万兆链路与核心层相连，且有冗余链路 。使用了两台WALL1600 防火墙保证数据中心的高安全数据中心有各种应用服务器， SAM 身份认证系统，START-VIEW 设备管理系统，RG-WS5708 无线控制器，同时有一套存储系统。

10.互联网接入设计出口处使用了RSR50 路由器与 RG-WALL1600 防火墙 。出口处仅使用了一个防火墙，若万一设备故障 ， 此级防火墙防护失效，但数据中心防护仍在，网络数据中心的安全性不会降低 ，且网络有其他安全策略， 仍旧保证了整个网络有足够的安全性。楼123456数量出口做策略路由，出口网通流量走网通线路，其他出口流量走电信线路，配置到10.0.0.0/8 、 到医院应用服务器IP 的路由，在出口处路由处配置NAT，将源地址为10.0.0.0/8 的包映射到外网。

11.冗余与负载均衡设计

冗余设计是网络设计的重要部分，是保证网络整体可靠性能的重要手段。在此方案中，采用 GEC链路聚合 （IEEE802.3ad ）实现端口级冗余 ，以克服某个端口或线路引起的故障。也可采用生成树协议（IEEE802.1d ）提供设备级的冗余连接。 在网络的每个关键结点，我们在设计时都做到了对其有效的冗余备份和负载均衡。在网络的核心层上。我们采用了一台锐捷网络的 RG-S8610 高密度多业务 IPV6 核心路由交换机和RG-S8610 核心交换机组建高性能的核心网络平台，在对骨干核心层提供足够的网络接点和接入需求的同时最大限度

的为网络提供了有效的冗余保障和负载均衡。 在核心层的区块 ，我们采用的两台锐捷网络的核心多业务IPV6 核心路由交换机做到冗余与负载均衡。在汇聚层的每个区块，我们采用了两台锐捷网络的RG-S6506 交换机多层交换机做到冗余与负载均衡。

12.路由设计

网络不需要运行动态路由协议。在核心层添加各个楼栋VLAN ，无线接入用户 VLAN到数据中心 VLAN 相互之间的路由 ，添加到出口设备的默认路由。添加出口路由到需要被外网访问的服务器的路由，添加 VPN 接入用户到应用服务器群的路由。

13.网络安全设计

（1）网络整体安全性 ：内网出口处有防火墙，选用锐捷 RG-WALL1600E 防火墙 ，可为内Word 格式完美整理网的整体防护提供安全措施。数据中心也设置了防火墙，让数据中心始终拥有很高的安全性。

（2）防范 ARP 攻击 ：网内除终端设备外 ，所有设备的 ARP 表有可信的第三方发布（位于数据中心的安全设备）， 该 ARP 表绑定所有重要设备MAC 与 IP。

（3）控制网络病毒 ：在汇聚 、核心交换设备设置由硬件实现ACL，对病毒进行过滤，我们选用的汇聚 、核心交换设备都支持SPOH（同步式硬件处理 ），所以在使用 ACL 时将不会影响整个交换机的性能。SPOH（synchronization process over hardware）即"同步式硬件处理"，通过最新的硬件芯片技术，让交换机每个端口都具备独立的数据处理能力，实现了端口级的数据同步交换，达到在高效应用Q0S 和 ACL 功能同时，交换机仍然保持海量数据的全线速转发，有效解决了网络的拥堵和安全问题。

（4）DHCP：开启接入层交换机的DHCP Snooping 功能 ，仅汇聚层交换机的

DHCP 通过，其他 DHCP 包会被过滤掉。

（5）抵御网络攻击 ：结合网络攻击的检测系统，能够抵御日益增多的内部网络攻击，并且自动对用户做出相应的控制动作，保证网络安全 。

（6）安全认证 ：采用六元素的自动绑定、 静态绑定 、动态绑定相结合 ， 可以确保用户入网时身份唯一 ，并且避免了 IP 冲突 。除不需身份认证的设备外

，其他设备入网均需一次身份认证 ，根据认证结果发放权限，同时某些重要应用服务器可能还需要进一步的身份认证。

（7）IDS：入侵检测系统以旁路的方式在网络中部署，并且实时检测数据包并从中发现攻击行为或可疑行为 。在此选用锐捷 RG-IDS2000S ，RG-IDS 在网络中能够阻止来自外部或内部的蠕虫 、病毒和攻击带来的安全威胁，确保企业信息资产的安全，能够检测因为各种IM即时通讯软高效 、 全面的事件统计分析，能迅速定位网络故障，提高网络稳定运行时件、P2P 下载等网络资源滥用行为，保证重要业务的正常运转。

14.网络管理与维护设计

为了帮助网管人员轻松实现对众多网络设备的管理、及时排查网络故障和提高用户管Word 格式完美整理理的效率 ，采用锐捷网络基于RIIL平台的 “业务运行健康管理中心”（RG-RIIL-BMC ）实现对网络和业务应用系统的集中智能管理

，可以让有限的 IT 运维人员精力和IT 预算投入到最关键的资源的维护和保障中，切实降低复杂IT 环境的管理难度 ，更轻松地把握支撑关键业务的网络和系统的运行状态，并不断提升关键业务系统的运行服务质量水平，提升用户满意度。 系统能对每个客户上下行的带宽上限加以限定，防止个别客户占用过多网络资源。 还能对不同的用户数据设定业务优先级， 以保证重要数据能得到更好的服务。

锐捷网络交换机都经过独特设计具备防尘、防潮 、防静电等多种适于在楼道安装和使用的特点 。而且具有强大的运行维护能力，能有效降低运营商的运维成本。支持 RS-232 本地管理口及 Telnet 、 WEB、SNMP 代理 ，远程监控 （RMON 1~3 ，9 组 ）可根据运营商的不同要求 ，使用不同的管理方案， 支持 SNMP 协议的全网集中网管。交换机能够提供全中文菜单或图形配置方式，为交换机的管理和配置提供了极大的便利。提供了故障告警和日志功能 ，可通过机箱面板上指示灯直观地了解设备的运行状态。

1. 虚拟专用网 VPN

根据需求 ，总共需要有医院到社保局、医保 、银行机构 、干保四条站点到站点VPN 隧道， 以及远程接入用户 。对于站点到站点VPN,采用 IPSEC，编址部分参考 IP 编址一节 。对于远程接入用户，采用 SSL VPN，编址部分参考 IP 编址一节 。在出口路由器和出口防火墙上同时开启VPN 功能，优先使用防火墙上

VPN 功能 。VPN 接入用户和远程站点仅能访问医院数据中心。在逻辑上所有 VPN 远程访问都相当于是医院的某个部门。对于一些特殊的医学资源，例如 ：患者的病历信息 ，医药学文献 ，医院内部的行政信息等等，这些信息在需要被医院以外的特殊用户访问的同时，其安全性和保密性要得到最高的保证。这可以通过 VPN 的角色进行划分 ，划分不用的 VPN 接入后的权限。

16.在网络中部署 QOS

QoS 的英文全称为 "Quality of Service" ，中文名为 " 服务质量 "。QoS 是网络的一种安全机制 , 是用来解决网络延迟和阻塞等问题的一种技术。在正常情况下 ，如果网络只用于特定的无时间限制的应用系统，并不需要 QoS， 比如 Web应用 ，或 E-mail 设置等 。 但是对关键应用和多媒体应用就十分必要

。当网络过载或拥塞时，QoS 能确保重要业务量不受延迟或丢弃，同时保证网络的高效运行。