9 网络基础架构

9.1 区域卫生信息网络体系架构

9.1.1 区域卫生信息网络体系架构概述

基于健康档案的区域卫生信息平台的核心业务是以区域内健康档案信息的采集、存储为基础，能够自动产生、分发、推送工作任务清单，为区域内各类卫生机构开展医疗卫生服务活动提供支撑的卫生信息平台。平台主要以服务居民为中心，兼顾卫生管理和辅助决策的需要。

下图重点描述不同类型的 POS 与信息平台数据交互的业务数据流向。

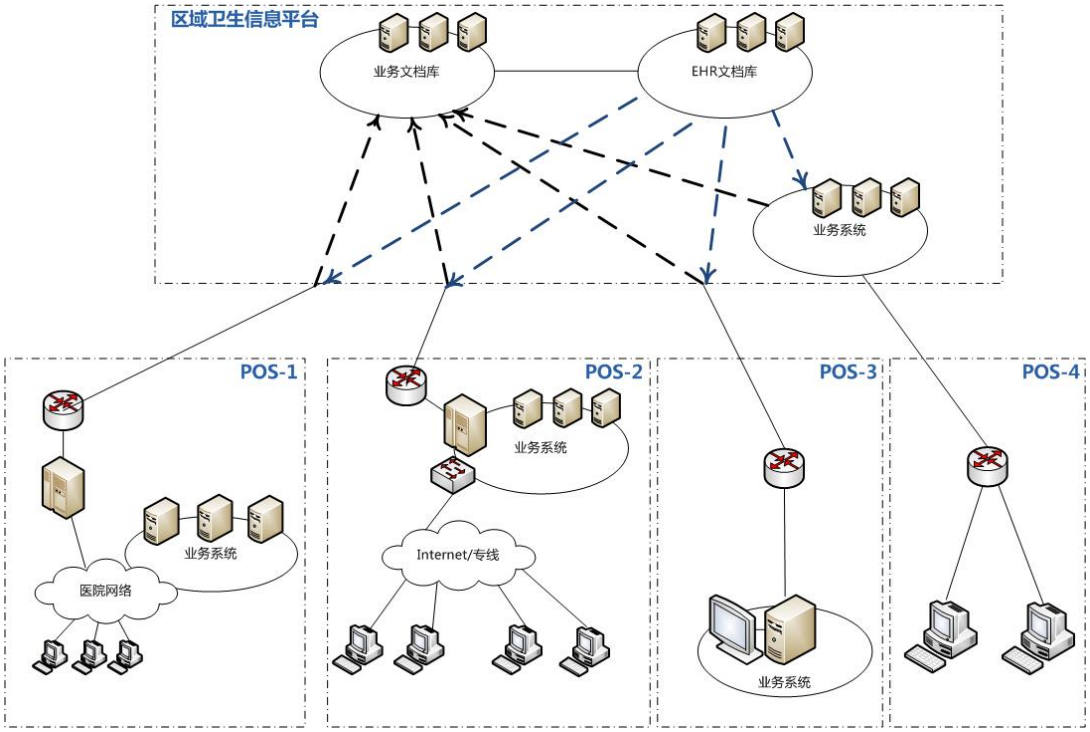


图 9-1 不同类型 POS 与信息平台数据交互业务数据流向示例图

1）信息平台

信息平台应用服务主要包括三个部分：业务文档库、EHR 文档库、业务集成平

台。

业务文档库：POS 的医疗服务产生的需要提交到信息平台的数据统称为业务文档，所有 POS 将业务文档提交并保存至业务文档库

EHR 文档库：业务文档库将收到的文档进行解析/组装（parser/rebuilder），转换成标准的 EHR 文档格式，然后转存到 EHR 文档库中。

业务集成平台：业务集成平台在域中会有多个，例如传染病管理、慢性病管理、计划生育和孕产妇管理、儿童保健等等，由业务集成平台产生业务文档提交给信息平台中的业务文档库。

2）POS 介绍：

- POS－1：该 POS 内部已有完善的业务系统，终端主机日常访问本 POS 内的业务系统。如：大、中型医院、妇幼保健等。
- POS-2：该 POS 内主机为单纯的 Portal，所有业务应用都依赖于远程的一个集中式的业务平台的支持，该业务平台位于上一级的管理机构，Client 端既没有应用程序，也没有存储。如：社区卫生服务站、社区卫生服务中心。
- POS-3：该 POS 内工作站端实际上是一个包含业务应用程序和存储的完整系统。如：社区卫生服务站、卫生室等。
- POS-4:该 POS 与 POS-2 相同,区别在于 POS-4 的业务系统在信息平台内部。POS 直接接入信息平台即可。

3）POS 业务文档的提交

- POS-1: 在 POS 的出口有一个文档重构的引擎/适配器（Engine/Adaptor），将 POS 内部医疗服务产生的医疗数据转换成标准的业务文档格式，提交到信息平台。
- POS-2:POS 自身无存储、无应用服务，POS 内工作站将业务数据提交给业务平台，在业务平台通过文档重构的引擎/适配器（Engine/Adaptor），将 EHR 有用的数据转换成标准的业务文档格式，提交到信息平台。
- POS-3:POS 终端设备自身包含的业务应用程序，同时安装文档重构的引擎/适配器（Engine/Adaptor），本终端即可产生业务文档，直接提交给信息平台进入业务文档库。
- POS-4：与 POS-2 相同，区别在于 POS-4 的终端直接将数据提交给信息平

台，由信息平台的业务系统进行文档的重构，提交给业务文档库。

总之，无论哪一类应用，提交给平台的文档格式（CDA）与流程（IHE）都是一样的，都是通过业务平台和 EHR 平台打交道，不同的只是内容

4）数据存储及调用

EHR 数据的存储方式主要有三种：集中式、分布式、混合（联邦）式。针对不同类型的数据可以采用不同的存储方式。但是在逻辑上当 POS 进行 EHR 数据调用时，首先是向信息平台提交调用请求，由 EHR 根据文档主索引确定文档位置，再由 POS 从指定位置调用。该文档位置可以是在信息平台本地，也可以是分布在不同的其他平台。只需保障 POS 与其能够互通即可。

5）本区域其他信息系统平台调用健康档案信息

对于区域内已建的其他信息系统平台（如疾病预防控制、卫生监督等）如需调用居民健康档案数据用于支撑其业务系统时，与 POS 点的信息调用方式一致，由信息平台提供开放接口，直接在 EHR 文档库中提取数据。

总结：通过上述分析，从逻辑上说，基于健康档案的区域卫生信息平台的核心业务模式为集中式，所有 POS 不论是信息的提交还是信息的获取均直接与 EHR 信息平台进行交互。在整体网络体系架构设计时充分考虑信息平台业务及数据流特征，使网络架构充分与业务体系架构相切合。**因此区域卫生信息网络体系架构逻辑采用以信息平台为核心的星型二层结构。**

9.1.2 设计原则

9.1.2.1 标准化原则

标准化是区域卫生信息平台网络建设的基础保障，应用服务系统建设必须在业务流程化、安全体系和安全技术、信息表示和信息交换、网络协议、软件结构、软件平台等标准方面遵循统一技术标准，才能达到“互联、互通”要求，实现“信息交换、资源共享”。

9.1.2.2 可靠性原则

区域卫生信息平台网络建设时必须重点考虑业务系统能否有效的避免单点失败，在设备选择和互联时应提供充分的冗余备份，实现业务系统的 7×24 小时不间断工作。

9.1.2.3 模块化设计原则

区域卫生信息平台网络建设时采用模块化、分区化设计，将整体网络基础设施平台划分为若干个区块，便于安全隔离和扩展。

9.1.2.4 安全保密性原则

区域卫生信息平台承载着区域内居民健康档案信息，涉及居民的个人隐私。因此在网络架构设计时充分保障数据在提交、传输、存储、调用时的数据安全。

9.1.2.5 高性能原则

随着区域卫生信息平台业务的不断完善、增加，远程协同医疗、健康档案中的 PACS 影像等系统和资源将对网络性能提出更高的要求。因此区域卫生信息平台整体网络架架构应具备高速转发性能，保证各项业务的顺利开展。

9.1.2.6 可管理性原则

区域卫生信息平台的网络设备必须支持标准的 SNMP 协议，使其易于管理、维护，操作简单，便于配置，在安全性、数据流量、性能等方面能得到很好的监视和控制，可以进行远程管理和故障诊断。

9.1.2.7 可扩展性原则

区域卫生信息平台的网络设备不但满足当前需要，也要考虑将来业务系统的业务量增加、以及更多的业务系统融入信息平台时能够提供有利保障。对于现有架构及设备应该尽可能通过扩展已有的功能或模块来实现，而无需更换已有资源。

9.1.2.8 技术成熟性原则

在网络建设方面，充分考虑采用国内通用的，成熟的软硬件产品，保证信息平台业务运行的高效稳定。

9.1.3 网络分层、分区设计

9.1.3.1 网络分层概述

基于健康档案的区域卫生信息平台业务模式为扁平化特点，所有 POS 点直接与信息平台的业务系统进行交互。进行网络架构设计时充分考虑此特点，设计信息平台主要由两大部分组成，POS 远程接入和信息平台。POS 远程接入主要负责各 POS 点的接入，实现业务数据的提交和健康档案资源的调用；信息平台主要负责各

POS 点的汇聚，业务系统的运行、管理、EHR 信息的存储、调用，以及信息平台的外联。

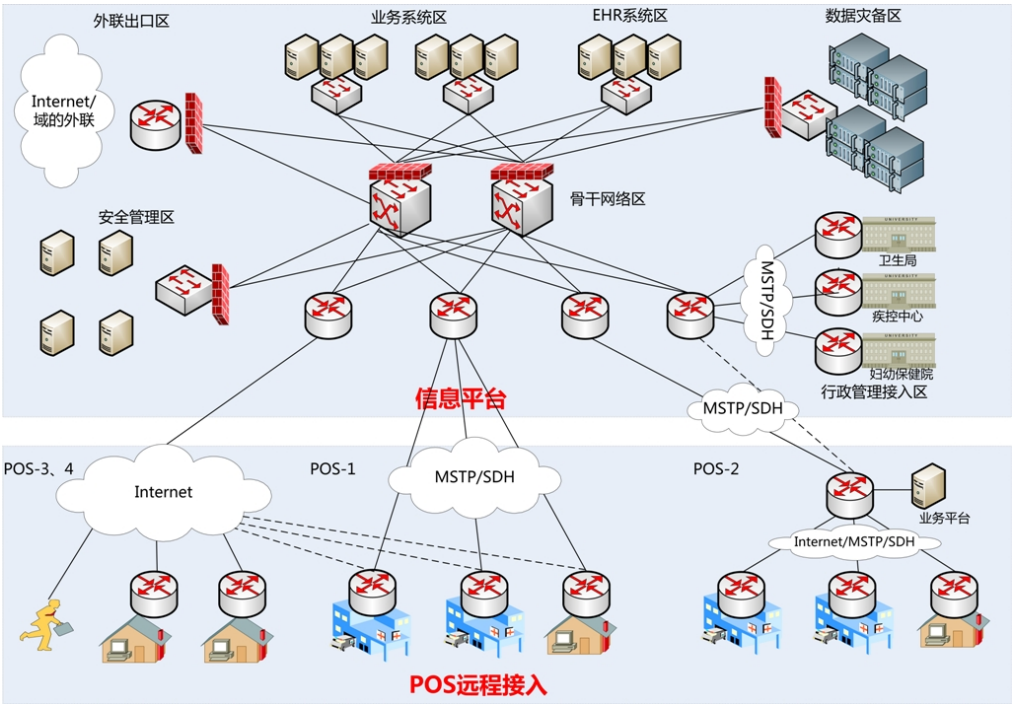


图 9-2 整体网络架构设计

进行整体网络架构设计时充分考虑此特点，将网络架构分为二层：POS 远程接入、数据中心。同时根据各自其特点进行进一步细化。

9.1.3.2 网络分区概述

网络基础设施平台根据其功能特点逻辑上划分 9 大模块：POS-3/4 接入区、POS-2 接入、POS-1 接入区、骨干网络区、业务系统区、安全管理区、数据灾备区、外联出口区、行政管理接入区。数据中心的各模块区域间通过防火墙进行安全隔离。

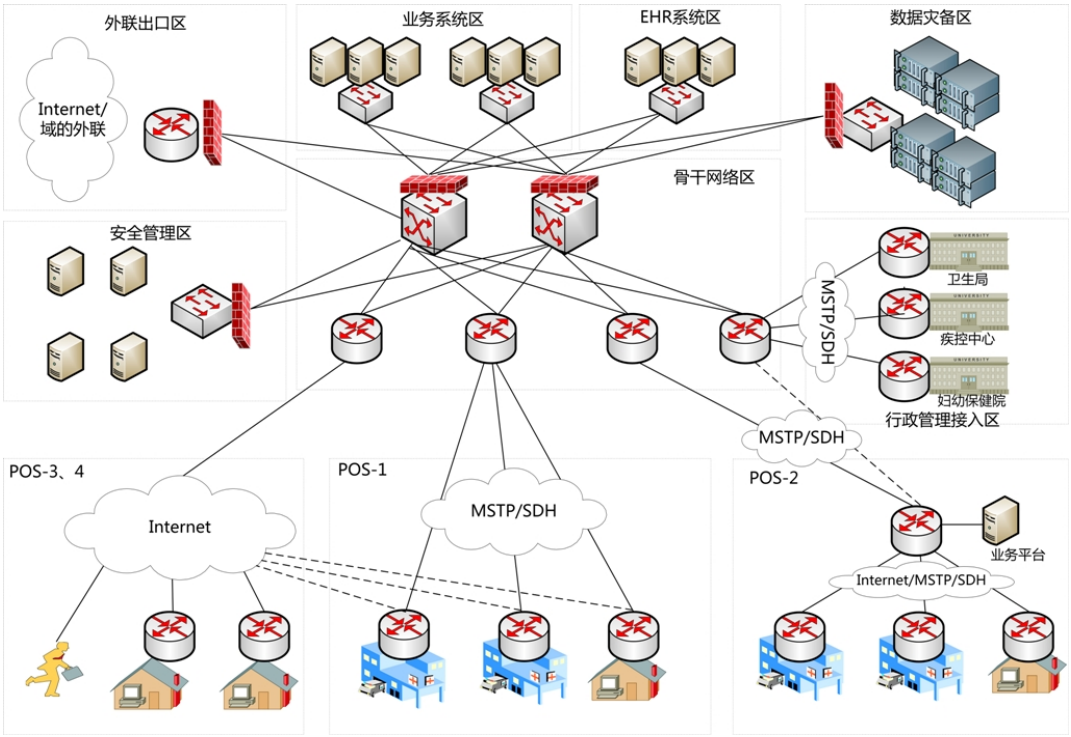


图 9-3 POS 网络分区

1). POS-1 接入区：

该 POS 大多为医院、大型社区卫生服务中心等机构，根据业务需求，建议采用专线方式连入信息平台。

2). POS-2 接入区

主要是指以市为单位建区域卫生信息平台，区县级以下的医疗机构如乡镇卫生院、区/县级医院等单位业务数据量大无法通过 Internet 方式满足，因此采用在区/县卫生局设立汇聚点，POS 通过 MSTP/SDH(Multi-Service Transfer Platform/Synchronous Digital Hierarchy)专线直接连入县卫生局汇聚点，县卫生局汇聚点再通过 2 条专线链路上连至市数据中心。

3). POS3-4 接入区：

主要针对小型 POS 点、离信息平台较远的 POS 点，以及信息平台管理人员外出办公，采用通过 Internet 方式远程拨 VPN 访问信息平台业务系统。

4). 骨干网络区

主要负责各 POS 的远程链路汇聚，以及数据中心各其他模块的连接、实现数据的高速转发处理。远程链路汇聚主要采用高性能的路由器、VPN 网关服务器，业务系统、安全管理等模块主要通过万兆平台的三层交换机进行连接。

5）. 业务系统区

区域卫生信息平台内所有的应用服务器、数据库服务器、中间件服务器、数据存储设备等一切业务系统相关的设备的集中连接区域。

6）. 安全管理区

数据中心内保障整体信息平台安全、稳定运行的安全管理运维系统的连接区域。如证书服务器、身份认证、漏洞扫描、入侵检测、网络管理等。

7）. 数据灾备区

业务系统及健康档案数据的灾备区域，一般该区域为远程灾备区域，通过高速链路直接与核心交换机相连，实现业务系统与灾备区域数据的同步。

8）. 外联出口区

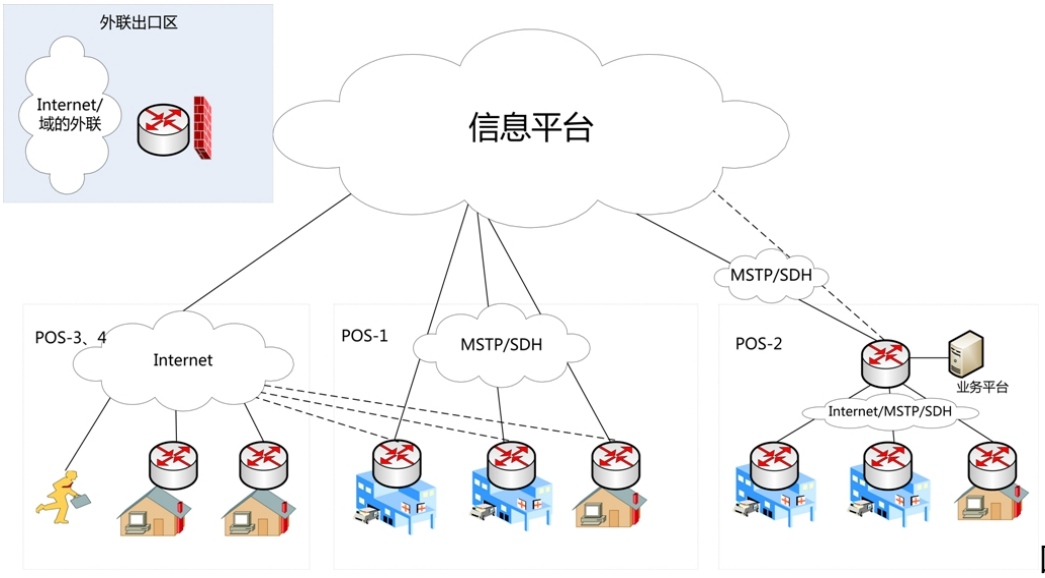
该区域主要负责连接外联单位，如民政局、社保中心、公安局等。以及将来实现域间互连互通时提供开放接口。使其不影响域内业务系统的正常运行。

9）. 行政管理接入区

该区域主机负责将区域卫生信息平台的行政管理部门接入数据中心，使居民健康档案得以更加充分利用，从而进一步实现基于健康档案的疾病预防控制、慢病跟踪治医疗、妇幼保健等业务。

9.1.3.3 POS接入层

负责所有 POS 接入数据中心，实现对业务系统的访问。根据 POS 点的不同类型、业务需求特点分别采用不同的接入方式。



图

图 9-4 POS 接入方式

根据 POS 点的规模及特点，划分为三种类别：

1)．POS-1 点

此类主要是指：市级二甲以上医院、市区内社区卫生服务中心。其特点为病人流量大、医院规模大、地理位置距离数据中心较近。此类 POS 点采用 MSTP/SDH 等专线方式直接连入数据中心，实现业务系统的高速访问，同时为保障业务的稳定开展，有条件的 POS 点采用 ADSL/3G 等方式做为备用链路通过 Internet 连入数据中心。当主要链路故障时，能够自动切换到备用链路，确保业务的 7*24 小时不中断。

2)．POS-2 点

此类 POS 主要是指：区或县级所属的大中型医疗机构。如县医院、大型乡镇卫生院、偏远社区卫生服务中心等。其特点为病人流量大、医院规模大、地理位置距离数据中心较远。此类 POS 点需采用高带宽的专线方式接入。但于由距离较远，所有 POS 点直接连入数据中心将大大提高链路成本。因此在区或县级卫生局设置汇聚点。所有 POS 点直接专线接入汇聚点，汇聚点设备再通过 2 条专线链路连入数据中心。

3)．POS-3/4 点

此类主要包括：个人、小型乡镇卫生院、社区卫生服务站。其特点为病人流量少、医院规模小、地理位置距离数据中心远。此类 POS 点采用 ADSL、3G、PSTN 等方式连入 Internet，再通过 VPN 方式安全访问数据中心的业务系统。

9.1.3.4 骨干层网络

网络基础设施平台的硬件系统一般包括：数据库服务器、备份服务器、应用服务器等；交换机、路由器、防火墙、VPN 等网络设备；存储设备如磁盘阵列、磁带库等。网络基础设施平台的硬件系统配置，应根据当地实际业务需求、网络覆盖范围和规模以及经济条件，本着经济、实用、高效和分步实施的原则，选择适当的建设方案。

9.1.3.5 域的外联及域间互联

本方案重点描述的是一个域（Domain）内基于健康档案的区域卫生信息平台的建设。同时考虑到域与域之间的互联互通，以及域与其他相关部门的互联互通。

在域内信息平台网络架构设计时，专门划分的外联出口区域模块。该区域通过一台路由器和一台防火墙直接与数据中心的核心交换机相连，在确保数据高速传输的基础上，保障数据传输的安全。同时通过模块化的划分确保域内信息平台业务的稳定运行，使其不受外部干扰。

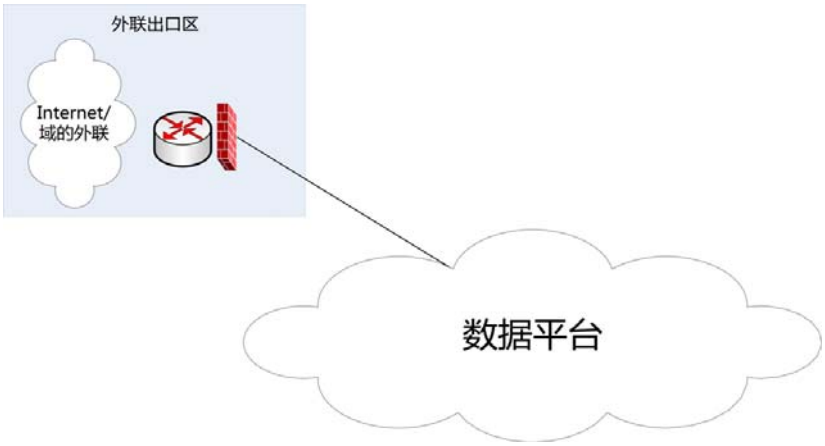


图 9-5 域的外联及域间互联示意图

9.1.4 网络带宽设计

9.1.4.1 社区卫生服务站信息处理量分析

本小节所计算的带宽需求数据均未将 PACS 信息传输列入计算范围，在实际平台建设过程中如需进行 PACS 信息的传输，请在此基础上根据实际情况增大带宽。

本小节所计算的性能参数相对较小，在实际带宽及设备性能确定是需要根据实际情况进行调整，以适应后续的业务扩展和应用需求。

1). 基本数据信息

根据 2008 年中国主要人口数据表明：儿童占比为 19%，成年人占比为 69%，老年人占比为 12%。女性育龄人口占总人口数的 28%，其中女性的孕产妇女占女性育龄人口的 25%，普通育龄妇女占 75%。

根据 2008 年我国卫生机构统计数据:我国共 2.4 万个社区卫生服务站(中心)，按照全国 13 亿人口计算，平均 54167 人配比一个社区卫生服务站（中心）。

表 9-1 社区人均服务需求数据量

特殊人群分类	一年内平均每人接受保健或随访服务次数	每次服务产生的数据量（KB）

儿童	2.7	5
孕产妇女	5	6
普通育龄妇女	1	7
老年人	1	2
慢病患者	2	2
其他人群	0.5	3

根据 2008 年我国卫生机构统计数据：我国卫生院诊疗人数为 8.62 亿人次，住院人次为 3355 万。

2). 计算参数定义

Pa 代表该 POS 范围内总人口数

Xa 表示 XDS、CDA 文档格式占比原始表数据量的系数：暂定 470%

Xb 表示业务数据在网络中传输的协议开销占比系数：暂定 20%

Xc 表示网络带宽冗余占比系统：暂定为 20%

Ca 表示社区卫生服务机构单位时间的并发连接数（即单位时间有几台主机需与信息平台交互数据）

注：数据存储的快照、数据容灾所占空间参数未列在内。

3). 业务数据量计算

社区卫生服务站接入带宽计算

- 通过上节业务流量分析得知，社区卫生服务机构每人最大数据　量为 7KB（普通孕龄妇女）
- 社区卫生服务机构的卫生服务数据需要实时上传至业务平台
- 网络传输数据量（ND）＝7KB*(1+Xa)*(1+Xb+Xc)×8＝446.9Kb
- 社区卫生服务机构的接入带宽＝ND×Ca
- 注：此带宽需求为最大负荷的带宽需求，各社区卫生服务机构可根据实际应用情况灵活调整。

范例：

某社区卫生服务站共有 3 台终端设备与区域卫生信息平台连接，为实现 3 台设备同时工作且快速提交患者相关的健康档案信息，所需的接入带宽＝ND×Ca=446.9Kb×3＝1340kbps。考虑到实际运营商的链路服务及实际业务开展情况，

该社区采用 1M 的 ADSL 接入区域卫生信息平台。

某社区卫生服务中心共有 20 台终端设备与区域卫生信息平台连接，某社区卫生服务站共有 3 台终端设备与区域卫生信息平台连接，为实现 3 台设备同时工作且快速提交患者相关的健康档案信息，所需的接入带宽＝ND×Ca=446.9Kb×20＝8938kbps。考虑到 20 台终端并非全部并发连接，按照 30%的并发比例计算，接入带宽需求为 8938kbps*30%=2681kbps，因此该社区建议采用 2M 的 ADSL 或专线接入接入区域卫生信息平台。

9.1.4.2 医院业务数据流量分析

1). 基本数据信息

表 9-2 全国医院诊疗工作量（2008 年）

服务分类	医院	人均诊疗次数
诊疗人次（亿）	17.82	1.37
住院人次（万）	7392	0.056

表 9-3 典型医院业务数据量（包括医嘱，不包括影像和检查报告）

医院核心医疗业务	每病人数据量（KB）
门诊	2
住院	11
检验	4

2). 计算参数定义

Ha 表示 XDS、CDA 文档格式占比原始表数据量的系数：暂定 470%

Hb 表示医院医生工作站数量

Hc 表示医院工作站并发访问比例：暂定 20%

注：数据存储的快照、数据容灾所占空间参数未列在内

3). 业务数据量计算

以下基于区域卫生信息平台完全建立起来，并且所有医生诊断时都进行 EHRS 申请调用的情况下进行估算。医院类 POS 的接入带宽合理计算：

①对于医院与信息平台的数据交互特点为，实时下载病人健康档案信息，周期性上传新记录的病人就诊信息（如一天一次）

②根据上节针对医院的业务流量分析得知，以最大数据量传输带宽为原则，单

位时间内下载查看的病人信息量最大的是病人住院信息记录（11KB）

③医院单位时间内下载带宽需求＝最大业务带宽需求 HD=11（KB）*（1+ Ha）* Hb*Hc*8

范例：

某二甲医院与区域卫生信息平台互通，该院当前医生工作站 40 台。该院调用居民健康档案所需的接入带宽为 HD=11(KB)*(1+470%)*40*20%*8=4013Kbps，由此可知该医院访问居民健康档案所需的接入带宽为 4Mbps

某三甲医院与区域卫生信息平台互通，该院当前医生工作站 200 台。该院调用居民健康档案所需的接入带宽为 HD=11(KB)*(1+470%)*200*20%*8=20,064Kbps，由此可知该医院访问居民健康档案所需的接入带宽为 20Mbps 以上的专线。

9.1.4.3 广域网链路汇聚带宽设计

根据三类不同 POS 接入类型其汇聚带宽设计分别为：

1).远程小型 POS 点

远程小型 POS 点采用 ADSL/3G 等方式通过 Internet 连入数据中心，该数据中心连入 Internet 的带宽设计为：其带宽总结为 512K ×POS 点数×并发率（30%）。当 POS 点较多时，可由多台汇聚设备分担带宽，保证数据的高速传输。

2).市级大中型 POS 点

市级大中型 POS 点连入数据中心均采用点到点的专线接入方式，因此汇聚设备的带宽及性能选择需根据最大支持的汇接点数据进行判断。

3).区/县级大中型 POS 点

在区/县级 POS 接入区，需在区/县卫生局配置汇聚设备，负责将区/县级以下的 POS 点专线连入汇聚设备。再由汇聚设备采用主备 2 条链路上连至数据中心。该汇聚设备的上传带宽为：其带宽总结为 2M 或 10M ×POS 点数×并发率（30%）＝汇聚设备的上连总带宽需求。当 POS 较多时，可由 1 台或多台汇聚设备分担带宽，保证数据的高速转输。

9.1.4.4 骨干网络带宽设计

区域卫生信息平台骨干网络设计时要重点考虑 2 个方面的需求：

一是转发性能，骨干层设备实现整个平台的数据的转发，根据之前业务流数据的分析，骨干层设备负责数据的高速转发，需要充分考虑分析信息平台的数据

转发性能需求。

二是可靠性，骨干层做为整个信息平台的核心部分，如果骨干层设备出现故障将导致整个信息平台业务中断，因此骨干层设计时需充分考虑设备、链路的高可靠性，保障业务的稳定运行。

1). 转发性能设计

骨干层网络设备的转发性能的设计首先需求明确信息平台网络数据流传输的类型：

- 所有 POS 通过骨干层向业务文档库提交业务文档
- EHR 文档库通过骨干层向 POS 传输电子健康档案信息
- 业务文档库能过骨干层向 EHR 文档库传输健康档案所需信息文档
- 网络管理、网络安全组件通过骨干层对信息平台网络进行监控、实施安全策略
- 数据灾备中心与主服务器区实现同步或异步的数据容灾

骨干层网络设备的转发性能设计参数：

- 所有汇聚设备的汇总链路带宽需求量(根据实际情况进行计算)
- 业务系统区与 EHR 系统区相互的传输带宽需求量（服务器为千兆接入，骨干网络万兆进行数据转发）
- 服务器区（业务系统区和 EHR 系统区）与数据灾备区传输带宽需求量（服务器为千兆接入，核心层万兆连接接入交换机，核心与数据灾备区千兆光纤连接）
- 安全管理区与其他各区域的数据交互带宽需求量（安全管理区服务器、安全设备千兆接入，接入交换机万兆连入核心交换机）
- 外联出口带宽需求量（外联出口设备千兆接入核心交换机）
- 核心设备数量选择，采用 2 台或 2 台以上的核心设备在提供冗余设备和链路的同时，能够有效对数据进行分流转发，避免单台核心设备承受巨大的转发压力，从而保障业务数据的高速转发。

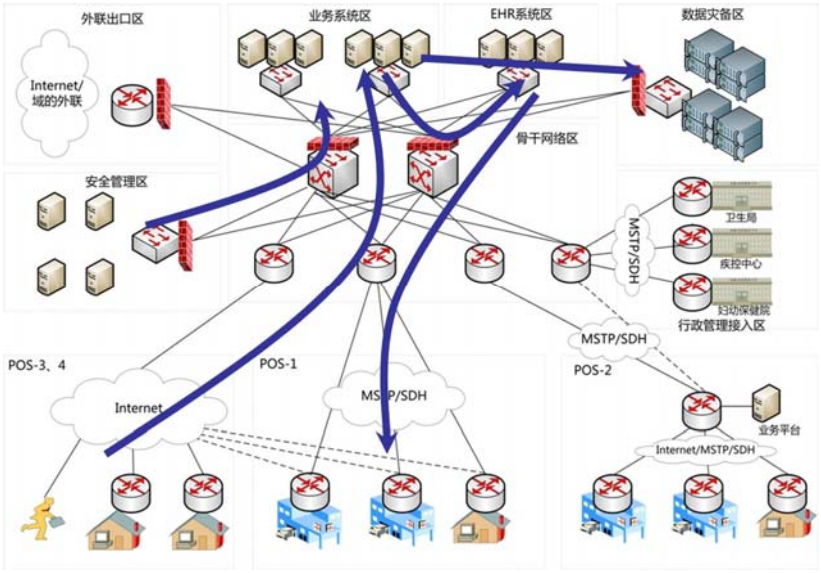


图 9-6 转发性能示意图

2). 高可靠性设计

高可靠性设计主要涉及 2 个方面：

- 设备的高可靠性，选择核心设备时重点需要考虑设备的高可靠性设计，确保核心设备自身的稳定、可靠。主要包括引擎冗余、风扇、电源冗余、引擎自动切换、设备恶劣环境承受能力等
- 冗余设计，汇聚设备、服务器区接入交换机、安全管理区通过 2 条或以上链路与核心设备相关，核心设备采用 2 台或以上进行冗余，确保核心设备故障或某条链路故障不会导至某区域的业务中断。不同规划的区域可选择不同程度的冗余性设计。

9.1.5 区域卫生信息平台网络架构模型

本小节所计算的带宽需求数据均未将 PACS 信息传输列入计算范围，在实际平台建设过程中如需进行 PACS 信息的传输，请在此基础上根据实际情况增大对设备要求。

本小节所计算的性能参数相对较小，在实际带宽及设备性能确定是需要根据实际情况进行调整，以适应后续的业务扩展和应用需求。

9.1.5.1 初级架构

1). 基础数据分析

表 9-4 100 万人口城市医疗机构分布特点

医疗机构类型	医疗机构数量	每机构终端 PC 数量	终端 PC 总数	并发连接比率	链路类型特征	每机构链路带宽（公式详见 9.1.4 小节）
社区卫生服务站	66	2	132	50%	ADSL	512K
社区卫生服务中心	20	5	100	30%	ADSL	1M
二级医院	30	20	600	20%	ADSL/ 专线	2M
三级医院	3	50	150	20%	专线	5M 以上
小计	119		并发终端总数：246			

2). POS 接入层分析

通过上述数据分析，可以得出，100 万人口规模的城市，POS 接入数量为 119，其中约 72%采用 ADSL 方式接入，28%为专线方式接入

社区卫生服务站接入带宽为 512Kbps

社区卫生服务中心接入带宽为 1Mbps

二级医院接入带宽为 1Mbps

三级医院接入带宽为 2.5Mbps

3). 汇聚层分析

- ADSL 方式汇聚需求，86 个 POS 采用 ADSL 方式接入，共有 96 个终端需要建立 VPN 连接

  因此基于 Internet 方式连网的汇聚设备至少需要支持 96 个以上的 VPN 隧道数，且支持数据吞吐量至少为：

  66*50%*512K+20*30%*1M+30*20%*1M+3*2*20%=19Mbps

- 专线方式汇聚需，由于专线采用点到点链路（逻辑），因此根据接入采用专线方式的 POS 数量可以计算出专线汇聚设备的需求，同时考虑设备、链路的冗余特性，至少需要 2 台汇聚设备。在本例中专线接入的链路在 28 条左右。因此汇聚设备至少支持 28 条链路（或逻辑通道）的接入。且

转发性能不低于 3*2M*20%+15*1M*20%＝4.2Mbps

4). 核心层分析

- 核心架构及设备数量

根据之前章节的描述，核心层网络采用交换机组网，并从网络架构稳定性考虑至少需要 2 台核心设备，并汇聚设备与核心设备采用双链路连接，确保网络架构稳定。

- 核心层设备选型

根据之前章节的描述，核心层需要负责整个平台所有数据的转发，其中，业务系统区、EHR 系统区、数据灾备区、安全管理区、外联出口区均采用 1000M 链路，汇聚设备与核心设备之间采用 100M 或 1000M 链路连接，考虑高性能数据转发的需求，建议核心层设备采用万兆核心设备。

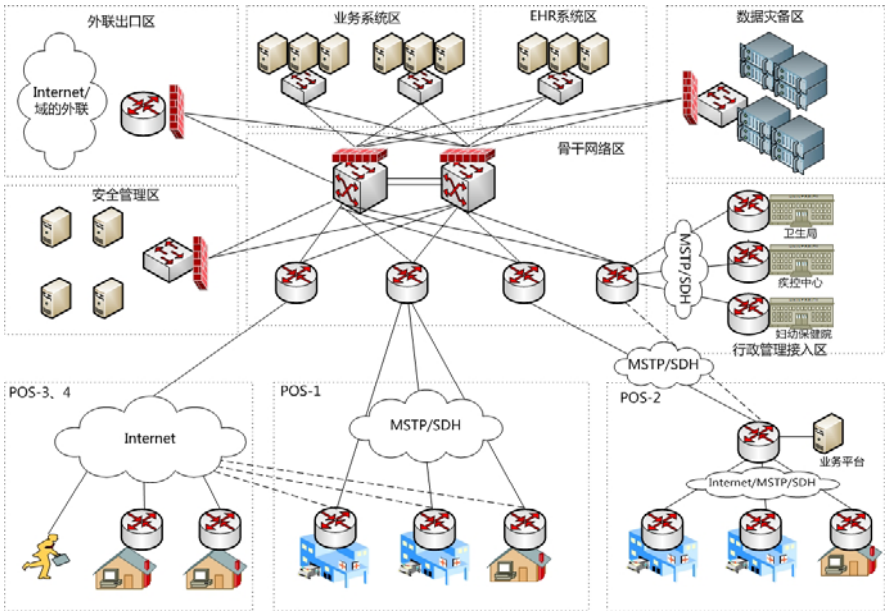


图 9-7　平台初级架构模型

（适用于：100 万人口左右的城市或区域）

9.1.5.2 中级架构

1). 基础数据分析

表 9-5 500 万人口城市医疗机构分布特点

医疗机构类型	医疗机构数量	每机构终端 PC 数量	终端 PC 总数	并发连接比率	链路类型特征	每机构链路带宽（公式详见 9.1.4 小节）
社区卫生服务站	236	3	708	60%	ADSL	512K
社区卫生服务中心	71	10	710	30%	ADSL	1M
二级医院	40	40	1600	20%	专线	4M 以上
三级医院	5	100	500	20%	专线	10M 以上
小计	352		并发终端总数：1057.8			

2). POS 接入层分析

通过上述数据分析，

社区卫生服务站接入带宽为 512Kbps

社区卫生服务中心接入带宽为 1Mbps

二级医院接入带宽为 1Mbps

三级医院接入带宽为 2.5Mbps

3). 汇聚层分析

- ADSL 方式汇聚需求，307 个 POS 采用 ADSL 方式接入，共有 1418 个终端需要建立 VPN 连接，因此基于 Internet 方式连网的汇聚设备至少需要支持 1418 个以上的 VPN 隧道数，且支持数据吞吐量至少为 236*60%*512K+71*30%*1M=93.8Mbps
- 专线方式汇聚需，由于专线采用点到点链路（逻辑），因此根据接入采用专线方式的 POS 数量可以计算出专线汇聚设备的需求，同时考虑设备、链路的冗余特性，至少需要 2 台汇聚设备。在本例中专线接入的链路在 45 条左右。因此汇聚设备至少支持 45 条链路（或逻辑通道）的接入。且总体转发性能不低于 5*2.5M*20%+40*1M*20%＝10.5Mbps

4). 核心层分析

- 核心架构及设备数量

根据之前章节的描述，核心层网络采用交换机组网，并从网络架构稳定性

考虑至少需要 2 台以上核心设备，并汇聚设备与核心设备采用双链路连接，确保网络架构稳定。

- 核心层设备选型

根据之前章节的描述，核心层需要负责整个平台所有数据的转发，其中，业务系统区、EHR 系统区、数据灾备区、安全管理区、外联出口区均采用 1000M 链路，汇聚设备与核心设备之间采用 100M 或 1000M 链路连接，考虑高性能数据转发的需求，建议核心层设备采用万兆核心设备。

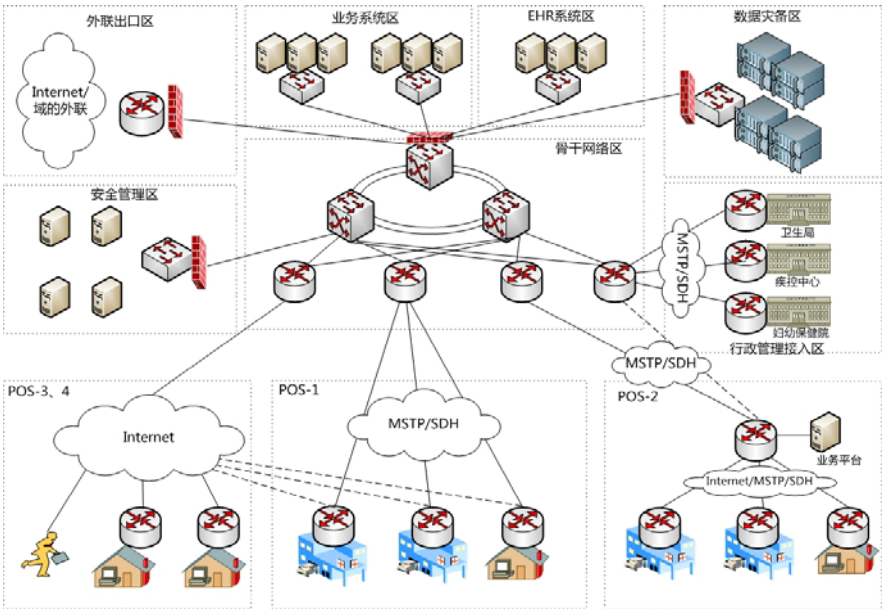


图 9-8 平台中级架构模型

（适用于 500 万人口左右的城市或区域）

9.1.5.3 高级架构

1). 基础数据分析

表 9-6 1000 万人口城市医疗机构分布特点

医疗机构类型	医疗机构数量	每机构终端 PC 数量	终端 PC 总数	并发连接比率	链路类型特征	每机构链路带宽（公式详见 9.1.4 小节）
社区卫生服务站	330	3	708	70%	ADSL	512K
社区卫生服务中心	100	20	710	30%	专线	2M 专线

二级医院	50	100	1600	20%	专线	10M 以上
三级医院	8	200	500	20%	专线	20M 以上
小计	352		并发终端总数：1057.8			

2). POS 接入层分析

通过上述数据分析，可以得出，

社区卫生服务站接入带宽为 512Kbps

社区卫生服务中心接入带宽为 2Mbps

二级医院接入带宽为 2.5Mbps

三级医院接入带宽为 5Mbps

3). 汇聚层分析

- ADSL 方式汇聚需求，330 个 POS 采用 ADSL 方式接入，共有 708 个终端需要建立 VPN 连接

  因此基于 Internet 方式连网的汇聚设备至少需要支持 708 个以上的 VPN 隧道数，且支持数据吞吐量至少为 330*70%*512K=118.2Mbps

- 专线方式汇聚需，由于专线采用点到点链路（逻辑），因此根据接入采用专线方式的 POS 数量可以计算出专线汇聚设备的需求，同时考虑设备、链路的冗余特性，至少需要 2 台汇聚设备。在本例中专线接入的链路在 158 条左右。因此汇聚设备至少支持 158 条链路（或逻辑通道）的接入。且总体转发性能不低于 100*2M*30%+50*2.5M*20%+8*5*20%＝93Mbps

4). 核心层分析

- 核心架构及设备数量

  根据之前章节的描述，核心层网络采用交换机组网，并从网络架构稳定性考虑至少需要 2 台以上核心设备，并汇聚设备与核心设备采用双链路连接，确保网络架构稳定。

- 核心层设备选型

  根据之前章节的描述，核心层需要负责整个平台所有数据的转发，其中，业务系统区、EHR 系统区、数据灾备区、安全管理区、外联出口区均采用 1000M 链路，汇聚设备与核心设备之间采用 100M 或 1000M 链路连接，考虑高性能数据转发的需求，建议核心层设备采用万兆核心设备。

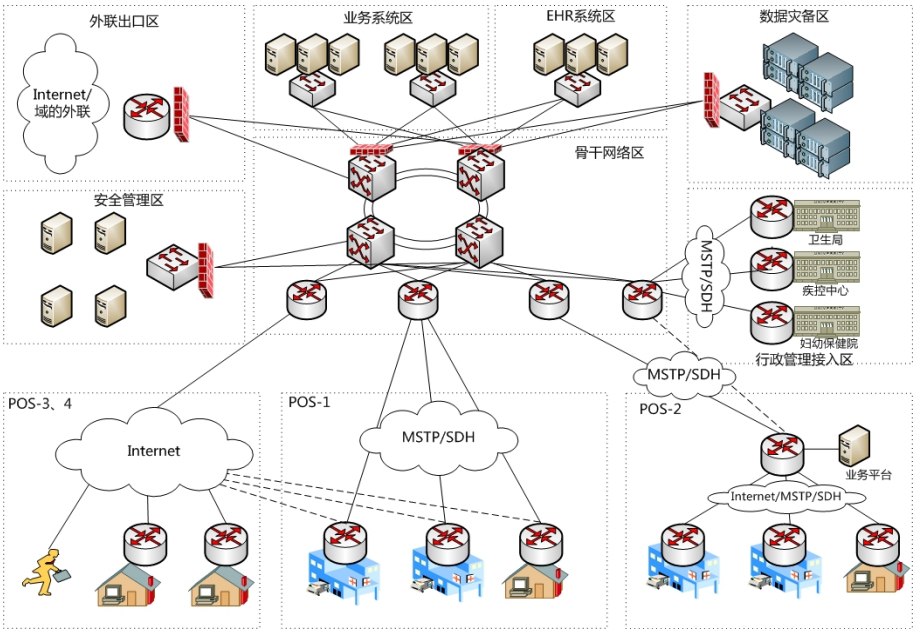


图 9-9 平台初级架构模型

（适用于 1000 万人口以上的城市或区域）

9.2 远程接入模式

9.2.1 远程接入模式分析

在一个区域卫生信息系统中，由于覆盖的卫生医疗单位的种类很多，物理位置相对分散。这些医疗卫生单位由于地理位置的原因或者规模的要求，对于传输网络的要求都不相同。区域卫生信息系统如何能够兼容各种不同的远程接入方式，这是一个很现实的问题。而且由于区域卫生信息系统传递的都是患者的相关信息，还需要保证就是数据传输的安全。

从接入方式的种类上来看，主要分为以下两类：

1） 专线接入方式。其基本方式是进行每个层次之间的专线方式连接，通过这种方式可以实现的星形结构的全局网络连接，基本满足医疗卫生机构与信息平台、卫生机构与卫生机构之间的数据传输需求，这种方式的优点是带宽固定可保障，而且接入单位严格受限。但是同时这种方式存在两个缺点：第一是不灵活，必须使用专用网络覆盖，无法利用 IP 网络资源。第二是费用高，专线方式的网络连接需要支付高昂的专线租用费用。

2） VPN 接入方式。利用公共网络来构建的私人专用网络称为虚拟私有网络

（VPN，Virtual Private Network），用于构建 VPN 的公共网络目前主要指 Internet。VPN 方案的一大特点是可以将远程接入费用减少 60～80%。而且 VPN 大大降低了网络复杂度、VPN 用户的网络地址可以由用户内部进行统一分配、VPN 组网的灵活方便等特性简化了企业的网络管理。另外，在 VPN 应用中，通过远端用户验证以及隧道数据加密等技术保证了通过公用网络传输的私有数据的安全性。主流的 VPN 技术分为三种 IPSec VPN、SSL VPN 和 MPLS VPN 技术。

9.2.2 专线接入方式

考虑到单独建设专用网络投资较高，而且电子政务外网已经基本覆盖县级区域。因此对于专线的接入方式可以考虑利用已经建好的电子政务外网。对于经济条件允许的区域或者电子政务外网尚未建设的区域，也可以考虑租用运营商的 SDH 专线或者 MPLS VPN 专线构建广域网。

9.2.2.1 电子政务外网介绍

政务外网的总体目标是依托统一的国家电子政务通信传输网络，整合建设电子政务外网，通过覆盖全国各级政务部门的网络平台和服务体系，支持电子政务业务系统的运行，支持跨部门、跨地区的信息资源共享，支持电子政务业务系统的互联互通和信息交换，促进政府监管能力和服务水平的提高。按照国家电子政务外网建设总体规划，电子政务外网分为国家、省、市和县四级，是可信且安全的政府公用网，承载多种跨部门、跨地区的政务业务应用系统，提供丰富的网络信息资源与服务，实现各部门专网以及各级外网的互联互通。

纵向网络的应用：电子政务外网可以满足互联互通的要求，而且保证卫生系统纵向的相对独立性和纵向网络系统的正常运行，提供包含卫生部门在内的各个部门高速通达、逻辑专用、安全可靠、方便使用的纵向系统虚拟专用网络（一般采用 MPLS VPN 技术）。

横向网络的应用：医疗卫生联网部门将逐步开展横向电子政务业务（区域卫生信息系统）。电子政务外网既可以满足互联互通的要求，又可以实现相关部门横向业务系统的相对独立性，使横向业务高速通达、逻辑专用、安全可靠、方便使用的横向系统虚拟专用网络（一般采用 MPLS VPN 技术）。

9.2.2.2 对于电子政务外网链路的要求

各地区的电子政务外网建设情况差异较大，主要有以下三种方式：

1）SDH 作为承载链路，使用 MPLS VPN 技术进行数据的逻辑隔离。此类型的链路可以充分保障链路的可靠性和数据传输的安全性，可以直接作为医疗卫生机构接入的链路使用。

2）裸光纤作为承载链路，使用 MPLS VPN 技术进行数据的逻辑隔离。此类型的链路可靠性低于 SDH 承载链路，同时成本也低于 SDH 承载链路的方式，也可以作为医疗卫生机构接入的链路使用

3）裸光纤作为承载链路，没有逻辑隔离措施。由于数据的传输没有隔离，不利于数据的保密要求，而且容易造成病毒的跨机构传播从而影响整网的安全状态，不推荐用于广域网接入，可以升级为 MPLS VPN 网络后使用。

9.2.2.3 适合的医疗卫生机构

由于各地电子政务网覆盖范围差异较大，且电子政务外网采用光纤专网接入方式，布设成本和时间代价较高，因此本区域内已有专网光纤覆盖的地区可以优先选择电子政务外网接入，需要新增光纤铺设的医疗卫生机构需要考虑成本，也可采用基于公网（Internet）的 VPN 加密传输方式（IPSec VPN 或 SSL VPN)。

9.2.2.4 医疗卫生机构的专线接入设备选择

由于电子政务外网已经构成了完善的广域网系统，也同时解决了广域网路由问题。在此主要考虑医疗卫生机构和区域卫生信息平台两端分别需要部署 OSPF、RIP 等静动态路由协议即可实现数据的转发功能。为了避免重复 IP 地址造成的冲突问题，还需要对部分医疗卫生机构的 IP 地址进行转换，也就是需要医疗卫生机构的专线接入设备支持 Nat（网络地址转换）技术。建议采用医疗卫生机构采用企业级路由器作为基本的专线接入设备，如果考虑到传输数据的安全问题，可以增加独立的硬件防火墙等安全设备过滤病毒、攻击等恶意数据。

9.2.3 大中型医疗机构基于公网的加密接入（IPSec VPN）

9.2.3.1 IPSec VPN技术

IPSec（Internet Protocol Security）即 Intenet 安全协议，是 IETF 提供 Internet 安全通信的一系列规范，它提供私有信息通过公用网的安全保障。IPSec

适用于目前的版本 IPv4 和下一代 IPv6。IPSec 规范相当复杂，规范中包含大量的文档。由于 IPSec 在 TCP/IP 协议的核心层——IP 层实现，因此可以有效地保护各种上层协议，并为各种安全服务提供一个统一的平台。IPSec 也是被下一代 Internet 所采用的网络安全协议。IPSec 协议是现在 VPN 开发中使用的最广泛的一种协议，它有可能在将来成为 IPVPN 的标准。

IPSec 的基本目的是把密码学的安全机制引入 IP 协议，通过使用现代密码学方法支持保密和认证服务，使用户能有选择地使用，并得到所期望的安全服务。IPSec 是随着 IPv6 的制定而产生的，鉴于 IPv4 的应用仍然很广泛，所以后来在 IPSec 的制定中也增加了对 IPv4 的支持。IPSec 在 IPv6 中是必须支持的。

9.2.3.2 IPSec VPN的特点

在区域卫生信息系统应用中，推荐在医疗卫生机构和区域卫生信息平台分别部署 IPSec VPN 网关。IPSec VPN 技术的优点在于：

由于是硬件网关间的传输过程进行数据加解密处理，对于业务平台的服务器是完全透明的，不需要单独更改其安全策略。

由于多年的技术发展，IPSec VPN 技术已经非常成熟，而且是独立硬件加解密，可以支持 7*24 小时的稳定运行。

IPSec VPN 技术的缺点在于：

不适合少量 PC 直接远程访问区域卫生信息平台的情况。这是因为 IPSec 协议的限制，对于社区服务站的少量 PC 需要访问区域卫生信息平台时必须安装 IPSec VPN 客户端软件，而这无论对于实施还是维护工作都比较复杂。

权限控制粒度较粗，一般只用来实现对于 IP 地址的访问管理。

9.2.3.3 适合的医疗卫生机构

结合 IPSec VPN 技术的特点，推荐大中型医疗卫生机构（三级、二级医院等）部署 IPSec VPN 硬件网关，与区域卫生信息平台的 IPSec VPN 网关对应部署。构建与区域卫生信息平台的数据安全传输通道。这是因为：

1) 大中型医疗卫生机构需要保持 7*24 小时的稳定数据连接，IPSec VPN 由于采用硬件加解密的方式，其运行稳定性较高。
2) 大中型医疗卫生机构的数据流量较大（主要为医疗影像调阅），IPSec VPN 技术成熟且成本较低（相对 SSL VPN 技术）。

3) 由于是硬件网关间的传输过程进行数据加解密处理，对于业务平台的服务器是完全透明的，部署更简单。

4) IP 地址级的权限控制粒度可以满足平台与大中型医疗卫生机构的数据管理要求。

9.2.3.4 加密技术

IPSec 协议采用 Internet 密钥交换协议（Internet Key Exchange，IKE），该协议用于通信双方协商和建立安全联盟，交换密钥。IKE 定义了通信双方进行身份认证、协商加密算法以及生成共享的会话密钥的方法。IKE 的精髓在于它永远不在不安全的网络上直接传送密钥，而是通过一系列数据的交换，通信双方最终计算出共享的密钥。其中的核心技术就是 DH（Diffie Hellman）交换技术。DH 交换基于公开的信息计算私有信息，数学上已经证明，破解 DH 交换的计算复杂度非常高从而是不可实现的。所以，DH 交换技术可以保证双方能够安全地获得公有信息，即使第三方截获了双方用于计算密钥的所有交换数据，也不足以计算出真正的密钥。

在身份验证方面，IKE 提供了共享验证字（Pre-shared Key）、公钥加密验证、数字签名验证等验证方法。后两种方法通过对 CA（Certificate Authority）中心的支持来实现。

IKE 密钥交换分为两个阶段，其中阶段 1 建立 ISAKMP SA，有主模式（Main Mode）和激进模式（Aggressive Mode）两种；阶段 2 在阶段 1 ISAKMP SA 的保护下建立 IPSec SA，称之为快速模式（Quick Mode）。IPSec SA 用于最终的 IP 数据安全传送。

另外，IKE 还包含有传送信息的信息交换（Informational Exchange）和建立新 DH 组的组交换（DH Group Exchange）。

9.2.3.5 身份认证技术

IPSec 隧道建立的前提是双方的身份的得到了认证，这就是所谓的身份验证。身份验证确认通信双方的身份。目前有两种方式：

一种是域共享密钥（pre-shared key）验证方法，验证字用来作为一个输入产生密钥，验证字不同是不可能在双方产生相同的密钥的。验证字是验证双方身份的关键。这种认证方式的优点是简单，但有一个严重的缺点就是验证字作为明

文字符串，很容易泄漏。

另一种是 PKI(rsa-signature)验证方法。这种方法通过数字证书对身份进行认证，安全级别很高，是目前最先进的身份认证方式。

公钥基础设施（Public Key Infrastructure，简称 PKI）是通过使用公开密钥技术和数字证书来确保系统信息安全并负责验证数字证书持有者身份的一种体系，它是一套软硬件系统和安全策略的集合，提供了一整套安全机制。PKI 采用证书进行公钥管理，通过第三方的可信任机构，把用户的公钥和用户的其他标识信息捆绑在一起，以在网上验证用户的身份。PKI 为用户建立起一个安全的网络运行环境，使用户可以在多种应用环境下方便的使用加密和数字签名技术，从而保证网上数据的机密性、完整性、有效性。数据的机密性是指数据在传输过程中，不能被非授权者偷看；数据的完整性是指数据在传输过程中不能被非法篡改；数据的有效性是指数据不能被否认。

一个 PKI 系统由公开密钥密码技术、证书认证机构、注册机构、数字证书和相应的 PKI 存储库共同组成。

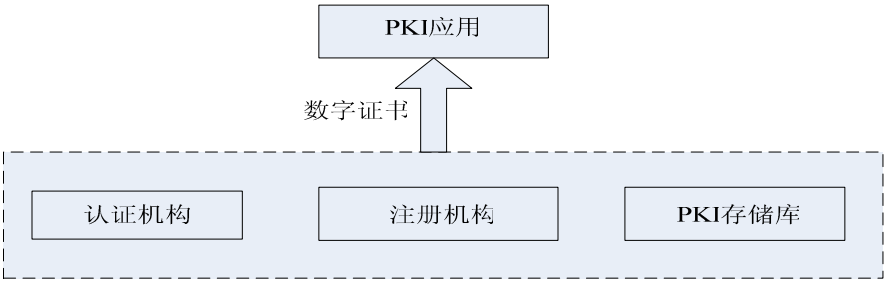


图 9-10 PKI 组成框图

其中，认证机构用于签发并管理证书；注册机构用于个人身份审核、证书废除列表管理等；PKI 存储库用于对证书和日志等信息进行存储和管理，并提供一定的查询功能；数字证书是 PKI 应用信任的基础，是 PKI 系统的安全凭据。数字证书又称为公共密钥证书 PKC（Public Key Certificate），是基于公共密钥技术发展起来的一种主要用于验证的技术，它是一个经证书认证中心数字签名的包含公开密钥拥有者信息以及公开密钥的文件，可作为各类实体在网上进行信息交流及商务活动的身份证明。证书是有生命期的，在证书生成时指定，认证中心也可以在证书的有效期到来前吊销证书，结束证书的生命期。

9.2.4 小型医疗机构基于公网的加密接入（SSL VPN）

9.2.4.1 SSL VPN技术

SSL VPN即指采用SSL （Security Socket Layer）协议来实现远程接入的一种新型VPN技术。SSL协议是网景公司提出的基于WEB应用的安全协议，它包括：服务器认证、客户认证（可选）、SSL链路上的数据完整性和SSL链路上的数据保密性。对于内、外部应用来说，使用SSL可保证信息的真实性、完整性和保密性。目前SSL协议被广泛应用于各种浏览器应用，也可以应用于Outlook等使用TCP协议传输数据的C/S应用。正因为SSL协议被内置于IE等浏览器中，使用SSL协议进行认证和数据加密的SSL VPN就可以免于安装客户端。

9.2.4.2 SSL VPN的特点

SSL VPN作为新兴的VPN技术，有着传统IPSec VPN无法比拟的优点：

1) 通过电脑直接远程访问内网的用户，如果是B/S架构，则不需要安装客户端软件（部署IPsec VPN需要预先安装一个客户端软件），因为部署和维护更简单。
2) 通过电脑直接远程访问内网的用户，如果是B/S架构，则客户端软件可以隐形部署且免维护（部署IPsec VPN需要预先安装一个客户端软件），因为部署和维护更简单。
3) 管理力度更细，一方面SSL VPN可以支持对URL、文件共享目录、TCP服务、IP网段等不同粒度的访问控制，另一方面SSL VPN的授权实现了基于角色或用户组的管理，从而方便了管理员对用户实施精确的权限管理。
4) 具备安全检查功能，SSL VPN可以做到在用户正式登录SSL VPN之前，通过下载一个主机检查器，自动检查远程主机的运行环境是否安全。

当然，目前SSL VPN也有自身的缺点：主要是对硬件资源的消耗较大，从成本角度来说要高于传统IPSec VPN方式。

9.2.4.3 适合的医疗卫生机构

结合SSL VPN技术的特点，推荐小型医疗卫生机构（社区服务站等）直接通过计算机远程登录SSL VPN网关，进行相关的业务操作。这是因为：

1) 小型医疗卫生机构计算机数量较少，采用硬件IPSec VPN方式成本较高，浪费资源。

2) SSL VPN 可以保证接入数据的安全性，且对于 B/S 架构无须安装客户端，对于 C/S 架构可以免于维护客户端。非常适合小型医疗卫生机构少量计算机的远程安全登录要求。

3) 可以支持本地认证、Radius(Remote Authentication Dial In User Service)认证、Ldap(Lightweight Directory Access Protocol)等多种认证方式，可以与应用认证系统相结合。

4) 更细粒度的管理，SSL VPN 可以支持对 URL、TCP 服务、IP 网段等不同粒度的访问控制。还可以实现了基于角色或用户组的管理，从而方便了管理员对用户实施精确的权限管理。

9.2.4.4 身份认证技术

1). 对用户名和密码的认证

目前网络上常用的身份认证方法就是对用户名和密码的验证。根据用户是否能提供正确的私密信息来判断用户身份的合法性。这种认证方法的好处是简单可行。根据服务器端保存验证信息的位置来划分，可以有两种工作方式：本地认证和外部认证。如下图所示的为本地认证：

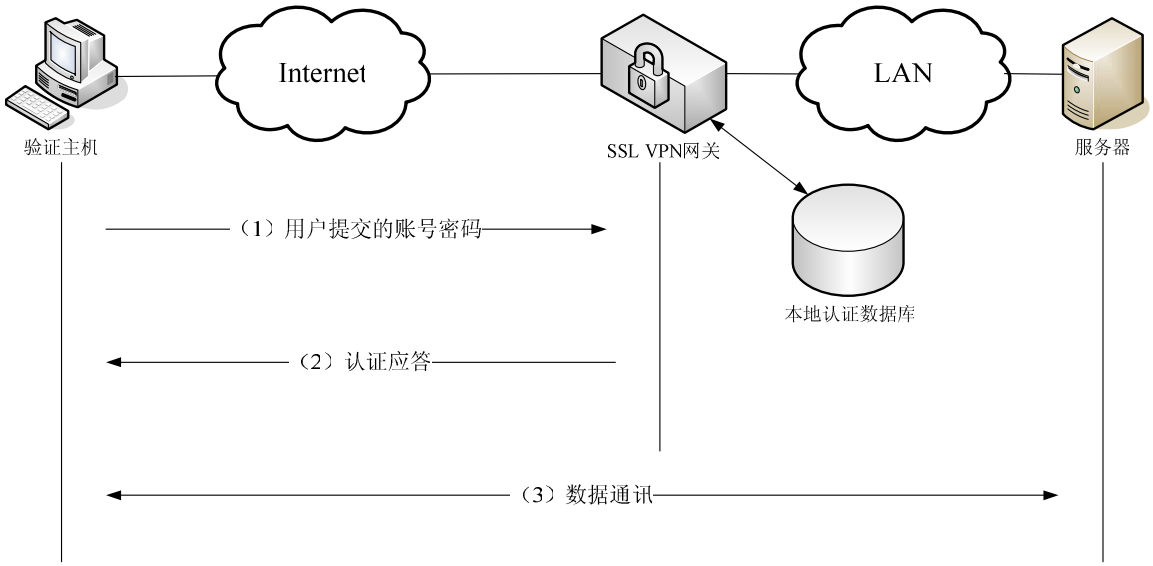


图 9-11 本地认证过程

在本地认证过程中，网关设备上保存着用户名和密码的验证信息，由网关对认证请求中的用户名和密码进行验证，以确认用户身份。如果认证成功，则可以

与远端建立受信任的连接。

如果用户身份的验证信息保存在外部服务器上，则网关设备就相当于一个认证代理，负责转送认证信息，并接收认证结果。如果外部认证服务器对用户身份认证成功，网关设备就与远程用户建立受信任的连接，允许用户访问内部网络。反之，则拒绝接入。外部认证过程如下图所示：

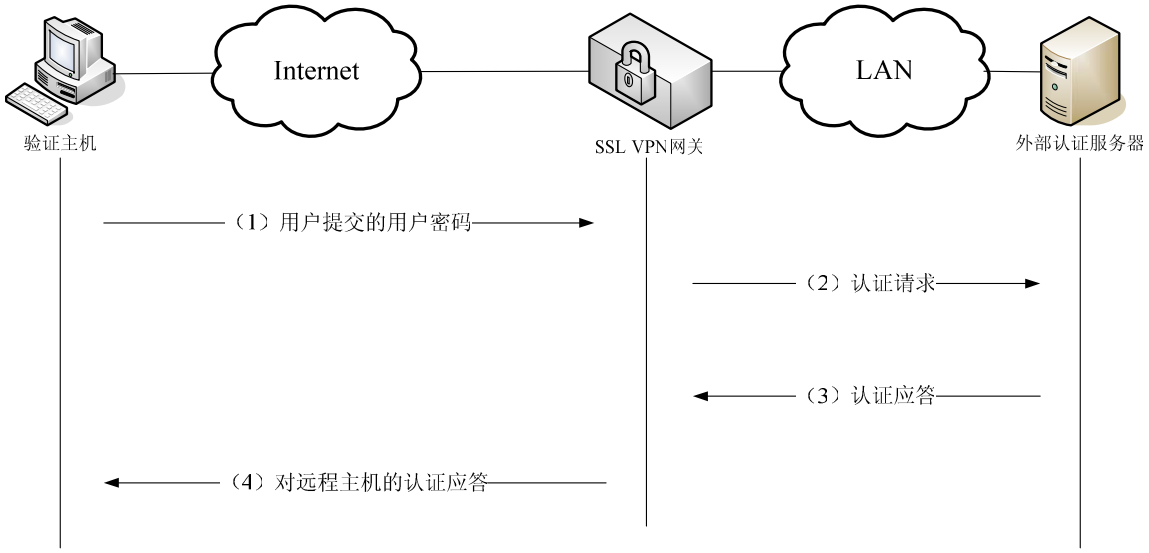


图 9-12 外部认证

网关与外部认证服务器之间可以有多种交互协议。在拨号上网时代，使用最多的是 RADIUS 协议，该协议除了能对用户名和密码进行验证外，还可以进行授权和计费等操作，因而也将 RADIUS 认证称为 AAA 服务(Authentication，Authorization，Accounting)。

随着网络信息容量的增大，人们对信息的组织和查询提出了更高的要求。一种称为 LDAP 的服务就应运而生了。LDAP 服务器可以很好地管理和组织一个企业的数据，当然也可以存储用户身份认证信息，这样使得 LDAP 服务器成为了认证服务器。网关设备可以通过查询 LDAP 数据库，来确认远程用户提交的用户名和密码是否正确。

微软公司扩展了 LDAP 协议，构建了适应 Windows 网络的 AD 服务。在 Windows 2000 以后的操作系统之中，AD 认证被广泛应用，成为目前应用较多的认证方式之一。

如前所述，用户名和密码在认证过程中有可能被截获，也有可能遭受中间人

攻击。对此，采用了 SSL 协议建立加密隧道的 SSL VPN 可以有效的消除这些危险。首先 SSL 隧道是加密的，明文的用户名和密码在传输时被加了密，不容易被破解。同时 SSL 协议建立连接的过程是被精心设计过的，可以有效抵御中间人的攻击；加密的连接一旦建立起来后，中间人由于无法破解密文，将无法窃取通讯数据内容。所以说用户名密码方式的认证与 SSL 协议相结合，将大大提高身份认证的的安全性。

2). PKI 证书认证

- **非对称加密算法的公钥和私钥**

非对称加密算法的密钥是一对不相同的密钥。用其中任意一个进行加密只能用另一个进行解密。在实际使用中，将一个密钥进行保密，不对外公开，该密钥被称为“私钥”；而将另一个密钥公开，该密钥称为“公钥”。

- **摘要**

对一段数据进行某种哈希计算，得到固定长度的计算结果。该结果就被称为摘要。摘要也被称为该段数据的特征码，不同数据段的摘要一般不会相同。

- **数字签名**

对数据段的摘要使用用户的私钥进行加密，其结果就被称为用户对该段数据的数字签名。对数字签名的验证只能使用与签名私钥对应的公钥先解密，并比较解密结果与数据段的摘要是否一致，从而判断出数字签名是否正确。如果数字签名正确，就说明签名的用户拥有与公钥相对应的私钥，从而证明了签名用户的合法身份。

- **CA 证书**

该证书是一份由 CA(证书授权机构)签发的文件，其中包含了用户名称、公钥、私钥、证书的有效期、证书的颁发者等信息。在文件的末尾附上了 CA 写的数字签名，以表明该证书是由合法的 CA 所签发。如果证书中只包含了公钥则被称为公钥证书，公钥证书是可以对外公开的。颁发给个人的证书中一般都包含了一对公私钥，私钥不可以公开，更不可以在网上传送;在个人证书中包含了一张公钥证书，这张公钥证书可以在通讯过程中传给对方，以验证个人的身份。通过 IE 浏览器可以看到证书的内容如下：

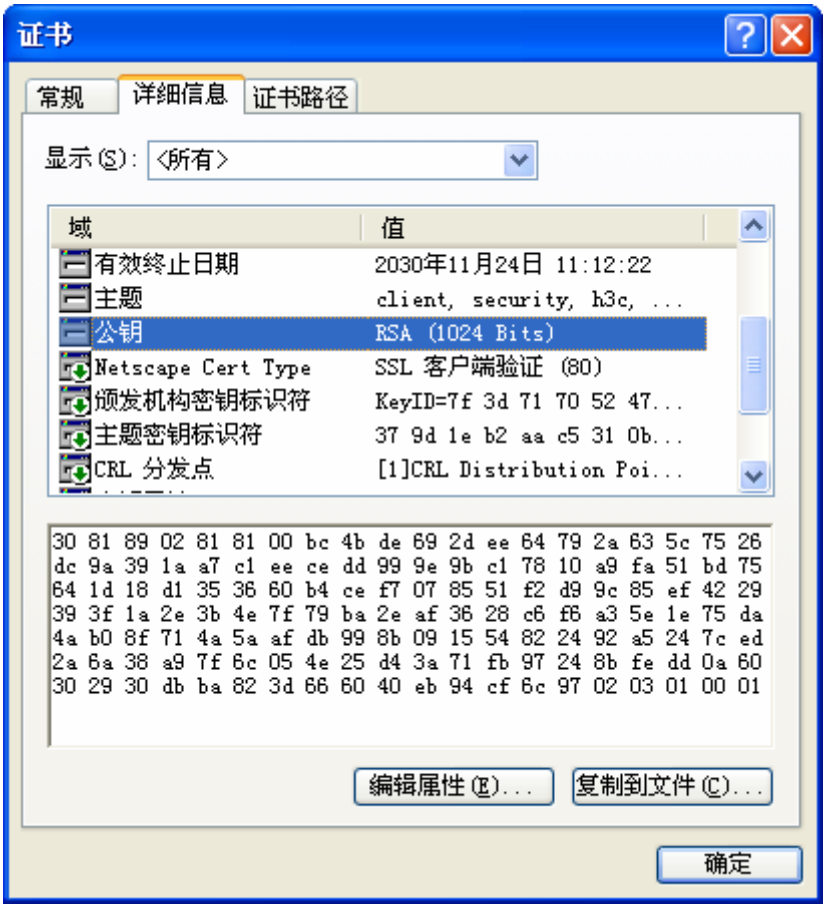


图 9-13 IE 浏览器中的个人证书

个人证书的获取一般采用带外方式，如通过移动硬盘拷贝证书，再以手工方式导入计算机，这样做可以保证证书的私密性；在要求不太高的情况下，证书也可以通过 Web 网站在线获取。

9.2.5 远程接入的可靠性设计

9.2.5.1 双出口备份

对于远程安全接入，出现故障更多的时候在于运营商链路的不可靠。而对于运营商链路传输的状况，需要能够做到实时的监视，以保证 VPN 隧道/广域网路由的实时切换。

传统的备份实现方式，通常依靠检测接口的物理 UP、Down 变化消息或者网络层协议 UP、Down 变化来触发主备切换。自动侦测特性利用 ICMP 的 request/response 报文，检测目的地的可达性，检测结果反馈到与之联动的备份功能模块，触发其主备切换，从而提供了基于网络层应用可达性的备份功能。

9.2.5.2 双机备份

双机备份是通过 VRRP 实现的。VRRP（Virtual Router Redundancy Protocol，虚拟路由冗余协议）是一种容错协议。通常，一个网络内的所有主机都设置一条缺省路由（如下图所示，10.100.10.1），这样，主机发出的目的地址不在本网段的报文将被通过缺省路由发往路由器 RouterA，从而实现了主机与外部网络的通信。当路由器 RouterA 坏掉时，本网段内所有以 RouterA 为缺省路由下一跳的主机将断掉与外部的通信。

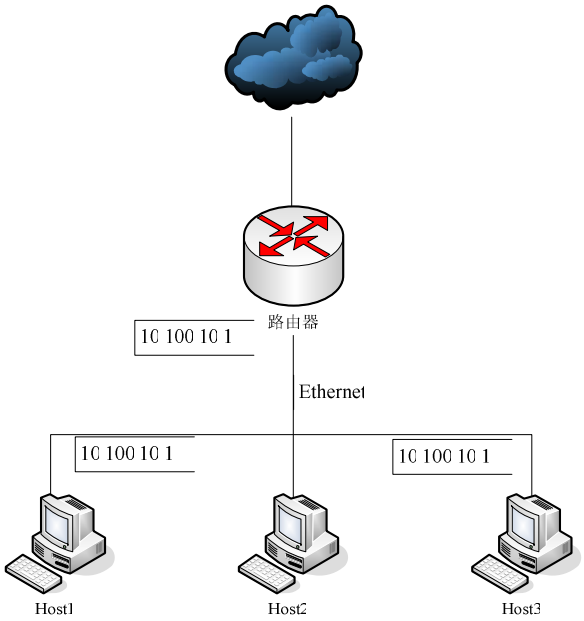


图 9-14 局域网组网方案

VRRP 就是为解决上述问题而提出的，它为具有多播或广播能力的局域网（如：以太网）设计。我们结合下图来看一下 VRRP 的实现原理。VRRP 将局域网的一组路由器（包括一个 Master 即活动路由器和若干个 Backup 即备份路由器）组织成一个虚拟路由器，称之为一个备份组。

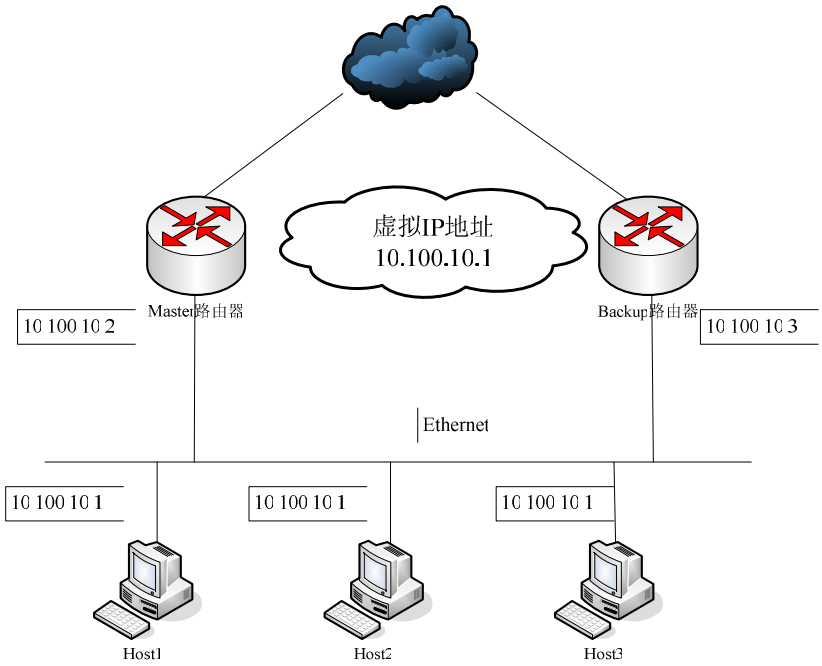


图 9-15 VRRP 组网示意图

这个虚拟的路由器拥有自己的 IP 地址 10.100.10.1（这个 IP 地址可以和备份组内的某个路由器的接口地址相同），备份组内的路由器也有自己的 IP 地址（如 Master 的 IP 地址为 10.100.10.2，Backup 的 IP 地址为 10.100.10.3）。局域网内的主机仅仅知道这个虚拟路由器的 IP 地址 10.100.10.1，而并不知道具体的 Master 路由器的 IP 地址 10.100.10.2 以及 Backup 路由器的 IP 地址 10.100.10.3，它们将自己的缺省路由下一跳地址设置为该虚拟路由器的 IP 地址 10.100.10.1。于是，网络内的主机就通过这个虚拟的路由器来与其它网络进行通信。如果备份组内的 Master 路由器坏掉，Backup 路由器将会通过选举策略选出一个新的 Master 路由器，继续向网络内的主机提供路由服务。从而实现网络内的主机不间断地与外部网络进行通信。

9.2.5.3 快速切换

网络异常的情况有很多种。如果不考虑运营商的网络异常，VPN 的异常主要有两大类：第一类是网关异常，包括网关瘫痪、重启等等；第二类是网关链路异常。在网络出现异常时，如何保证业务流量能够尽快恢复？

网关快速切换，这一切换由自动侦测特性发现，VRRP 实现。当主网关或其链路出现异常时，自动侦测特性能够保证在 1~2 秒内发现，通过 VRRP3~4 秒内完成主

备网关的切换。而且为了保证网关切换后，网关内外的流量能同时切换到新的网关上，需要在网关内外都设置 VRRP 组，并将这一对 VRRP 组关联起来。一旦其中一个 VRRP 组发生切换，另一个方向的 VRRP 能发起同步切换。

IPSec 隧道快速切换，这一切换由 IPSec DPD 实现。IPSec DPD（IPSec Dead Peer Detection on-demand）为按需型 IPSec/IKE 安全隧道对端状态探测功能。启动 DPD 功能后，当接收端长时间收不到对端的报文时，能够触发 DPD 查询，主动向对端发送请求报文，对 IKE Peer 是否存在进行检测。与 IPSec 中原有的周期性 Keepalive 功能相比，DPD 具有产生数据流量小、检测及时、隧道恢复快的优点。

9.3 平台架构

9.3.1 平台架构概述

网络基础设施平台的由业务系统、EHR 系统、数据存储及灾备系统组成，其硬件一般包括：

- 数据库服务器、备份服务器、应用服务器等；
- 交换机、路由器、防火墙、VPN 等网络设备；
- 存储设备如磁盘阵列、磁带库等。

网络基础设施平台的硬件系统配置，应根据当地实际业务需求、网络覆盖范围和规模以及经济条件，本着经济、实用、高效和分步实施的原则，选择适当的建设方案。

9.3.2 平台整体规划

9.3.2.1 平台分区设计

平台根据应用的不同，可分为医疗业务区、办公应用区、网络管理区、安全防护区、数据存储区、HER 系统区和备份区等几大常规区域。不论平台规模的大小，上述几个平台区域都是必备的。

9.3.2.2 平台分层设计

区域卫生信息平台数据中心网络架构大体分为接入层、核心交换层及业务服务层三部分。

- 接入层主要是作为整个平台的网管，负责对外连接相关节点；
- 核心交换层由核心交换机组成，主要完成数据的高速、安全的交换；
- 业务服务层由多台服务器组成，主要提供核心业务服务。

9.3.3 平台架构模型

由于不同区域规模的情况不同，因此给出三类平台架构予以参考。

9.3.3.1 初级架构

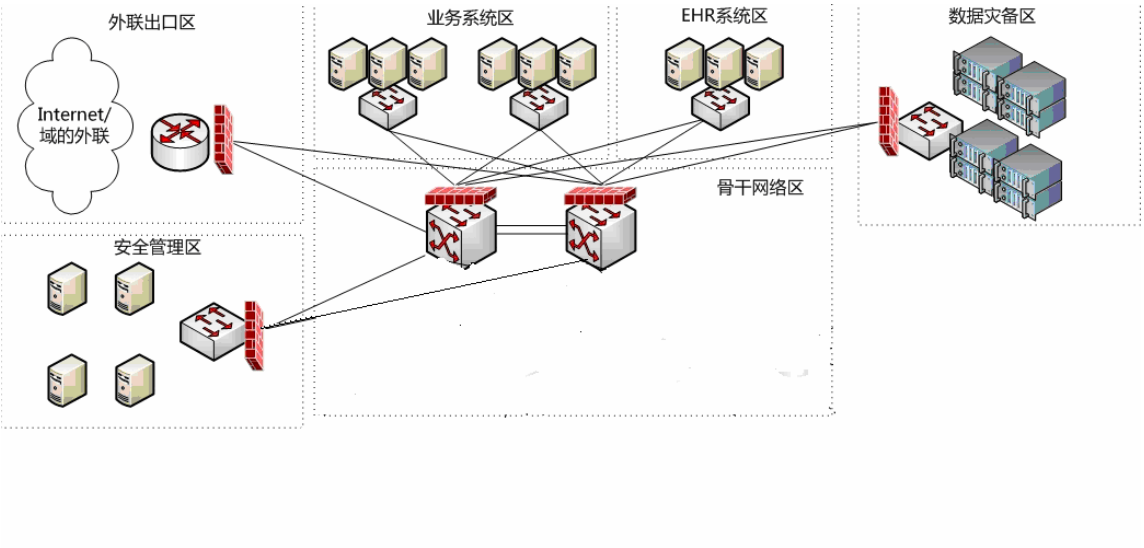


图 9-16 平台初级机构模型

适用条件：

健康档案的区域卫生信息平台建设的初期阶段；

数量在 100 万以下的市级或区县级区域卫生信息平台；

医疗机构数和业务系统数比较少的区域卫生信息平台。

9.3.3.2 中级架构

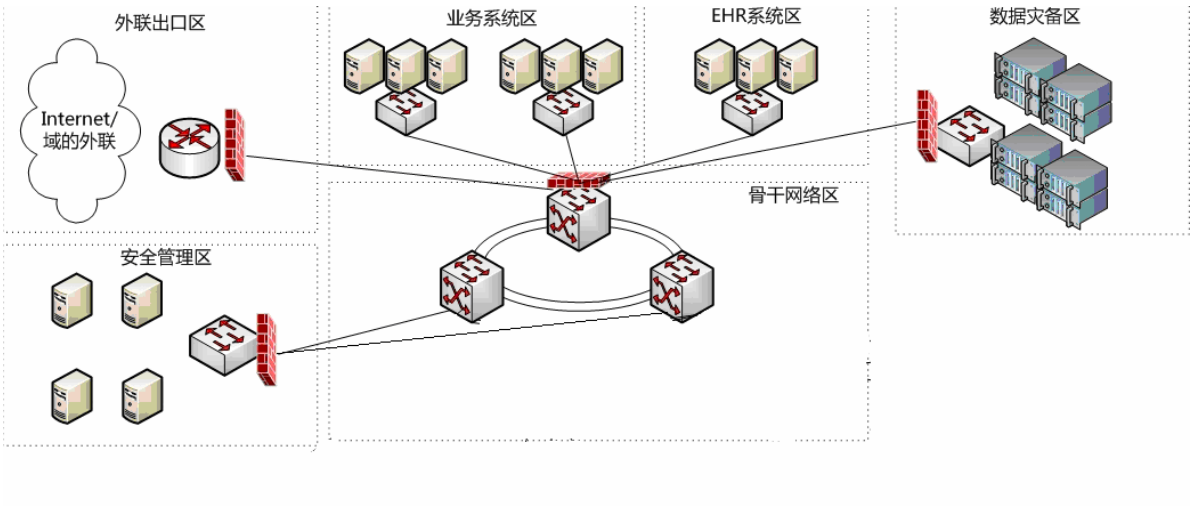


图 9-17 平台中级机构模型

适用条件：

基于健康档案的区域卫生信息平台建设的发展阶段；

人口数量在 500 万以下的市级单位区域卫生信息平台；

基于健康档案的区域卫生信息平台建设初期阶段的省级平台。

9.3.3.3 高级架构

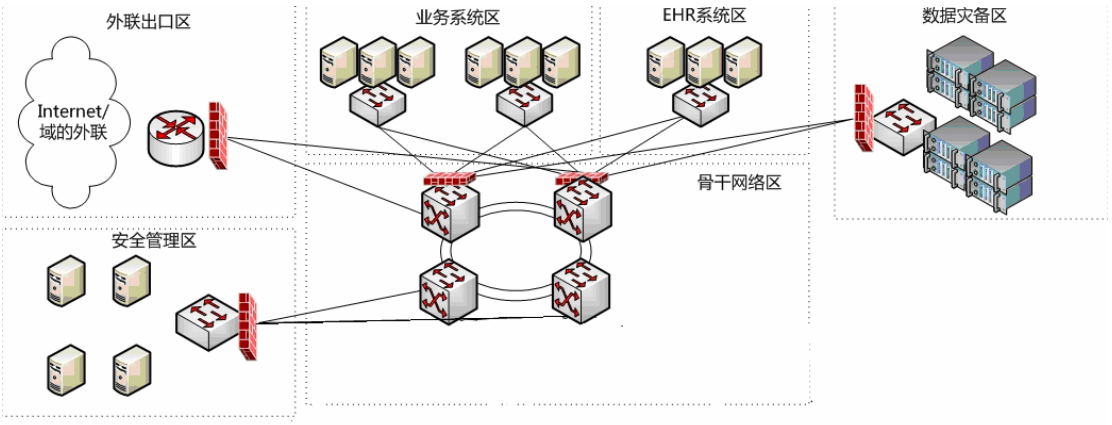


图 9-18 平台高级机构模型

适用条件：

基于健康档案的区域卫生信息平台建设的高级阶段；

人口数量在 1000 万以上的市级单位区域卫生信息平台；

完善阶段的省级区域卫生信息平台。

9.4 网络安全可用性设计

9.4.1 网络可靠性和冗余

建议从以下几个方面考虑高可用设计：

- 网络设备考虑交换引擎、接口、风扇、电源等冗余配置。
- 服务器接入层交换机成对部署，以支持服务器的多网卡双归属接入方式
- 在服务器接入交换机与汇聚交换机之间部署全交叉的物理链路，以实现链路的可靠性。
- 当服务器采用二层接入时，应将主汇聚交换机做为第一级服务器的默认网关以及 STP 的根节点，并将备份汇聚交换机设置为备用网关和备用 STP 根。
- 将 VRRP＋MSTP 或交换机虚拟化技术做为保证高可用型的实现技术。

9.4.2 线路备份

建议从以下几个方面考虑双链路部署：

1) 数据中心每个分区的边缘设备都被连接到Core-SW1 和Core-SW2 网络模块上。每个 VLAN 都配置在两台交换机上。以保证当第一个交换机上的模块或端口问题引起链路中断时，第二个交换机能够继续数据的传输。交换机之间创建聚合链路连接，在端口上配置生效 trunking，这样两台交换机上的 VLAN 之间能够实现互通。
2) 运营商的网络状态可能出现不稳定情况，因此可考虑联通、电信等多网络出口备份以保证可用性。

9.4.3 路由备份

通过配置备份的静态路由和动态路由，可以保证路由的畅通，网络的可达，当由于某种原因主路由失效时候，设备可以根据备份路由继续提供网络服务。也可以使用 VPN 和物理专线互为备份。

9.4.4 网络安全技术部署

1) 基于 VLAN 的端口隔离

交换机可以由硬件实现相同 VLAN 中的两个端口互相隔离。隔离后这两个端口

在本设备内不能实现二、三层互通。当相同 VLAN 中的服务器之间完全没有互访要求时，可以设置各自连接的端口为隔离端口(如下图)。这样可以更好的保证相同安全区域内的服务器之间的安全：

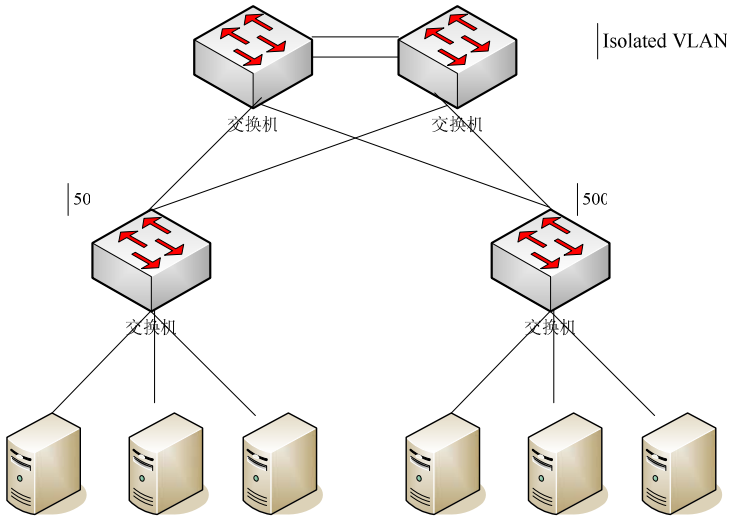


图 9-19 基于 VLAN 的端口隔离

2) STP Root/BPDU Guard

基于 Root/BPDU Guard(Root/Bridge Protocol Data Unit Guard)方式的二层连接保护保证 STP/RSTP(Spanning Tree Protocol/ Rapid Spanning Tree Protocol)稳定,防止攻击,保障可靠的二层连接（如下图)。

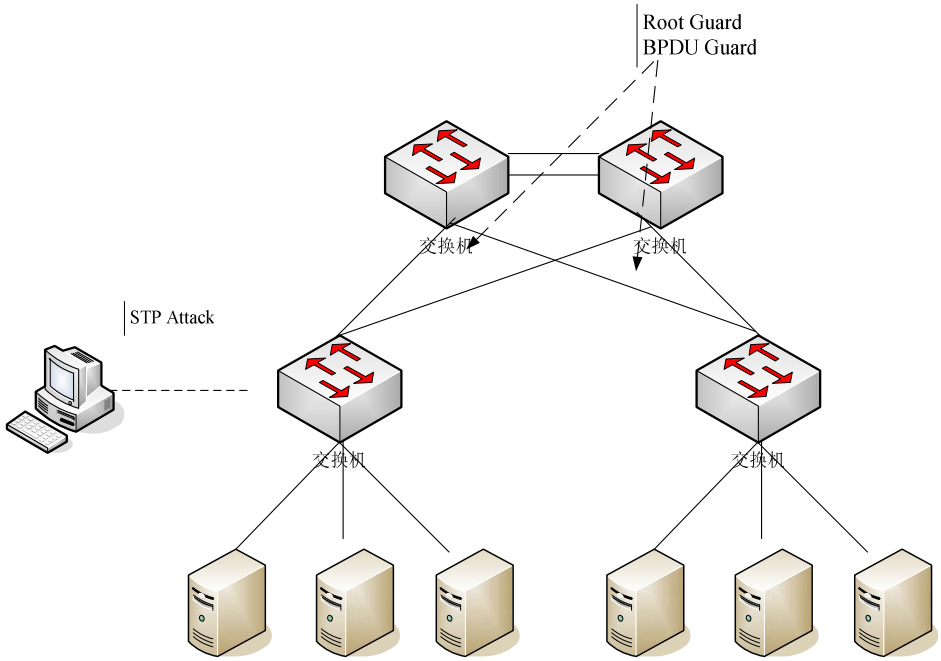


图 9-20 交换机 Root Guard/BPDU Guard 技术

■ **BPDU Guard**

对于接入层设备，接入端口一般直接与用户终端（如 PC 机）或文件服务器相连，此时接入端口被设置为边缘端口以实现这些端口的快速迁移；当这些端口接受到配置消息（BPDU 报文）时系统会自动将这些端口设置为非边缘端口，重新计算生成树，引起网络拓扑的震荡。这些端口正常情况下应该不会收到生成树协议的配置消息的。如果有人伪造配置消息恶意攻击交换机，就会引起网络震荡。BPDU 保护功能可以防止这种网络攻击。

交换机上启动了 BPDU 保护功能以后，如果边缘端口收到了配置消息，系统就将这些端口 shutdown，同时通知网管。被 shutdown 的端口只能由网络管理人员恢复。推荐用户在配置了边缘端口的交换机上配置 BPDU 保护功能。

■ **ROOT Guard**

由于维护人员的错误配置或网络中的恶意攻击，网络中的合法根交换机有可能会收到优先级更高的配置消息，这样当前根交换机会失去根交换机的地位，引起网络拓扑结构的错误变动。这种不合法的变动，会导致原来应该通过高速链路的流量被牵引到低速链路上，导致网络拥塞。Root 保护功能可以防止这种情况的发生。

对于设置了 Root 保护功能的端口，端口角色只能保持为指定端口。一旦这种端口上收到了优先级高的配置消息，即其将被选择为非指定端口时，这些端口的状态将被设置为侦听状态，不再转发报文（相当于将此端口相连的链路断开）。当在足够长的时间内没有收到更优的配置消息时，端口会恢复原来的正常状态。

3) 端口安全

端口安全（Port Security）的主要功能就是通过定义各种安全模式，让设备学习到合法的源 MAC 地址，以达到相应的网络管理效果。对于不能通过安全模式学习到源 MAC 地址的报文或 802.1x 认证失败的设备，当发现非法报文后，系统将触发相应特性，并按照预先指定的方式自动进行处理，减少了用户的维护工作量，极大地提高了系统的安全性和可管理性。

端口安全的特性包括：

NTK：NTK（Need To Know）特性通过检测从端口发出的数据帧的目的 MAC 地址，保证数据帧只能被发送到已经通过认证的设备上，从而防止非法设备窃听网

络数据。

Intrusion Protection：该特性通过检测端口接收到的数据帧的源 MAC 地址或 802.1x 认证的用户名、密码，发现非法报文或非法事件，并采取相应的动作，包括暂时断开端口连接、永久断开端口连接或是过滤此 MAC 地址的报文，保证了端口的安全性。

Device Tracking：该特性是指当端口有特定的数据包（由非法入侵，用户不正常上下线等原因引起）传送时，设备将会发送 Trap 信息，便于网络管理员对这些特殊的行为进行监控。

4) 防 IP 伪装

病毒和非法用户很多情况会伪装 IP 来实现攻击。伪装 IP 有三个用处：

- 本身就是攻击的直接功能体。比如 smurf 攻击。
- 麻痹网络中的安全设施。比如绕过利用源 IP 做的接入控制。
- 隐藏攻击源

设备防止 IP 伪装的关键在于如何判定设备接收到的报文的源 IP 是经过伪装的。这种判定的方式有三种。分别在内网和内外网的边界使用。

在 Internet 出口处过滤 RFC3330 和 RFC1918 所描述的不可能在内外网之间互访的 IP 地址。

- **利用 IP 和 MAC 的绑定关系网关防御**

利用 DHCP relay 特性，网关可以形成本网段下主机的 IP、MAC 映射表。当网关收到一个 ARP 报文时，会先在映射表中查找是否匹配现有的映射关系。如果找到则正常学习，否则不学习该 ARP。这样伪装 IP 的设备没有办法进行正常的跨网段通信。

- **接入设备防御**

利用 DHCP SNOOPING 特性，接入设备通过监控其端口接收到的 DHCP request、ACK、release 报文，也可以形成一张端口下 IP、MAC 的映射表。设备可以根据 IP、MAC、端口的对应关系，下发 ACL 规则限制从该端口通过的报文源 IP 必须为其从 DHCP 服务器获取的 IP 地址。

- **UPRF**

UPRF 会检测接收到的报文中的源地址是否和其接收报文的接口相匹配。其实现机制如下：设备接收到报文后，UPRF 会比较该报文的源地址在路由表中对应的出接口是否和接收该报文的接口一致。如果两者不一致，则将报文丢弃。

5) 路由协议认证

攻击者也可以向网络中的设备发送错误的路由更新报文，使路由表中出现错误的路由，从而引导用户的流量流向攻击者的设备。为了防止这种攻击最有效的方法就是使用局域网常用路由协议时，必须启用路由协议的认证。

另外，在不应该出现路由信息的端口过滤掉所有路由报文也是解决方法之一。但这种方法会消耗掉许多 ACL(Access Control List)资源。

9.4.5 防火墙部署

1) 状态防火墙

状态防火墙设备将状态检测技术应用在 ACL 技术上，通过对连接状态的的检测，动态的发现应该打开的端口，保证在通信的过程中动态的决定哪些数据包可以通过防火墙。状态防火墙还采用基于流的状态检测技术可以提供更高的转发性能，可以根据流的信息决定数据包是否可以通过防火墙，这样就可以利用流的状态信息决定对数据包的处理结果加快了转发性能。

2) 虚拟化技术

卫生信息平台的服务器种类较多，而且需要划分不同的安全区域。传统方式是在各区域服务器群前部署一台防火墙，由管理员或用户管理防火墙安全策略。造成了管理难度加大、网络拓扑混乱的问题。虚拟防火墙技术，则可以只用一台防火墙就能提供给多个区域独立使用，并分别管理。

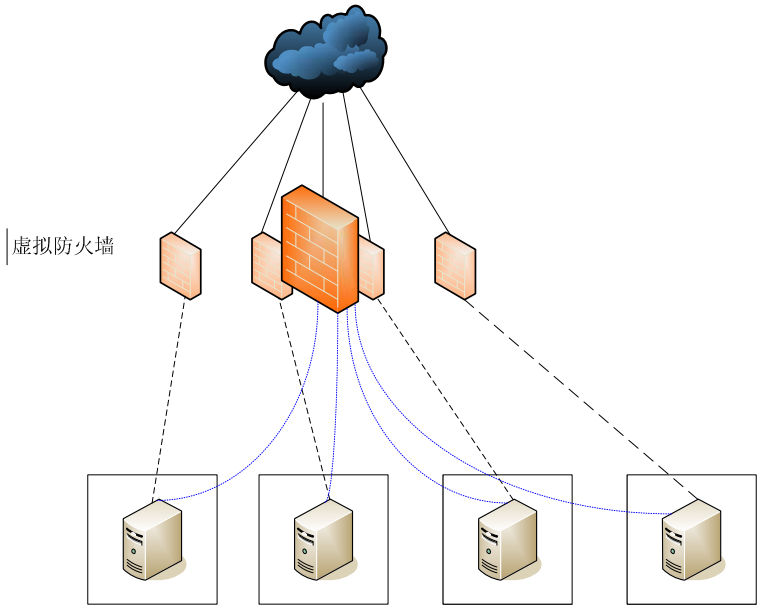


图 9-21 虚拟防火墙示意图

3) 防火墙安全区域管理

边界安全的一项主要功能是网络隔离，并且这种网络隔离技术不是简单的依靠网络接口来划分的，因为网络的实际拓扑是千差万别的，使用固定接口来进行网络隔离不能适应网络的实际要求。防火墙提供基于安全区域的隔离模型，每个安全区域可以按照网络的实际组网加入任意的接口，因此安全管理模型不会受到网络拓扑的影响。

业界很多防火墙一般都提供受信安全区域（trust）、非受信安全区域（untrust）、非军事化区域（Demilitarized Zone,DMZ）三个独立的安全区域，这样的保护模型可以适应大部分的组网要求，但是在一些安全策略要求较高的场合，这样的保护模型还是不能满足要求。

高级防火墙默认提供四个安全区域：trust、untrust、DMZ、local，在提供三个最常用的安全逻辑区域的基础上还新增加了本地逻辑安全区域，本地安全区域可以定义到防火墙本身的报文，保证了防火墙本身的安全防护，使得对防火墙本身的安全保护得到加强。例如，通过对本地安全区域的报文控制，可以很容易的防止不安全区域对防火墙本身的 Telnet、ftp 等访问。

4) 防火墙安全策略部署

对常见的网络攻击方式，如拒绝服务攻击（ping of death, land, syn flooding, ping flooding, tear drop）、端口扫描（port scanning）、IP 欺骗(ip spoofing)、

IP 盗用等进行有效防护；并提供 NAT(Network Adress Translation)地址转换、流量限制、用户认证、IP 与 MAC 绑定等安全增强措施。

防火墙可以部署在网络内部数据中心的前面，实现对所有访问数据中心服务器的网络流量进行控制，提供对数据中心服务器的保护。

设备部署模式：

建议在两台核心交换机与两台汇聚交换机之间配置两台防火墙，两台防火墙与两台核心交换机以及两台汇聚交换机之间采取全冗余连接。或在汇聚交换机上部署防火墙插卡；

为了保证系统的可靠性，我们建议配置两台防火墙为双机热备方式，在实现安全控制的同时保证线路的可靠性，同时可以与动态路由策略组合，实现流量负载分担；

安全控制策略：

- 防火墙设置为默认拒绝工作方式，保证所有的数据包，如果没有明确的规则允许通过，全部拒绝以保证安全；
- 建议在两台防火墙上设定严格的访问控制规则，配置只有规则允许的 IP 地址或者用户能够访问数据中心中的指定的资源，严格限制网络用户对数据中心服务器的资源，以避免网络用户可能会对数据中心的攻击、非授权访问以及病毒的传播，保护数据中心的核心数据信息资产；
- 配置防火墙防 DOS/DDOS 功能，对 Land、Smurf、Fraggle、Ping of Death、Tear Drop、SYN Flood、ICMP Flood、UDP Flood 等拒绝服务攻击进行防范，可以实现对各种拒绝服务攻击的有效防范，保证网络带宽；
- 配置防火墙全面攻击防范能力，包括 ARP 欺骗攻击的防范，提供 ARP 主动反向查询、TCP 报文标志位不合法攻击防范、超大 ICMP 报文攻击防范、地址/端口扫描的防范、ICMP 重定向或不可达报文控制功能、Tracert 报文控制功能、带路由记录选项 IP 报文控制功能等，全面防范各种网络层的攻击行为；
- 根据需要，配置 IP/MAC 绑定功能，对能够识别 MAC 地址的主机进行链路层控制，实现只有 IP/MAC 匹配的用户才能访问数据中心的服务器；

其他可选策略：

- 可以启动防火墙身份认证功能，通过内置数据库或者标准 Radius 属性认证，实现对用户身份认证后进行资源访问的授权，进行更细粒度的用户识别和控制；
- 根据需要，在两台防火墙上设置流量控制规则，实现对服务器访问流量的有效管理，有效的避免网络带宽的浪费和滥用，保护关键服务器的网络带宽；
- 根据应用和管理的需要，设置有效工作时间段规则，实现基于时间的访问控制，可以组合时间特性，实现更加灵活的访问控制能力；
- 在防火墙上进行设置告警策略，利用灵活多样的告警响应手段（E-mail、日志、SNMP 陷阱等），实现攻击行为的告警，有效监控网络应用；

启动防火墙日志功能，利用防火墙的日志记录能力，详细完整的记录日志和统计报表等资料，实现对网络访问行为的有效的记录和统计分析；

9.4.6 入侵防御/检测系统部署

1) 网络应用层攻击防御

今天，各种蠕虫、间谍软件、网络钓鱼等应用层威胁和 EMAIL、移动代码结合，形成复合型威胁，使威胁更加危险和难以抵御。这些威胁直接攻击数据中心核心服务器和应用，给业务带来了重大损失。需要部署应用层攻击防御/检测系统，避免恶意数据的侵犯。

2) 入侵防御/检测系统在数据中心的部署

入侵防御系统：建议在两台核心交换机与两台汇聚交换机之间配置两台入侵防御系统，两台入侵防御系统与两台核心交换机以及两台汇聚交换机之间采取全冗余连接。或在汇聚交换机上部署入侵防御系统插卡；

入侵检测系统：旁路连接核心交换机，将可以流量导入入侵检测系统一般进行检测。

9.5 网络管理

基于健康档案的区域卫生信息平台是一个综合性的城域网信息平台，且最大的特点是 POS 接入环境复杂。同时该信息平台对于业务的依赖性很强，因此在日常的运维管理过程中一方面要能够清晰掌握当前信息平台的整体运行情况，另一方面当发生一些问题时能够借用网络管理系统及时告警，协助运维人员快速定位故障和解决问题。

9.5.1 IP地址规划

9.5.1.1 IP地址规划原则

IP 地址规划应该是区域卫生信息平台网络建设整体规划的一部分，即 IP 地址规划要和网络层次规划、路由协议规划、流量规划等统一。通过合理的 IP 地址规划和划分到达提升网络性能、简化网络的管理和维护的目的。

区域卫生信息平台 IP 地址原则主要包括：

- 在 Internet IP 地址紧张的情况下，尽可能采用私有 IP 地址进行网络的地址规划，保证足够的网络地址可用空间；
- 地址分配是由业务驱动，按照接入单位的网络规模和业务量的大小分配各地的地址空间；
- IP 地址的规划与划分应该考虑到网络的后续规模和业务上的发展，能够满足未来发展的需要；
- IP 地址的分配需要有足够的灵活性，能够满足各种用户接入需要；
- IP 地址的分配必须采用 VLSM(Variable Length Subnet Mask，变长掩码)技术，保证 IP 地址的利用效率；
- 采用 CIDR(Classless Inter-Domain Routing)技术，这样可以减小路由器路由表的大小，加快路由器路由的收敛速度，也可以减小网络中广播的路由信息的大小；

依据和参照的标准和规范：

RFC 1366	《Guidelines For Management of IP Address Space》
RFC 1466	《Guidelines For Management of IP Address Space》
RFC 1597	《Address Allocation for Private Internets》

RFC 1918　　《Address Allocation for Private Internets》

RFC 0793　　《Transmission Control Protocol》

RFC 0791　　《Internet Protocol》

9.5.1.2 IP地址规划与设计

IP 地址规划应该是区域卫生信息平台网络建设是一个大型的城域网络，接入的单位数量众多，且大型单位中需要接入平台的主机数亦较多，因此建议每个区域卫生信息平台网络地址的使用范围采用 10.0.0.0/8 的私有地址范围，确保充足的地址空间来满足各单位的接入应用需求和未来网络的扩展性需求；同时根据网络分区的设计原则来划分子网，各区域之间通过三层路由协议互访；在每个区内部根据接入单位的数量和规模进一步划分子网。

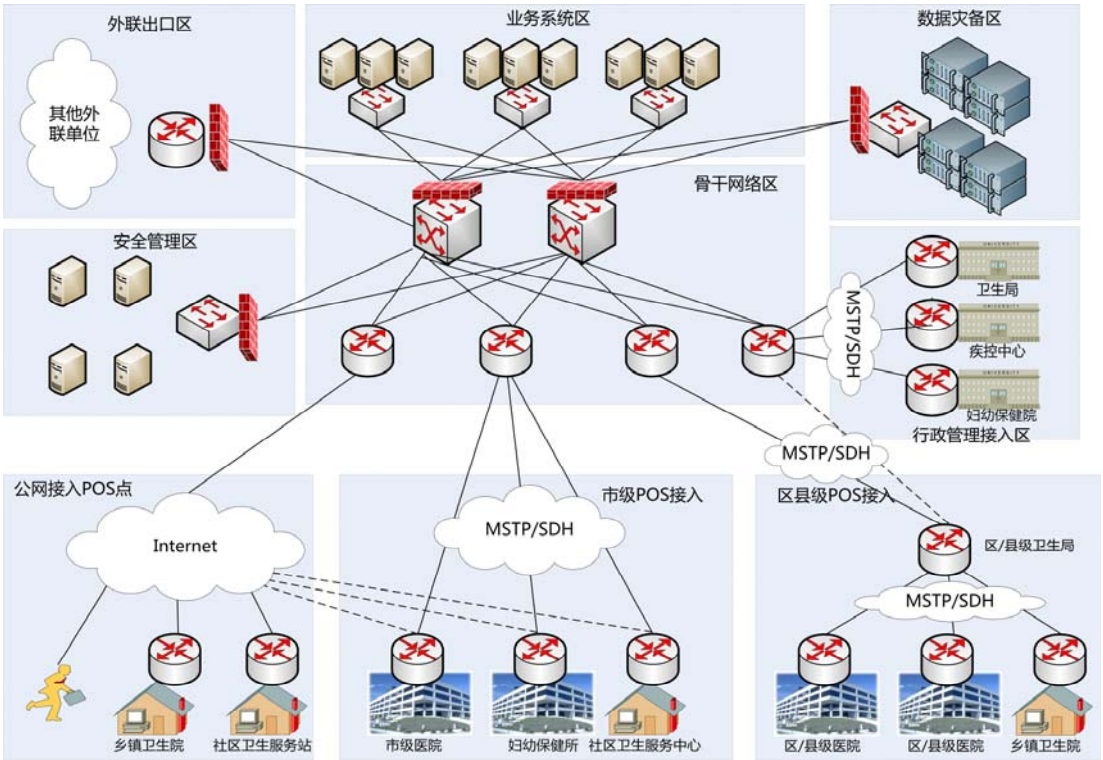


图 9-22 IP 地址设计图

结合区域卫生信息平台网络建设的整体模型以及各功能分区的对网络需求特点，现对 IP 的详细规划与设计做如下阐述：

1)．骨干网络区

此区域主要各分区之间的互连，网络运行时做路由的处理进而完成分区之间的数据转发， IP 地址主要是用来做三层设备的互联。因此，分配一个 B 类的地址

空间 10.0.0.0/16，两个三层设备之间的互连地址的子网掩码为 30。

2)．业务系统区

此区域主要是区域卫生信息平台内所有的应用服务器、数据库服务器、中间件服务器、数据存储设备等一切业务系统相关的设备的集中连接区域。因此，分配一个 B 类的地址空间 10.1.0.0/16，根据提供业务系统的用途和关联性在进一步划分子网。如：

业务系统种类	IP 地址
注册管理服务器	10.1.1.0/24
数据共享与交换管理器	10.1.2.0/24
EHR 的管理与服务器	10.1.3.0/24
…	…

3)．安全管理区

此区域主要是数据中心内保障整体信息平台安全、稳定运行的安全管理运维系统的连接区域。因此，分配一个 B 类的地址空间 10.2.0.0/16，根据管理的功能性需求进一步划分子网。如：

安全管理种类	IP 地址
网络管理类服务器	10.2.1.0/24
网络安全类服务器	10.2.2.0/24
身份认证、证书类服务器	10.2.3.0/24
…	…

4)．数据灾备区

此区域主要是业务系统及健康档案数据的灾备区域，因此，分配一个 B 类的地址空间 10.3.0.0/16，根据功能性需求进一步划分子网。如：

灾备应用种类	IP 地址
灾备中心办公区	10.3.1.0/24
灾备中心服务器	10.3.2.0/24
灾备存储设备	10.3.3.0/24
…	…

5)．外联出口区

此区域主要负责连接外联单位，如民政局、社保中心、公安局等。因此，分配一个 B 类的地址空间 10.4.0.0/16，根据部门数量和规模进一步划分子网。如：

外联单位	IP 地址

民政局	10.4.1.0/24
社保中心	10.4.2.0/24
公安局	10.4.3.0/24
…	…

6). 行政管理接入区

此区域主机负责将区域卫生信息平台的行政管理部门接入数据中心，因此，分配一个 B 类的地址空间 10.5.0.0/16，根据部门数量和规模进一步划分子网。如：

行政管理单位	IP 地址
卫生局	10.5.1.0/24
妇幼保健院	10.5.2.0/24
疾控中心	10.5.3.0/24
…	…

7). 公网 POS 接入区

此区域的 POS 点主要是小型 POS 点、离信息平台较远的 POS 点，因此规模不大，但数量众多。因此分配一个或多个连续的 B 类地址范围，每个接入点位的子网掩码为 27（每个 B 类地址范围最大可以满足 2048 个公网 POS 接入点，每个公网 POS 接入单位可以最大满足 30 台主机接入区域医疗信息平台），子网掩码也可以结合公网 POS 接入点的数量进行调整，在对应的上连骨干网络区的设备处作 IP 地址汇总和路由发布。如：

	接入单位	IP 地址
公网 POS 接入	社区服务站 1	10.10.0.0/27
	乡镇卫生院 1	10.10.0.32/27
	小型医院 1	10.10.0.64/27
	…	…

8). 市 POS 接入区

此区域的 POS 点主要是市区内大中型 POS 点，部分 POS 点像二、三级医院规模较大，因此分配的地址需容纳较多的主机数以满足正常的业务应用和日后的扩展性。因此分配一个或多个连续的 B 类地址范围，每个接入点位的子网掩码为 24（每个 B 类地址范围最大可以满足 256 个市 POS 接入点，每个市接入 POS 单位可以满足 254 台主机接入区域医疗信息平台），子网掩码也可以结合市 POS 接入点的数量进行调整，在对应的上连骨干网络区的设备处作 IP 地址汇总和路由发布。如：

	接入单位	IP 地址
市 POS 接入	三甲医院 1	10.20.1.0/24
	社区卫生服务中心 1	10.20.2.0/27
	二甲医院 1	10.20.3.0/27
	…	…

9)．区县级 POS 接入区

此区域的 POS 点主要是指以市为单位建区域卫生信息平台，区县级以下的医疗机构如乡镇卫生院、区/县级医院等单位，因此区县中每个 POS 点的网络规模中等，数量也不多，但是存在多个区县。因此，分配每个区县一个 B 类的地址范围，根据各区县内 POS 点的数量进行在近一步划分子网，如子网掩码设为 25（每个区县可以最大满足 512 个 POS 接入单位，每个 POS 单位可以满足 126 台主机接入区域医疗信息平台）。(如下图)

	接入单位		IP 地址
区县 POS 接入	区县 1	区县卫生局	10.30.1.0/25
		区级医院 1	10.30.1.128/25
		乡镇卫生院 1	10.30.2.0/25
		…	…
	区县 2	区县卫生局	10.31.1.0/25
		区级医院 1	10.31.1.128/25
		乡镇卫生院 1	10.31.2.0/25
		…	…
	…	…	…

9.5.1.3 域间互联IP地址规划

基于健康档案的区域卫生信息平台是国家卫生信息平台建设中最基础的建设单位，也是一期卫生信息平台主要建设的对象。当各区域卫生信息平台建设完毕后，将会在省级平台实现各区域卫生信息平台互连，进而统一连接到国家卫生信息平台，因此后续域间 IP 的地址规划需要考虑，并结合域间交互的应用对网络的需求特点，规划和部署合适的 IP 和域间互联技术。

区域之间需要交互的数据主要是居民的电子健康档案和电子病历等文档模板数据，因此数据量较小，且仅与业务系统中的部分服务器产生联系。因此，后期的域间互连建议从国家到省级平台进行完整的 IP 地址划分，再分给每个域一个地址空间，域内需要与上级进行数据交互的服务器和主机通过 NAT 转换的方式与上级单位互连。

9.5.2 路由选择与设计

9.5.2.1 路由协议选择

对路由协议的选择，考虑以下几个方面：

- 开放性和标准化：选择的城域网路由协议将不是设备厂商私有的路由协议，而是业界的标准协议，是众多设备厂商都支持的协议。
- 动态路由选择协议：区域卫生信息平台是一个大型的城域网络，需要选择部署动态的路由协议来实时地适应网络结构的变化，通过动态的更新、计算发布路由来满足网络高可用和简化网络的管理和维护。
- 可扩展性：目前，区域卫生信息平台设计有 9 个分区，选择的路由协议除了要能支持分区的网络划分，还要能够支持新增区的连入。
- 支持路由隔离：为防止局部路由振荡对整个区域卫生信息平台整个网络的影响，选择的广域网路由协议要能隔离不同层次的路由。
- 支持数据分流：集中式的设计架构会使业务系统区的流量负载较重，业务系统区的服务器和核心交换机有多条连接，选择的路由协议要能够支持数据分流，从而提高业务系统区提供服务的性能。

基于以上考虑的 5 方面，结合区域卫生信息平台网络采用以数据中心为核心的二层星型架构设计，在全网的路由策略选择设计时充分考虑最佳路由选择、路由快速收敛、区域划分等原则，在域内选择和部署 OSPF 动态路由选择协议。

9.5.2.2 路由协议的部署

域内全网采用 OSPF(Open Short Path First)协议，根据各分区的功能及面向的对象，将网络骨干区、业务管理区和安全管理区设为 Area0，集中的连接和向其他各区提供服务和网络里的支撑；其他分区依次定义为 Area1—Area N，分别与 Area0 相连，在汇聚的三层设备上做路由汇总。

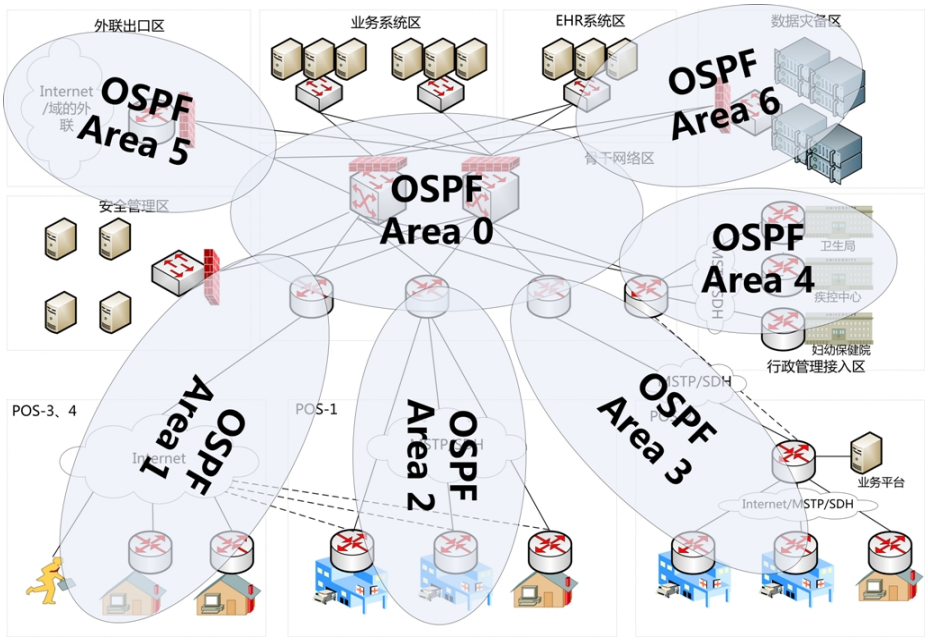


图 9-23 路由协议规划

9.5.2.3 域间路由规划

根据域间 IP 地址互连的规划，在省级平台将各域互连采用 OSPF 路由协议，通过 OSPF 的进程号来标识省级平台互连的网络，同时达到与下属区域卫生网络平台的路由无关性的目的。

省级卫生信息平台连接到国家卫生信息平台可以用 BGP(Border Gateway Protocol)路由协议,通过合理的划分 IP 地址和分配相应的 AS(Autonomous System)号码，通过将省级卫生平台的互连互通达到全国范围内的医疗卫生信息的数据共享和使用。

9.5.3 QoS设计

9.5.3.1 业务应用需求分析

由于最初 IP 协议设计时采用的逐跳的包转发模式，传统的 IP 网络是一种“尽力而为”的服务模型，如果一段网络发生拥塞，后续的 IP 包就可能被丢弃了，无法保证一些对时延、抖动等要求比较高的应用的服务质量。为了解决这个问题，引入了 QOS(Quality of Service)的概念。

IP QoS 的研究目标是有效地为用户提供端到端的服务质量控制或保证。QoS 就是网络单元（例如，应用程序，主机或路由器）能够在一定级别上确保它的业

务流和服务要求得到满足。QoS 并没有创造带宽，只是根据应用程序的需求以及网络状况来管理带宽。IP QoS 有一套性能参数，主要包括：

业务可用性：用户到 Internet 业务之间连接的可靠性。

传输延迟：指两个参照点之间发送和接收数据包的时间间隔。

可变延迟：也称为延迟抖动（Jitter），指在同一条路由上发送的一组数据流中数据包之间的时间差异。

吞吐量：网络中发送数据包的速率,可用平均速率或峰值速率表示。

丢包率：在网络中传输数据包时丢弃数据包的最高比率。数据包丢失一般是由网络拥塞引起的。

基于健康档案的区域卫生信息平台核心业务及对网络的应用需求对应如下：

表 9-7 业务应用需求特点及要求

业务类型	业务特点	数据对网络要求
文本类医疗 数据调阅	调阅诊疗记录 调阅诊疗处方明细 调阅检验检查报告 调阅病史等	数据量小 实时性高
文本类医疗数据采集	病人基本信息采集 病人诊疗信息采集	数据量小 实时性高
互联网服务	门诊预约 查询诊疗档案 网上医疗服务咨询	数据量小 实时性中
医学影像调阅	放射类影像 核医学类影像 超声影像 内镜影像	数据量大，定时上传
远程会诊	音视频交互	384Kbps-1Mbps 的通信带宽，对网络延时和抖动要求高

9.5.3.2 QoS技术设计

目前的 QOS 技术主要三种模型：Best-Effort 模型，IntServ 模型和 DiffServ

模型。

Best-Effort 模型：又叫尽力而为模型，,网络尽最大的可能性来发送报文,但对时延、可靠性等性能不提供任何保证 Best-Effort 服务是现在 Internet 的缺省服务模型。

IntServ 模型：集成服务模型,它可以满足多种 QoS 需求。这种服务模型在发送报文前,需要向网络申请特定的服务。应用程序首先通知网络它自己的流量参数和需要的特定服务质量 。

IntServ 模型的缺点：

1) 资源管理由路由器承担，增加了路由器的负担；

2) 在无连接的网络中，资源预留和分配很难实现；

3) 要求端到端所有的设备支持 RSVP(Resource Reservation Protocol，资源预留协议)信令协议，推广较困难；

DiffServ 模型：多服务模型，它可以满足不同的 QoS 需求。与 Integrated service 不同，它不需要信令，即应用程序在发出报文前，不需要通知路由器。对 Differentiated service，网络不需要为每个流维护状态，它根据每个报文指定的 QoS，来提供特定的服务。可以用不同的方法来指定报文的 QoS，如 IP 包的优先级位（IP Precedence），报文的源地址和目的地址等。网络通过这些信息来进行报文的分类、流量整形、流量监管和排队。

目前端到端的 QoS 主要是基于 DiffServ 模型的。

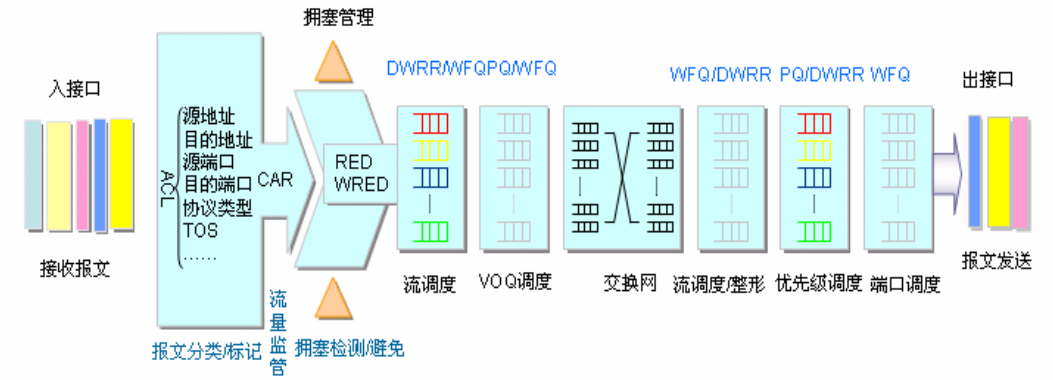


图 9-24 DiffServ QoS 技术体系

通过业务应用需求分析可知，区域医疗卫生信息平台上交互的数据所包括的业务种类多样，且每一种业务数据对网络的需求不一，合理的规划和部署拥塞管

理策略才能保证关键业务的正常运行；同时由于 POS 点的接入带宽的限制，拥塞避免和流量监管的是十分必要的；从而可以减少甚至避免网络抖动和关键业务的丢丢弃，进一步保证网络平台对应用平台的服务支撑。由此分析，DiffServ 模型是最适合区域医疗卫生信息平台上应用的 QOS 模型，根据业务对网络的需求特点制订如下队列策略：

表 9-8 业务网络需求特点

业务类别	业务	重要性	实时性	时延敏感性	流量	DSCP 定义	队列
网络管理类	网络控制	高	高	高	小	EF	LLQ
视频/语音类	远程会诊、远程教学、视频会议	高	高	高	大	EF	
文本类医疗数据调阅	调阅诊疗记录、诊疗处方明细、检验检查报告、病史等	高	高	中	小	EF	
互联网服务	门诊预约、查询诊疗档案、网上医疗咨询	高	中	中	小	AF31	CBWFQ
医疗影像类调阅	放射类影像 核医学类影像、超声影像、内镜影像等	中	中	中	大	AF21	
其他	其他生产、办公数据流	低	低	低	小	0	尽力而为

根据以上分析实施的 DiffServ 模型需要利用到的技术点现做介绍如下：

1)报文分类标记:

- 报文分类及标记是 QoS 执行服务的基础；
- 报文分类使用技术：ACL 和 IP 优先级（MF 五元组）；

- 根据分类结果交给其它模块处理或打标记（着色）供核心网络分类使用；

图 9-25 报文分类

2)拥塞避免(RED/WRED：随机早期检测/加权随机早期检测)：

- 通过采取随机丢弃的方式,避免传统的尾丢弃方式造成的 TCP 全局同步带来的流量传输波动；
- 可引入 IP 优先级,区分丢弃策略；
- 存在不丢弃、尾丢弃和随机丢弃三种处理方式；

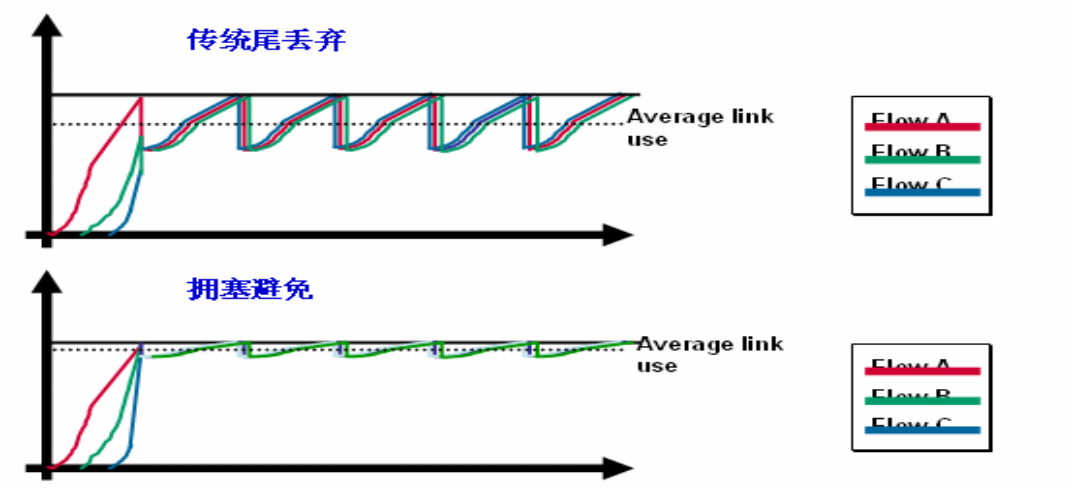


图 9-26 拥塞避免示意图

3)流量监管（CAR：约定访问速率)：

- 整形（shaping）对流量进行控制，输出的速率符合业务模型的规定
- 丢弃（droping）可根据设定规则丢弃分组
- 打标记（marking）设置报文的 DS 域（或 IP 优先级）

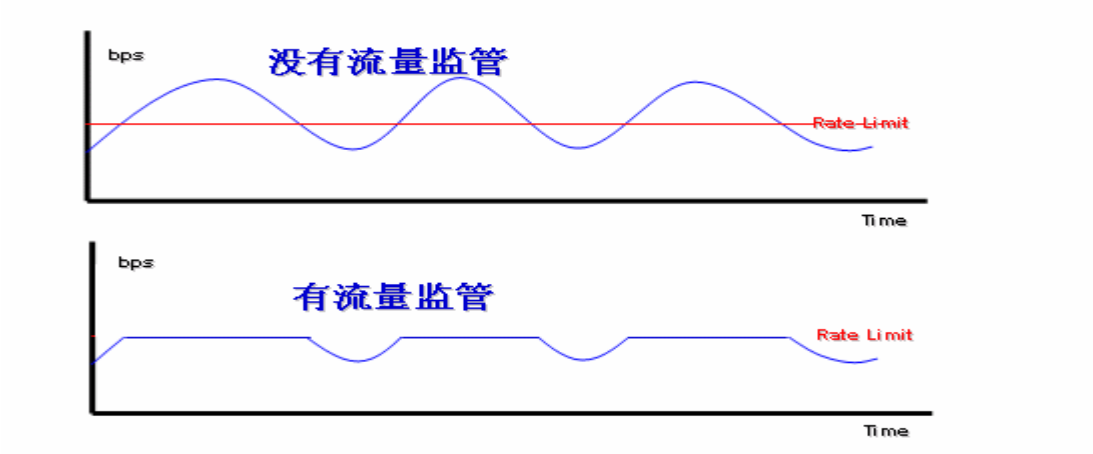


图 9-27 流量监管示意图

4)拥塞管理（队列机制）：

- 网络拥塞时，保证不同优先级的报文得到不同的 QoS 待遇，包括时延、带宽等；
- 将不同优先级的报文入不同的队列，不同队列将得到不同的调度优先级、概率或带宽保证；
- 算法： FIFO(First in,First out，先入先出)、PQ(优先队列)、CQ(Custom Queuing，自定义队列)、WFQ（Weighted Fair Queuing，加权公平队列） CBWFQ（Class Based WFQ ） LLQ（Lower Latency Queueing，低延迟队列） RTPQ （Real-time Transport Protocol Queue，RTP 队列）

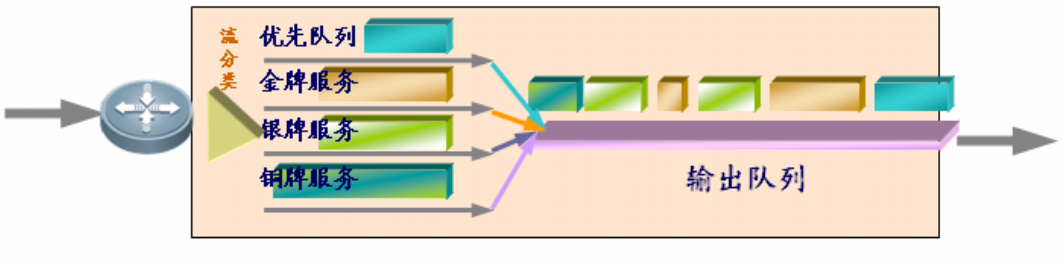


图 9-28 拥塞管理示意图

9.5.3.3 QoS的部署

1） 从业务系统区的出来的数据流，在接入层交换机处进行数据分类及 DSCP(Diffenenttiated Services Code Point，差分服务代码点)标记；

2） 核心节点交换机信任 DSCP 值，并部署流量监管和拥塞控制机制；

3） 网络骨干区与 POS 接入区和其他区域之间通过运营商的链路是带宽瓶颈产生的地方，开启队列技术和拥塞控制和管理等 QOS 功能；

4） 在各 POS 及其他区域各单位的出口设备上部署拥塞控制和流量监管机制；

9.5.4 网络设备管理

基于居民健康档案的区域卫生信息平台由于其业务的特殊性，信息平台的建设由市/区卫生管理机构负责组建，而对于各种 POS 来说只是平台的使用者。因此信息平台内所有的 IT 资源应采用集中式的管理模式，由统一的管理人员负责管理维护。同时区域卫生信息平台又是一个广域网环境的网络平台，因此在 IT 资源的统一管理方面需要进行整体、合理、有效的部署和实施。

区域卫生信息平台的网络 IT 资源主要包括：

信息平台可能涉及 IT 资源：三层交换机、二层交换机、VPN 网关、路由器、防火墙、IDS/IPS、Windows/Unix 服务器、数据库、中间件等 IT 资源。

POS 点可能涉及 IT 资源：防火墙、路由器、VPN 网关、Windows/Unix 服务器

网络 IT 资源的管理主要包括四个层面：网络规划管理、网络监控、故障管理、报表管理。

9.5.4.1 网络规划管理

网络规划管理主要是指信息平台及各 POS 接入所需的网络 IT 资源（非 POS 内部的原网络 IT 资源）能够实现在统一的界面进行直观的查看、管理，简化网管人员的管理难度。

1）. 网络 IT 资源发现

网络管理软件能够管理所有支持标准 SNMP 网管协议的网络设备，为多厂商设备共存的网络提供了统一的管理方式。

- 拓扑图自动发现多厂商设备；

利用网络管理软件能够自动发现平台中的 IT 资源，并自动生成相关联的拓扑图。并且网管人员能够在此基础上进行手工的添加、删除、修改，并标记资源的描述。

- 自动识别不同类型的设备

针对网络中的 IT 资源能够进行准确的识别和添加。主要包括：三层交换机、二层交换机、VPN 网关、路由器、防火墙、IDS/IPS、Windows/Unix 服务器、数据

库、中间件等 IT 资源、防火墙、路由器、VPN 网关等

- 可以对设备进行性能监视，包括接口的流量监视，利用率监视等；

能够根据不同类型的设备，定义其监控的主要参数。下表列出重点资源的监控参数描述，实际管理过程中可进行必要性选择。

表 9-9 重点资源的监控参数

资源类型	部件	指标中文描述
网络设备	接口	包含错误的输出包数
		接口丢弃的总包数
		接口包含的错误的总包数
		接口输入错误百分率
		接口输出错误百分率
		接口总流速
		接口流入速率
		接口流出速率
		接口输入丢包率
		接口输出丢包率
		带宽利用率
		该接口带宽
		接口流入量
		接口流出量
		接口总流量
		接收的字节数
		发送的字节数
		输入单播包数
		输出单播包数
		输入的非单播包数
		输出的非单播包数
		丢失的输入包数
		丢失的输出包数
		包含错误的输入包数
		由于定向到未知协议而被丢弃的包数
		输出队列中所有包数
网络设备	CPU	CPU 最近 1 分钟利用率
		CPU 最近 5 分钟利用率
		CPU 最近 5 秒利用率
	内存	内存利用率
主机（服务器）	CPU	CPU 利用率

	存储器	总空间
		利用率
		已用空间
		请求失败次数
	进程	CPU 占用率
		内存占用大小
	硬盘	设备发生的错误数
		磁盘容量
数据库	库信息	数据库日志使用率
		数据库日志缓冲命中率
		数据库数据文件的大小
	服务器信息	缓冲区池保留的页的数目
		发生的网络数据包错误数
		锁的动态内存总量
		当前动态内存总量
		动态内存总量
		SqlServer 数据库活动事务数
		SGA 缓冲池大小
		CPU 使用率
		缓存命中率
		支持的最大连接数
		执行输入和输出操作的时间
		Cpu 的工作时间
		每秒的探测扫描数
		每秒索引搜索数
		所有可用列表页总数
		每秒所发出的物理数据库页写入的数目
		每秒发出的物理数据库页读取数
		写到网络上的输出数据包数
		每秒大容量复制的行数
		每秒要求调用者等待的锁请求数
		每秒导致死锁的锁请求数
		当前用户连接数
		读取磁盘的次数
		写入磁盘的次数
		数据库闲置时间
		从网络上读取的输入数据包数目

IIS		当前连接数
		HTTP404 总错误连接数
		服务的 I/O 带宽
中间件	服务端口信息	当前线程数
		请求命中率
	应用程序信息	活动会话数
		平均会话在线时间
	JVM	内存利用率

• 可以接收设备告警，并进行告警信息显示。

在监控设备的同时，根据设备的运行状态进行有效评估，设定合理的告警阀值，当设备故障或某参数达到指定阀值后，能够自动进行告警，使网管人员及时掌握告警信息。告警方式主要有：终端显示告警、日志告警、邮件告警、短信平台告警。

2)．网络拓扑管理

网络管理软件提供统一拓扑发现功能，实现本项目全网监控，可以实时监控所有网络和安全设备的运行状况，并根据网络运行环境变化提供合适的方式对网络参数进行配置修改，保证网络以最优性能正常运行。

• 全网设备的统一拓扑视图，拓扑自动发现，拓扑结构动态刷新；

• 可视化操作方式：拓扑视图节点直接点击进入设备操作面板；

• 在网络、设备状态改变时，改变节点颜色，提示用户；

• 对网络设备进行定时（轮询间隔时间可配置）的轮询监视和状态刷新并表现在网络视图上；

• 拓扑过滤，让用户关注所关心的网络设备情况；

• 快速查找拓扑对象，并在导航树和拓扑视图中定位该拓扑对象。

9.5.4.2 网络监控

1)．网络流量与带宽管理

网管系统应提供丰富的性能管理功能，同时以直观的方式显示给用户。通过性能任务的配置，可自动获得网络的各种当前性能数据，并支持设置性能的门限，当性能超过门限时，可以以告警的方式通知网管系统。通过统计不同线路、不同

资源的利用情况，为优化或扩充网络提供依据。

2)．服务器性能监控

服务器是基于健康档案的区域卫生信息平台中的重要组成部分，通过服务器监视管理系统，实现对服务器与设备的统一管理。

- 支持对 CPU、内存资源消耗的监视；
- 支持对硬盘使用情况的监视；
- 支持运行进程的资源监视；
- 支持对服务的资源监视；

9.5.4.3 故障管理

故障管理主要功能是对全网设备的告警信息和运行信息进行实时监控，查询和统计设备的告警信息。

- 告警实时监视，提供告警声光提示；
- 支持告警转到 Email 或手机短信；
- 支持告警过滤，让用户关注重要的告警，查询结果可生成报表；
- 支持告警拓扑定位，将显示的焦点定位到选定告警的拓扑对象；
- 支持告警相关性分析，包括屏蔽重复告警、屏蔽闪断告警等

9.5.4.4 报表管理

网络管理系统够针对 IT 资源的监控参数，根据管理人员的要求制定周期性的参数监控并产生相应的报表。从而使网管人员能够根据报表数据进行有效的分析，优化 IT 资源的使用、更新、维护。

报表主要包括二种类型：

- 实时性报表：当前设备的运行状态下，针对特定参数生成相应的报表清单。如当前网络平台所有在线的 IT 资源列表。
- 周期性报表：针对某类或某类特定设备或资源参数，按照一定的时间周期进行参数变化跟踪，从而进行有效分析，以便于排除故障或优化资源。如，将核心交换机 1 天内的 CPU 占用率走势图产生报表进行分析能够准确判断出每天业务繁忙程度的时间规律。

9.5.4.5 网络设备配置、更新

因为区域卫生信息平台规模庞大，设备繁多，网络管理员的配置文件管理工

作将十分繁重，如果没有好的配置文件维护工具，网络管理员就只能手动备份配置文件。这样就给网络管理员管理、维护网络带来一定的困难。

网络配置中心支持对设备配置文件的集中管理，包括配置文件的备份、恢复以及批量更新等操作，同时还实现了配置文件的基线化管理，可以对配置文件的变化进行比较跟踪。

9.5.5 IT服务管理

9.5.5.1 统一集中服务

区域医疗信息化应用，关乎每个百姓的切身，这势必导致对它的日常基础运营管理提出高的要求，因为它是业务连续性、系统整合、应用服务的基础，而同时区域医疗信息化的点分布又分散，对其的管理也将会困难，这就需要一种统一的集中服务。

对于 IT 管理来说，期望能够统一集中服务承载着多个业务系统的 IT 基础架构，实现全局管理、统一监控、统一报表和统一规划，以降低分散管理的复杂性。从而提升可用性、缩短故障排除时间，减轻总体管理负担。

从发展阶段的角度可以清楚地看出，未来 IT 运维管理之路是有章可循的：首先一定是服务管理，其中服务支持流程主要面向用户（End-Users），用于确保用户得到适当的服务以支持组织的业务功能，确保 IT 服务提供方（Provider）所提供的服务质量，符合服务级别协议（Service Level Agreement，SLA）的要求。

服务提供流程主要面向为服务付费的机构和个人客户（Customer）。它的任务是根据组织的业务需求，对服务能力、持续性、可用性等服务级别目标进行规划和设计，同时还必须考虑到实现这些服务目标所需要耗费的成本。也就是说，在进行服务提供流程设计时，必须在服务级别目标和服务成本之间进行合理的权衡。由于这些管理流程必须解决“客户需要什么”、“为满足客户需求需要哪些资源”、“这些资源的成本是多少”、“如何在服务成本和服务效益（达到的服务级别）之间选择恰当的平衡点”等问题。

另外就是 IT 服务管理的发展是沿着设备管理（Networking and System Management，NSM），IT 服务流程管理（IT Service Management, ITSM），业务服务管理（Business Service Management, BSM）的路线不断进步和发展。前两个阶段是 BSM 的基础，而 BSM 是在传统的系统和网络管理的基础上发展而来的，是

对 NSM 和 ITSM 的扩展。其目标与 ITSM 有重叠的部分，例如提高 IT 服务质量，降低运营成本等。

未来 IT 应用成熟度会不断提高，面我们在业务上对 IT 系统的依赖性也会越来越强，甚至会成为业务流程的核心部分，是某些业务赖以运行的基础。所以我们一定要先把 IT 基础设施建立管理起来，建立统一的服务管理之后，再来细化考虑它与业务的目标一致，从而实现 IT 服务应对业务需求做出更快速的反应。

9.5.5.2 服务业务的响应

在日常运营过程中，我们须要实际而有效的响应，来完成我们的服务，这关系一切相关服务活动的展开，这里我们想重点提出服务台的概念，因为它是一个经常被采用的有效的方式，我们可以通过这种方式对服务业务做出快速的响应。如果建立服务台，它将是卫生局与外界进行联络的第一道窗口；而以兼顾效率和效果的方式 针对客户疑难问题及关注事项做出回应则有助于公司声誉的持续改善。对于分散在不同地理位置开展独立工作的技术支持团队成员来说，服务台还将成为他们保持卫生局性和协调性的“前沿阵地”。

1） 服务台概述

服务台的一大优势表现为，它是目标客户与技术服务专家进行联络的单一接合点。它为各分散的繁忙人员提供了一个快捷有效的解决方案，而一些不起眼的事情往往关乎区域医疗的成败。

2） 目的与目标

明确界定服务台的用途和目标并将其记录在案具有至关重要的意义。编制任务说明或明确界定支持提供途径属于实现上述目标的一种方法。

在计划阶段及早明确项目意图可确保全体团队成员围绕公司既定目标开展密切协同。考虑到企业希望通过服务台提供的服务类型各不相同，因此，上述目标可能取决于卫生局机构规模和服务台既定职能范畴等众多因素。现举例说明某些服务目标：

- 在用户与 IT 部门之间提供单一、集中联络点。
- 为用户提供通往其它服务管理职能（如变更管理、问题解决、配置管理和发布管理等）的切入点。
- 提交实现业务目标所需高质量支持服务。

- 辨别并压缩 IT 服务总体拥有成本（Total Cost of Owership，TCO）。
- 跨越业务、。技术和过程界限为变更提供支持。
- 提高客户满意程度。
- 保持客户忠实度。
- 发现更多商业机遇

3） 关键定义

- 呼叫。 呼叫是由客户通过一切通信手段（包括电话、电子邮件、语音邮件等）向服务台发出的联络信息。
- 事故。事故指不属于标准服务运转范畴并可能导致服务中断或服务质量下降的问题。
- 重大事故。重大事故指具有严重影响或可能导致严重影响的事故，通常需要采取超出一般事故的应对措施。重大事故往往在企业间协作、管理升级、资源机动和联络改进等方面提出更高要求。
- 服务请求。服务请求是针对新增或变更服务提出的调用需求。不同卫生局机构可能提出不同类型的服务请求，但常规服务请求无外乎变更请求（RFC）、信息请求（RFI）和服务扩展等。
- 问题。 问题是导致一或多次事故却未经查明的根源。
- 已知错误。已知错误是指已查明根源并找到权宜之计或永久替代方案的事故或问题。业务问题一旦出现，变更请求（RFC）就会产生，但它无论如何都属于已知错误——除非已被某项变更修复。
- 应对方案。 应对方案是为确保常规服务得到恢复而对特定事故加以排除的已知手段；当然，这种手段将首先解决引发事故的问题。

4） 服务台结构

我们可通过集中方式在卫生局机构范围内营造服务台。我们必须在项目计划阶段内确定所需运用的服务台结构。

- 集中式服务台

表 9-10 集中式服务台特点

服务台类型	要求	工具	优势

服务台类型	要求	工具	优势
集中式服务台可为广泛分布在不同地理位置的全体企业用户提供支持。	清晰的卫生局领导脉络和紧密衔接的伺服任务。	允许用户通过单键拨号呼叫服务台的电话系统。	用户清楚地知道向哪里请求支持。

- 服务台建设建议

基本建设：

其一，设立固定的组织，明确人员与职责；

其二，与固定合作伙伴签定相关服务协议；

其三，设定统一的服务电话、邮箱；

其四，装备有关的运营监控软件。

深入建设 1：

其一，建立服务网站；

其二，建立联络中心，将各种通信模式统一，并将服务过程进行记录；

其三，应用工作流程管理管理软件。

深入建设 2：

其一，建立 E－learning 平台，进行人员能力提升；

其二，建立 KM，管理支持报务所须的问题知识；

其三，与其它的业务应用进行集成。

9.5.5.3 问题解决服务

区域医疗将会遇到影响或可能影响业务正常运作的问题。因为区域医疗的业务将日益依赖 IT 服务，迅速和有效地对负面影响 IT 服务或基础结构的任何问题做出反应的需要变得极为重要。

问题解决是非常关键的，它为卫生局提供首先检测问题然后准确确定正确的支持资源以便尽快解决问题的能力。该流程还为管理层提供关于影响卫生局的问题的准确信息，以便他们能够确定必需的支持资源，并为支持资源的供给做好计划。

通过利用问题解决流程，卫生管理部门能够确保他们的服务支持资源集中在

最紧迫并且可能对业务产生最大影响的问题上。如果没有该流程提供的控制和管理信息，卫生管理部门将无法确保他们在 IT 支持方面的投入是否真正满足其目标。

问题解决的主要优点有：及时解决问题，从而最小化业务影响；改善对支持资源的利用；更好地理解问题对 SLA 指标的影响，从而允许改进优先顺序；关于正在发生的问题的准确信息；消除“遗漏”的问题和服务请求。

1). 问题解决概述

问题解决流程旨在确保检测到问题，然后记录服务请求。记录确保没有遗漏的问题或服务请求，允许记录得到跟踪，并提供帮助问题解决和活动计划的信息。该流程包括利用技术向客户提供自助服务的功能，为他们提供到支持功能的灵活和方便的接口，同时还降低支持服务台的工作负担和人员要求。

问题经过分类以确保为它们安排正确的优先顺序并发送到正确的支持资源。问题解决包括初始支持流程，这些流程允许根据已知的错误和问题检测新的问题，以便能够快速定位任何以前确定的解决办法。

然后问题解决提供一个可以调查、诊断、解决并终结问题的结构。该流程确保问题在整个生命周期中得到控制、跟踪和监视。

有时可能会发生需要超出常规问题流程所提供的反应的重大问题。问题解决包含用于处理这些重大问题的流程，包括管理和功能上报、有效的沟通和正式的回滚计划。

2). 目的与目标

问题解决的主要目标是尽快恢复正常服务运作，并最小化对业务运营的的负面影响，从而确保维持良好的服务质量和可用性级别。正常服务运作被定义为服务级别协定 (SLA) 限制内的服务运作。

3). 问题解决的目标包括：

- 尽快恢复正常服务。
- 最小化问题对业务的影响。
- 确保一致地处理问题和服务请求而不会有任何遗漏。
- 定向到最需要的支持资源。
- 提供允许优化支持流程、减少问题数量和执行管理计划的信息。