|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |
| 河南省医疗保障业务专网建设方案 |
| **河南省医疗保障局**  **2020年4月** | | |

目 录

[1 设计概述 1](#_Toc36662461)

[1.1 医疗保障业务专网简介 1](#_Toc36662462)

[1.1.1 概述 1](#_Toc36662463)

[1.1.2 术语和定义 1](#_Toc36662464)

[1.1.3 参考规范 2](#_Toc36662465)

[1.1.4 接入网络技术要求 2](#_Toc36662466)

[1.1.5 接入方式选择 3](#_Toc36662467)

[1.2 网络现状 3](#_Toc36662468)

[1.3 设计目标 3](#_Toc36662469)

[2 总体架构 5](#_Toc36662470)

[2.1 纵向网络连接 7](#_Toc36662471)

[2.2 横向网络连接 8](#_Toc36662472)

[2.3 远程办公接入 9](#_Toc36662473)

[3 网络规划设计 10](#_Toc36662474)

[3.1 网络架构设计 10](#_Toc36662475)

[3.2 承载网络规划设计 14](#_Toc36662476)

[3.2.1 链路指标要求 14](#_Toc36662477)

[3.2.2 链路带宽要求 15](#_Toc36662478)

[3.2.3 链路连接方式要求 15](#_Toc36662479)

[3.3 IPv4、IPv6双栈运行方案 15](#_Toc36662480)

[3.4 SDN部署 16](#_Toc36662481)

[3.4.1 全局流量优化 16](#_Toc36662482)

[3.4.2 网络精细化管理 17](#_Toc36662483)

[3.4.3 运维效率提升 17](#_Toc36662484)

[3.5 SRv6部署 17](#_Toc36662485)

[3.5.1 SR技术 17](#_Toc36662486)

[3.5.2 SRv6优势 18](#_Toc36662487)

[3.5.3 SRv6应用效果 18](#_Toc36662488)

[3.6 无线接入VPDN设计 19](#_Toc36662489)

[3.6.1 VPDN组网方式 19](#_Toc36662490)

[3.6.2 国密加密算法 19](#_Toc36662491)

[3.7 网络可靠性设计 20](#_Toc36662492)

[3.7.1 设备可靠性 20](#_Toc36662493)

[3.7.2 链路可靠性 21](#_Toc36662494)

[3.7.3 故障检测 21](#_Toc36662495)

[3.8 骨干网流量设计 22](#_Toc36662496)

[3.8.1 骨干网流量分析 22](#_Toc36662497)

[3.8.2 骨干网流量Qos划分 22](#_Toc36662498)

[3.9 网络性能和质量监测设计 24](#_Toc36662499)

[4 安全体系设计 25](#_Toc36662500)

[4.1 安全保障体系建设 25](#_Toc36662501)

[4.2 网络建设的安全性要求 25](#_Toc36662502)

[4.2.1 横向接入区安全 25](#_Toc36662503)

[4.2.2 安全运维区 26](#_Toc36662504)

[4.3 平台管理的安全性要求 29](#_Toc36662505)

[4.4 网络接入安全 29](#_Toc36662506)

[4.4.1 终端安全 29](#_Toc36662507)

[4.4.1.1 内部用户终端要求 30](#_Toc36662508)

[4.4.1.2 外部用户终端 31](#_Toc36662509)

[4.4.2 身份认证安全 32](#_Toc36662510)

[4.4.3 防火墙接入安全 32](#_Toc36662511)

[4.4.3.1 远程接入安全配置要求 32](#_Toc36662512)

[4.4.3.2认证、授权安全配置要求 32](#_Toc36662513)

[4.4.3.3 日志服务安全配置要求 32](#_Toc36662514)

[4.5 等级保护建设规划 33](#_Toc36662515)

[4.5.1 行业安全等保建设背景 33](#_Toc36662516)

[4.5.2 等级保护要求 33](#_Toc36662517)

[4.5.3 等级保护流程 34](#_Toc36662518)

[5 机房建设规划 35](#_Toc36662519)

[6 方案组件与选型建议 36](#_Toc36662520)

[6.1 省级方案组件与选型建议 36](#_Toc36662521)

[6.2 市级方案组件与选型建议 43](#_Toc36662522)

[6.3 县（区）级方案组件与选型建议 48](#_Toc36662523)

[7 项目实施方案 50](#_Toc36662524)

[7.1 实施计划与内容 50](#_Toc36662525)

[7.2 项目建设实施方案 51](#_Toc36662526)

[7.2.1 系统架构设计 51](#_Toc36662527)

[7.2.2 安装实施服务 51](#_Toc36662528)

[7.2.3 项目实施保障 54](#_Toc36662529)

[7.2.4 应急预案及措施 54](#_Toc36662530)

[8 网络运维设计 56](#_Toc36662531)

[8.1 网管基本功能设计 56](#_Toc36662532)

[8.2 运行维护建设要求 58](#_Toc36662533)

[8.2.1 运维服务概览 58](#_Toc36662534)

[8.2.2 运维服务内容 60](#_Toc36662535)

[8.2.3 驻场服务工作内容 61](#_Toc36662536)

[8.2.4 质保内容 61](#_Toc36662537)

[8.2.5 培训内容 61](#_Toc36662538)

[9 域名规划 62](#_Toc36662539)

[10 IP地址规划 63](#_Toc36662540)

[10.1 接入地址分配 63](#_Toc36662541)

[10.2 设备互联地址分配 64](#_Toc36662542)

[10.3 Loopback地址分配 65](#_Toc36662543)

[11 路由配置方案 67](#_Toc36662544)

[11.1 GRE穿越政务外网实施方案 67](#_Toc36662545)

# 设计概述

## 医疗保障业务专网简介

### 概述

根据国家医疗保障局《医保核心业务网网络安全接入规范》，医保核心业务网作为支撑医保业务工作的专用网络，为非涉密网络，禁止存储和处理涉密数据，信息安全等级保护级别为三级。医保核心业务网与医保公共服务网之间需要实现自动数据交换的，应采用安全隔离与信息交换系统。

### 术语和定义

医保核心业务网：医保核心业务网是连接各级医保部门的大型网络系统，是国家医保信息系统的运行基础，是各级医保部门开展业务工作及内部办公管理工作的重要支撑。

医保公共服务网：医保公共服务网是与互联网逻辑隔离的内部局域网络，是各级医保部门为本级内部用户提供互联网接入服务，并通过互联网向社会公众提供医保信息和医保业务服务的网络。

定点（协议）医药机构 ：定点医药机构是定点医疗机构和定点零售药店的统称。定点医疗机构是指与医疗保障经办机构签订服务协议，为参保人提供医疗服务的医疗机构。定点零售药店是指与经办机构签订服务协议，为参保人提供处方外配和非处方药等零售服务的药店。

信息资源共享部门 ：信息资源共享部门是指与医保部门有信息资源共享和数据交换需求的单位，如人社、卫健、民政、公安、财政、税务等。

纵向连接：纵向连接是指在医保系统内部建立的由国家医疗保障局到省、市、县（区）的纵向网络连接。

横向连接：横向连接是指各级医保核心业务网与同级人社、卫健、民政等部门，以及定点医院、定点药店、商业银行、保险公司等单位之间的网络连接。

安全隔离与信息交换系统：安全隔离与信息交换系统，是外部单位与医保部门进行数据交换或在医保内部不同安全等级的网络之间进行数据交换的处理系统。该系统由网闸设备和数据交换系统（交换服务器或文件服务器）组成。

远程办公：远程办公是指医保内部用户在医保核心业务网覆盖范围外，通过医保部门提供的安全接入方式，远程连接到医保核心业务网进行办公的场景。

点对网连接模式：接入单位只将单个用户或者与其单位网络物理隔离的小型局域网连接到医保核心业务网。

网对网连接模式：接入单位将其单位内部网络按照一定的安全保障措施连接到医保核心业务网。

### 参考规范

下列文件对于本文的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。

凡是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/T 25069-2010 信息安全技术术语
* GB/T 22080-2016 信息技术安全技术信息安全管理体系要求
* GB/T 22081-2016 信息技术安全技术信息安全管理实用规则
* GB/T 22239-2008 信息安全技术信息系统安全等级保护基本要求
* GB/T 25070-2010 信息安全技术信息系统等级保护安全设计技术要求国家电子政务外网安全接入平台技术规范

### 接入网络技术要求

**接入方式**：依据医保业务需求和核心业务网特点，结合当前广域网、城域网组网技术，医保系统纵向和横向网络连接主要采用以下方式：

**专线**：专线是指在广域或城域连接中使用光纤，或者租用运营商SDH/MSTP、DWDM链路、PTN等进行互联的专用线路。xDSL等其他接入方式不属于专线。

**电子政务网络**：电子政务网络是指国家电子政务外网和各级党政部门已建成的非涉密网。

**MPLS VPN 网络**：MPLS VPN网络是指运营商利用MPLS（多协议标签交换） VPN技术提供的网络服务，安全性、可靠性低于专线。

**VPDN 网络**：VPDN虚拟专用拨号网是运营商基于L2TP等技术为客户提供的一种相对可控的网络接入方式。这种接入方式可以提供对终端的认证功能，数据经过隧道传输。 VPDN方案的终端接入方式可以采用有线接入，也可以采用4G/5G无线接入。

### 接入方式选择

医保核心业务网接入用户分为医保系统内用户和外部用户，医保系统用户主要通过纵向网络接入，完成医保系统内部上下级之间的网络连接，可通过专线或电子政务网络等方式实现；外部用户包括人社、卫健、民政、公安、税务、其他信息资源共享部门，以及定点医院、定点药店、商业银行、保险公司等，主要通过横向网络接入，完成与医保核心业务网的网络连接，通过专线、电子政务网络、MPLS VPN、GRE、SRv6、VPDN等方式实现；此外内部用户在出差或者外出时，需要远程接入医保核心业务网进行远程办公。对不同的接入用户和接入方式，应在线路安全、边界安全、数据安全、访问控制等方面采取对应的措施。

## 网络现状

省级医疗保障网络多由人社原有网络组成，尚不能发挥整体多业务融合、高可靠及大带宽作用，各级医疗保障机构、各转隶单位在有线网络方面的建设与通信水平不一，整体医保业务通信保障能力偏弱。部分单位通过电子政务外网线路分别与各省市县医疗保障单位、医疗保险中心、药采中心等、政府等相联接，进行公文收发、业务处理、视频会议等，在遇到突发事件或信息高峰期时，跨部门、跨层级大协同无法保障。

## 设计目标

根据《全国医疗保障系统核心业务区骨干网络建设指南》纲要，结合河南省具体需求，坚持“打基础、提能力”的思路，采用SDN、IPv6等先进组网技术，构建健壮网络架构，建设覆盖省医疗保障局、18个地市医疗保障局以及区县医疗保障局的互联互通及安全保障。满足医疗保障业务大容量信息数据传输、业务经办、医保结算、融合视频会议等多类关键业务承载需求。

**提升网络能力：**全面支持IPv4与IPv6双栈运行，提供协议转换能力，实现互联互通。

**保障网络可靠**：在节点设置、路由方案、链路保护等方面为医保业务提供安全可靠的保护方案，逐步推进市级和县级节点采用双链路上联到上级网络节点，提高网络可靠性。

**强化网络管理**：前瞻性采用先进的SDN等技术，强化资源的综合管理和深度挖潜，实现基于带宽资源及低时延需求的灵活调度，保障业务的快速开通及智能运维。

**边界清晰：**省、市级建立安全接入区，采取相应控制措施，保证核心业务网络横向接入的边界可控，与其他网络、终端等的数据交换安全可控。

医保核心业务专网设备需采用具备大带宽、弹性扩容、高可靠、易运维、SLA保障、绿色节能、安全可信的国产高端核心路由器，平台能力足够支撑未来5年以上的发展。要求设备预留足够槽位数量，可以平滑扩容增加单板，支持GE、10GE、40GE、100GE端口平滑扩容，支持SDN，IPv6，SRv6新技术，具备板卡冗余保护能力。设备端口数量根据各地实际业务需求配置，冗余数量不低于50％。

# 总体架构

医保核心业务专网通信网络概念图如下所示：

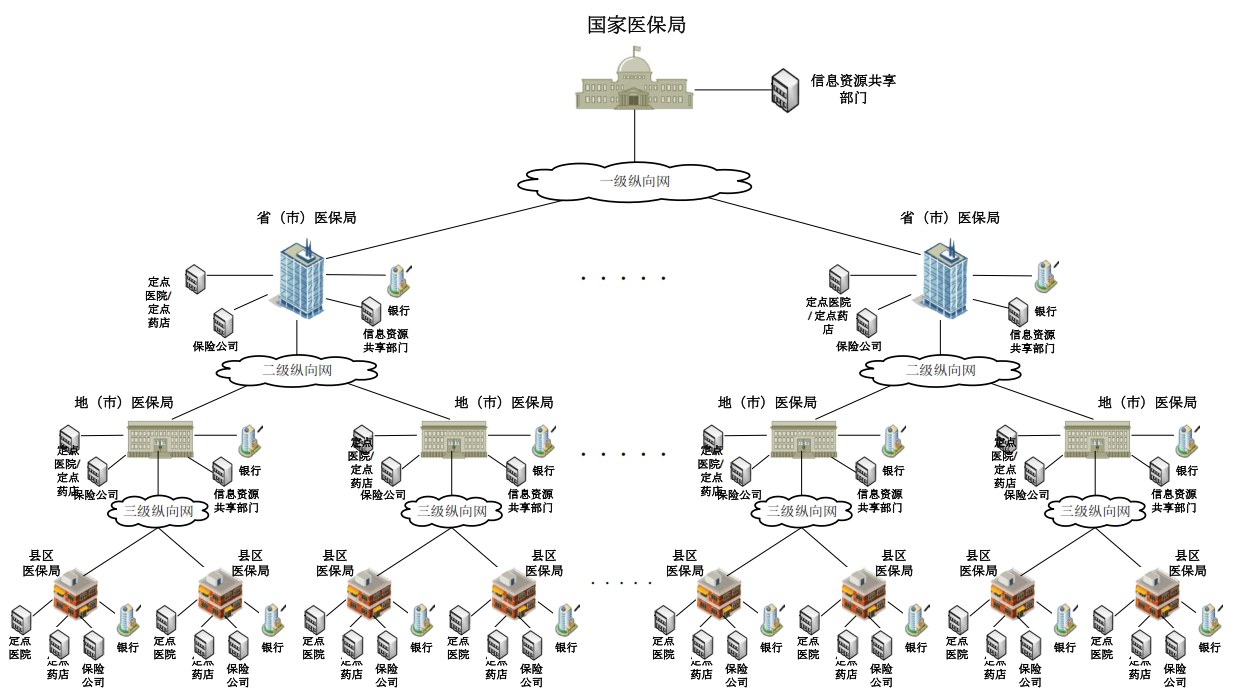


图2‑1医保核心业务专网网络拓扑结构图

医保核心业务专网采用树形网络结构为主，纵向主要由各级医保部门按垂直的上下级模式连接成广域骨干网络，由国家医疗保障局连接全国各省级医保局，并向下覆盖到市、县（区）医保部门；横向以各级医保部门为中心向同级信息资源共享部门等辐射，并与定点医院、定点药店、银行、保险公司等相关单位连接，形成该级的城域接入网。各单位通过点对网连接模式或网对网连接模式横向连接到医保核心业务网。

医保纵向网络涵盖国家医疗保障局、省、市医保部门，国家医疗保障局到各省级医保部门的网络构成一级纵向骨干网，省级医保部门到各市医保部门构成二级纵向骨干网。

医保横向网络分为国家医疗保障局接入网络、省级医保接入网络、市级接入网络，分别与本级的人社、卫健、民政、公安、税务等部门，以及定点医院、定点药店、商业银行、保险公司等有关外部单位进行网络互接，按照医保业务需要，定点医院、定点药店、商业银行、保险公司也可以省级或者市级网络为统一节点进行网络互接。各区域业务逻辑连接图如下所示：

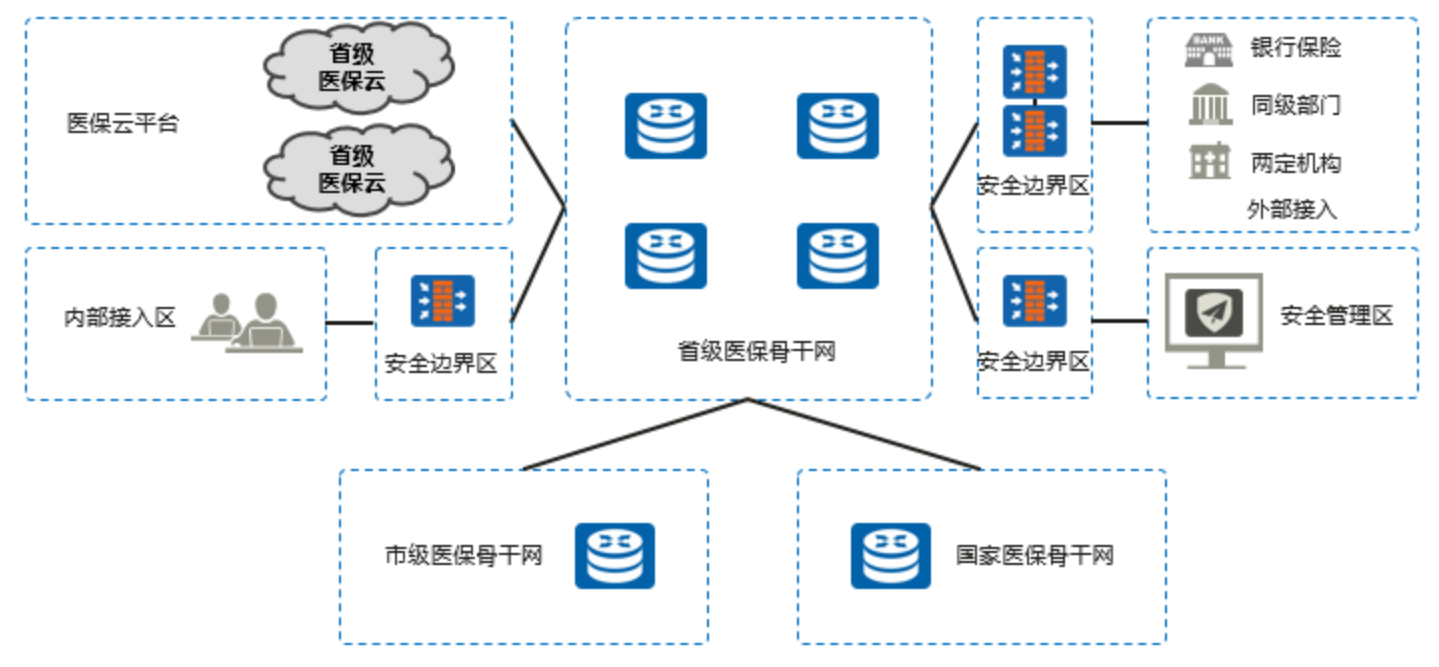


图2‑2医保核心业务专网逻辑连接图

国家医疗保障局到省医保局的纵向一级骨干网络、横向接入网络和内部局域网构成局本级核心业务网，省级到市的纵向二级网络和本级横向接入网络、内部局域网构成省级医保核心业务网，市级到县（区）的纵向三级网络和本级横向接入网络、内部局域网构成市级医保核心业务网。

依据集约建设原则，河南省医疗保障局依托电子政务外网建设省级核心业务专网，省级医保部门到各市医保部门的纵向网络通过电子政务外网+办公资源网提供服务，省政务外网以GRE形式提供虚拟链路，办公资源网以L3 VPN形式提供虚拟链路。根据业务需要，省级出口带宽1000M，市级出口带宽100M，县（区）出口带宽20M。整体线路架构图如下所示：

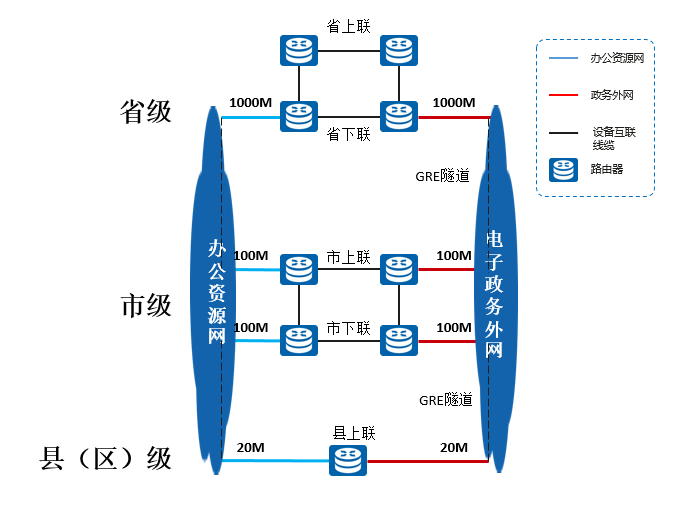


图2‑3医保核心业务专网线路架构图

## 纵向网络连接

医保纵向网络应采用电子政务外网+办公资源网作为通讯线路。省级、市级医保核心业务网，纵向上联上级医保部门核心业务网，下联下级医保部门核心业务网。

医保纵向网络采用电子政务外网+办公资源网作为通讯线路。其中

* 国家局到省本级：专线+电子政务外网
* 省本级到地市：办公资源网+电子政务外网
* 市本级到区县，乡镇或社区：不建设三级纵向网，作为接入单位通过电子政务外网或办公资源网上联对应接入区域

偏远地区乡村和社区卫生室考虑采用4G+VPDN方式接入医保数据中心网络，并须采用二次认证方式。

接入方式如下表所示：

| **接入场景** | **接入方式** | | | | |
| --- | --- | --- | --- | --- | --- |
|  | **电子政务外网** | **办公资源网** | **经办专线** | **VPDN+4G/5G** | **IPsec VPN** |
| 国家局到省本级 | √ |  | √ |  |  |
| 省本级到地市 | √ | √ |  |  |  |
| 市本级到县（区） | √ | √ |  |  |  |
| 区县到乡镇、街道 |  |  | √ | √ |  |
| 乡镇、街道到社区、村 |  |  | √ | √ |  |

## 横向网络连接

医保横向网络连接主要用于人社、卫健、民政、公安、税务、其他信息资源共享部门，以及定点医院、定点药店、商业银行、保险公司等外部用户与医保网络的连接。其中，定点医院、定点药店、商业银行、保险公司采用专线等作为网络连接链路。人社、卫健、民政、公安、税务、其他信息资源共享部门采用专线、电子政务网络、运营商MPLS VPN或者VPDN等方式接入相应的地方医保核心业务网。其中：

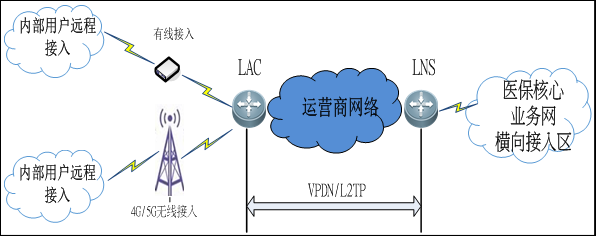
与银行、医药机构连接：省、市定点（协议）医药机构和协议金融机构通过专线等形式连接横向接入LNS设备，通过省级医保核心业务专网访问医保数据中心网络。县、乡（镇）、村定点（协议）医药机构和协议金融机构通过专线或非专线形式连接到对应市级横向接入LNS设备，通过省级医保核心业务专网访问医保数据中心网络；

与同级税务、财政、公安等单位连接：在省级建设与政务外网互通链路，省、市、县（区）信息共享部门，如人社、卫健、民政、公安、税务等部门，直接通过政务外网虚拟链路访问医保数据中心网络。

| **接入场景** | **接入方式** | | | |
| --- | --- | --- | --- | --- |
|  | **电子政务外网** | **经办专线** | **VPDN+4G/5G** | **IPsec VPN** |
| 地方人社、卫健、民政、公安、税务、其他信息资源共享部门 | √ |  |  |  |
| 银行、保险公司 |  | √ | √（仅能用作备份链路） |  |
| 三级甲等医院 |  | √ | √（仅能用作备份链路） |  |
| 其他医院，定点药店，乡镇卫生所等 |  | √ | √ | √ |

## 远程办公接入

远程办公用于医保工作人员出差或外出时，在医保核心业务网覆盖范围以外访问医保内部业务应用，采用VPDN方式建立网络连接。终端接入方式可以采用有线接入或4G/5G无线接入，并须采用二次认证方式，如下图所示。



# 网络规划设计

## 网络架构设计

按照国家医疗保障局网络安全和信息化领导小组办公室下发《全国医疗保障系统核心业务区骨干网络建设指南》文件要求，医疗保障核心业务网络采用树形网络结构，纵向主要由各级医疗保障部门按垂直的上下级模式连接成广域骨干网络，由国家医疗保障局连接全国各省级医疗保障局，并向下覆盖到市、县级医疗保障部门；横向原则上以中央和省级医疗保障部门为中心向同级信息资源共享 部门辐射，并与医院、药店、银行、保险公司等相关单位连接，形成该级的城域接入网。各单位通过点对网连接模式或网对网连接模式横向连接到医疗保障核心业务区网络。

针对医保结算等业务对于链路时延和抖动敏感度要求高，结合河南省电子政务网络现状，河南省医疗保障局骨干网建设采用“办公资源网+政务外网链路”方式，建议省级网络采用SDN/SRv6架构，用于满足后续医疗保障局相关业务承载的需求。整体逻辑架构如下：

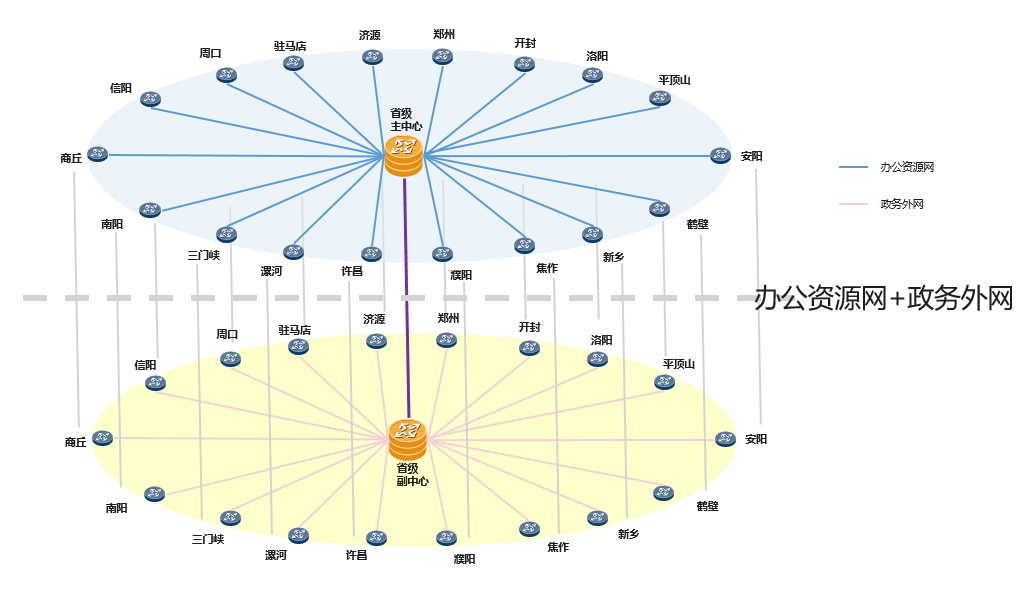


图3‑1河南省医保业务专网逻辑结构图

医疗保障业务专网全网部署IPv4 。IP网络地址按每市32个C类地址（郑州64个C）进行分配，各地根据分配的IP地址范围进行规划使用，如业务需要启用新的地址，须报备河南省医保局备案同意。IPv6 地址的规范和使用，省局将视情况再行发布使用。

按照核心业务省集中模式建设，业务专网按照省、市两级节点模式建设，银行、保险公司等垂直管理单位直接与省级接入区互联，市以下两定单位通过市级接入区与省级平台互联，整体组网示意图如下：

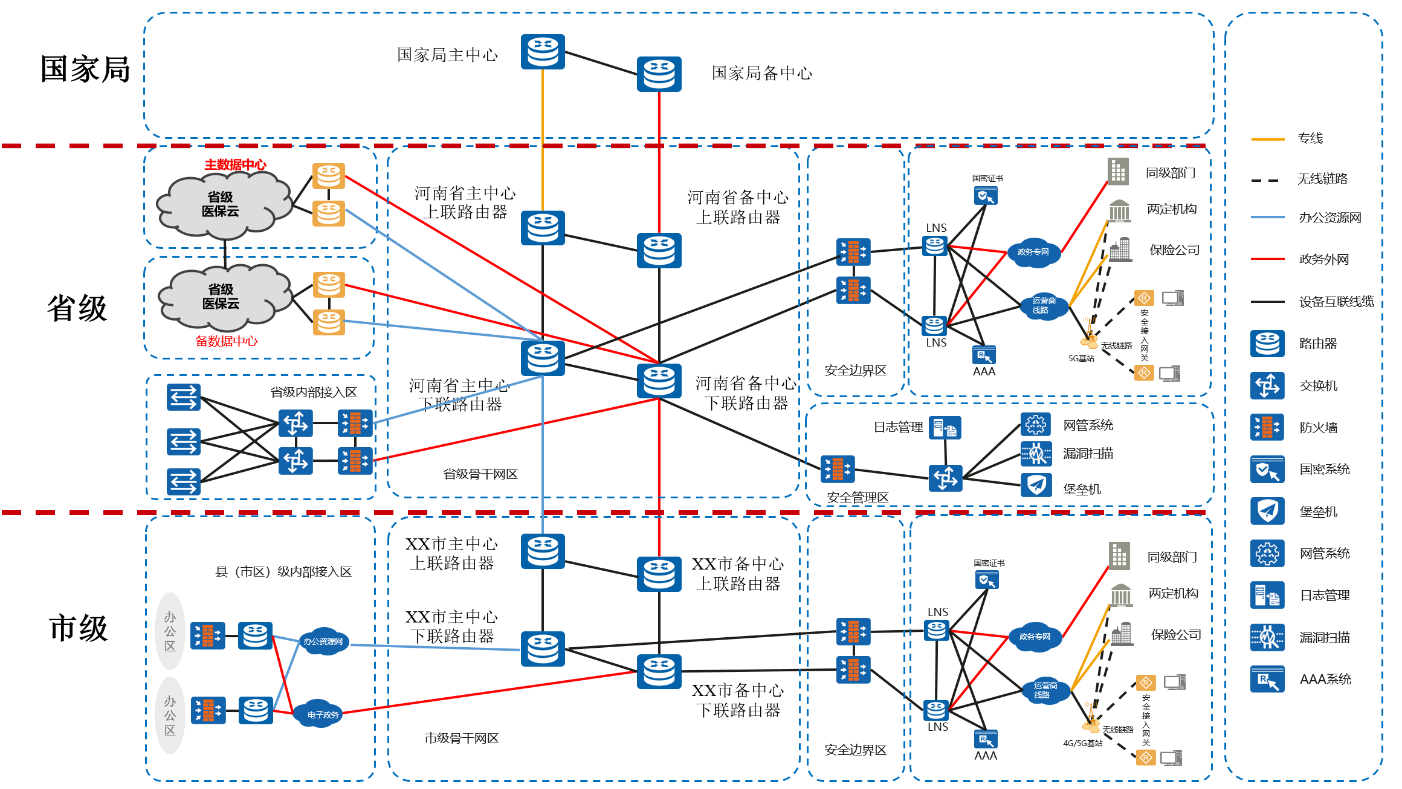


图3‑2河南省医保业务专网网络拓扑结构图

1. 河南省省级医保业务专网：

两台省级核心上联路由器负责连接到国家局核心下联路由器，采用双链路方式，政务外网链路和办公资源网链路互为备份。两台省级核心下联路由器负责连接省级内部接入区，外部接入区，安全管理区和骨干网区。

* 内部接入区为省级医保局工作人员内部办公网络。
* 外部接入区为人社、卫健、民政、公安、税务、其他信息资源共享部门，以及定点医院、定点药店、商业银行、保险公司等外部用户与医保网络的连接区域。
* 安全管理区为医保骨干网安全维护区域。
* 骨干网区为医保核心骨干接入区域。

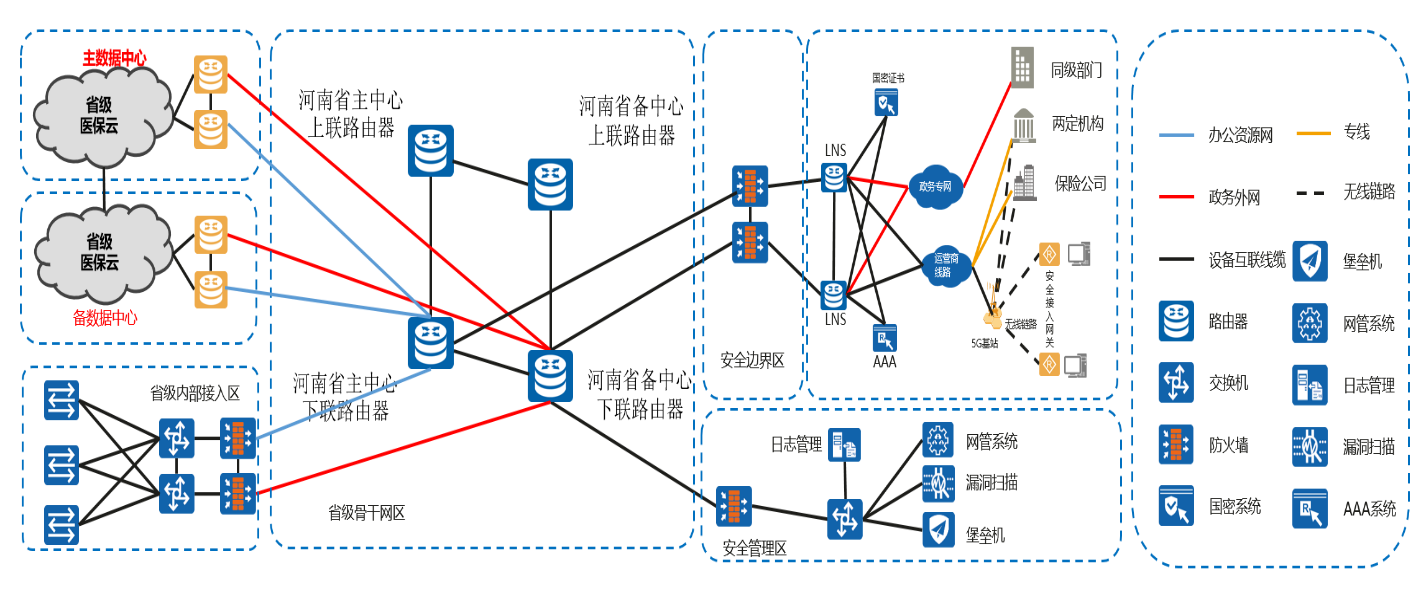


图3‑3河南省医保业务专网省级网络拓扑结构图

1. 河南省市级医保业务专网：

两台市级核心上联路由器通过电子政务外网+办公资源网的方式与省级核心下联路由器连接。两台市级核心下联路由器负责连接省级内部接入区，外部接入区。

* 内部接入区为县（市区）级医保局内部网接入区域。
* 外部接入区为人社、卫健、民政、公安、税务、其他信息资源共享部门，以及定点医院、定点药店、商业银行、保险公司等外部用户与医保网络的连接区域。

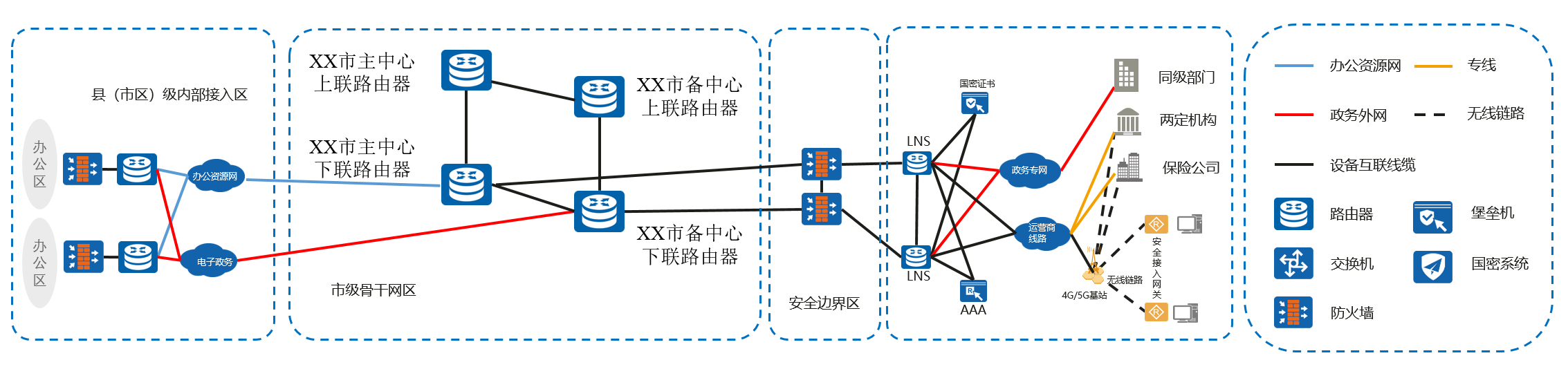


图3‑4河南省医保业务专网市级网络拓扑结构图

3、横向接入区：

定点医药机构横向接入分为两种情况，通过专线形式接入方式和非专线方式接入，须和医保核心业务区CA 强身份认证方式进行准入，同时接入设备须在同级医保局安全接入管理平台进行统一认证纳管后，才能允许访问医保核心业务区网络，非专线接入方式分为无线VPDN 接入方式和有线VPN 方式接入。

**专线方式：**

定点医药机构采用专线链路完成地方医保网的接入建设，带宽独享，该接入方式要求如下：

要采用具备有线、无线双备份能力接入网关接入，并实时检测双线路备份状态，确保医保信息业务不中断。

**非专线方式：**



国家医保局负责建立全国统一的安全接入管理平台（以下简称管理平台），各地市根据情况分级进行部署使用。河南省医保局建设省、市两级安全接入管理分平台，部署在医保部门核心业务区，内容包括CA、LNS、AAA。定点医药机构通过各运营商网络接入各级管理平台，同时管理平台通过运营商提供的API 接口对接入终端使用情况进行监控。管理平台须具备角色管理、发放管理、设备管理、联网管理、应用管理、监控管理、入库管理、下载管理等功能。该接入方式要求如下：

河南省医保局建设省、市两级安全接入管理分平台，内容包括CA、AAA、4G接入管理等。市级安全接入分平台含有线VPN、4G/5G无线接入网关，边界防护设备。边界防护设备需要具备防火墙、应用特征检测、防病毒、入侵防御、URL过滤、IPSEC VPN等功能，能够实现对接入网关设备的自动管控。

可采用具备有线、或有线无线双备份能力接入网关接入，接入网关需要支持国密局认证的密码模块隧道加密技术对链路加密，接入网关通过地市医保局数字证书进行认证，确保专用接入网关的合法性、链路的安全性。

市级医保局需要实现对非专线接入设备的监控管理，实时检测双线路状态，中断及时告警。通过无线接入实时显示设备位置，实现设备位置超出范围锁定告警，防范设备丢失。

接入终端专机专用，不得连接互联网以及其它网络，严禁处理涉密信息。

接入终端应安装客户端安全监控与管理软件。

终端侧需具备杀毒能力，确保病毒库即时更新，防范恶意代码。

终端使用医疗保障部门颁发的医疗保障数字证书进行身份认证，在市级医保局安全接入管理平台进行统一认证纳管后，再访问医保核心业务区网络。

## 承载网络规划设计

### 链路指标要求

医疗保障业务专网具有高带宽、低时延的网络特性，骨干网络采用政务外网+办公资源网方案，骨干链路主要指标要求如下：

* 可利用率不低于99.9%；
* 本地链路延时≤10ms；
* 长途链路每100公里的延时增加≤1ms，误码率<10E-7；
* 封包成功率≥99.999%；
* 抖动≤2ms；
* 平均修复时间 4 小时。

对于横向接入网络可以采用运营商的专线链路，有线VPN链路和无线VPDN链路。

专线链路主要指标要求如下：

1. 运营商干线提供双路由的传输保护，组成自愈环网，保护倒换时间小于50ms。

2. 电路测试指标：

吞吐量（Throughput）： 100%

丢包率（Frame Loss）：≤0.1%

3. 接口类型：百兆以太网接口及以上。

4. 网络必须具备可扩展能力，具有灵活的带宽伸缩能力，满足业务发展的需要。

5. 不能同互联网连接。

### 链路带宽要求

省市县链路需做到带宽独享，根据业务需要，省级下联出口带宽1000M，市级出口带宽100M，县（区）出口带宽20M。

横向采用专线接入方式的单位，带宽以2M颗粒度递增。

### 链路连接方式要求

医疗保障业务专网使用电子政务外网+办公资源网双链路方式，医保局业务不能直接接入政务外网运行，需要穿越电子政务外网。根据国家局发文，可选用L3VPN、GRE 或SRv6 三种方案穿越政务外网。

根据河南省情况以及医保业务实际需求，本次选择GRE隧道穿越政务外网方案。若由省到各地市的电子政务外网完成IPv6的改造，可以升级为SRv6方式穿越政务外网。办公资源网链路，通过L3 VPN方式穿越。

## IPv4、IPv6双栈运行方案

医保核心业务未来需要承载IPv6业务，在承载方案设计需要考虑未来的演进。由于需要利旧政务外网的网络，根据当前各省市政务外网的实际情况（主要考虑为政务外网为IPv4/IPv6双栈场景和IPv4单栈场景），方案分为两种场景。

**政务外网IPv4和IPv6 三层链路场景设计**

医保核心业务网依托政务外网建设，政务外网为医保核心业务网提供虚拟链路。当政务外网可以同时提供IPv4和IPv6 GRE虚拟链路时，医保核心业务专网采用裸IP方式承载IPv4和IPv6医保业务。

**政务外网仅IPv4三层链路场景设计**

医保核心业务专网依托政务外网建设，政务外网为医保核心业务网提供虚拟链路。当政务外网仅提供IPv4 GRE虚拟链路时，医保核心业务专网采用裸IP方式承载IPv4医保业务，采用IPv6 L3VPN over LDP over GRE方式承载IPv6医保业务。

## SDN部署

随着业务云化、高清视频、物联网等新技术的蓬勃发展，广域网上需要承载的数据量成倍增长，业务种类多样化，要求广域网具有更高的可靠性、带宽灵活适应性、分支快速部署及远程运维、关键业务的安全性等，传统的广域网技术已经无法满足新业务发展的需求。

通过采用SDN技术可打破传统广域网的限制，解决网络面临的带宽利用率低，业务体验差、部署低效、运维复杂等问题。实现高效利用网络资源（空间、能源、设备容量）简化运维管理、节省建设和维护开销等目标。

采用SDN技术的广域网络能够比传统网络更敏捷、可靠，同时降低运维管理难度。广域网采用SDN及未采用SDN技术的各项指标区别表如下：

表3‑1各项指标区别表

| **类别** | **未采用SDN技术** | **采用SDN技术** |
| --- | --- | --- |
| 网络质量监控 | 监控带宽 | 监控带宽、丢包、时延 |
| 突发拥塞 | 报障后人工调整 | 自动发现、调整 |
| 高价值业务 | 保证优先转发 | 保证带宽、路径、时延 |
| 链路利用率 | 无法保证 | 流量调整保证 |
| 转发控制 | 基于路由控制 | 逐跳可控 |

随着业务逐步汇聚到医保信息平台，对广域网有了更高的带宽需求，而传统广域网的链路利用率始终维持在20%-30%，因此需要将隐藏的带宽潜力释放出来。同时，要尽量简化部署过程，以应对新时代快速上线的业务趋势。

### 全局流量优化

传统广域网的业务依赖IGP最短路径转发，导致网络流量不均衡。广域网络基于SDN （软件定义网络）架构，综合带宽、时延、费用等因素，全局统一计算路由，实现网络流量均衡，提升链路带宽利用率，节省链路成本。

广域网基于SDN的解决方案可实现资源统一调配，使得SDN具备跨层的全网视野，能够快速调度全网资源，提高网络利用率，实现业务自动快速部署，增强网络可靠性。

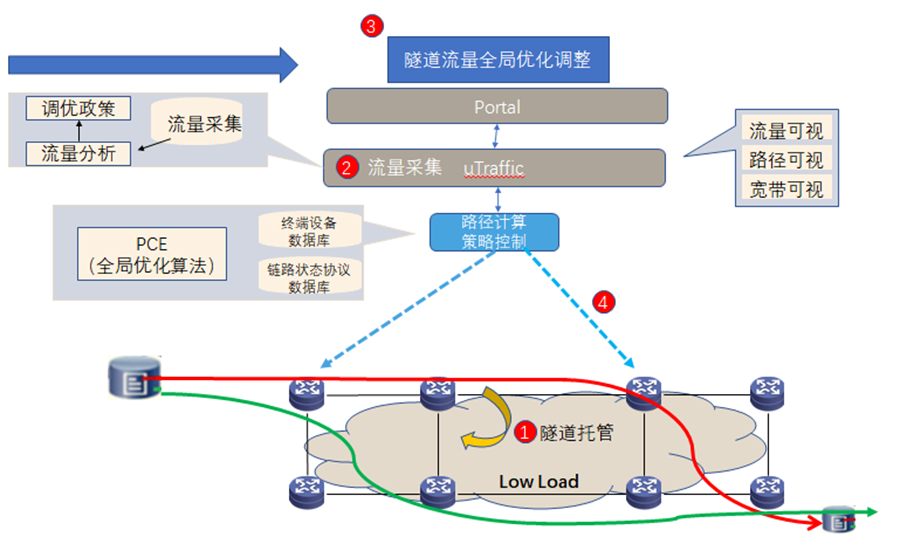


图3‑5广域网SDN流量智能管理示意图

通过SNMP、Telemetry等收集链路质量统计进行监控和分析当前流量和链路可用性，经过路径计算和策略控制器来定义智能路径策略；根据网络拓扑和流量策略，达到全网逐跳链路质量可视（带宽、丢包、时延），支持转发路径带宽端到端的检查和保障；支持上下行流量经过相同的物理路径（双向共路）转发路径逐跳可控制，保证主备路径、物理路径完全分离。

### 网络精细化管理

采用SDN的广域网络能够实现端到端的对网络进行性能监控，提供对业务的智能感知、实时检测和精准的全网业务质量报告，从而实现网络故障的快速定位，使传统网络变得可视可管可控。

### 运维效率提升

SDN将网络抽象化，面向应用层提供开放的软件接口，支撑应用对网络能力的直接调用，从而提高部署效率，减少新业务上线时间，降低运维管理压力。

## SRv6部署

### SR技术

Segment Routing（SR）是一种源路由技术。它为每个节点或链路分配Segment，头节点把这些Segment组合起来形成Segment序列（Segment路径），指引报文按照Segment序列进行转发，从而实现网络的编程能力。

Segment Routing有如下四个优点：

1. 简化了控制协议。它只采用IGP，统一了控制协议，不再像MPLS那样在IGP的基础还要LDP、RSVP-TE等协议，降低了运维的复杂度。

2.良好的扩展性。SR技术路径编程是在头结点进行，海量的路径都是依赖于有限的表示链路和节点的Segment的组合，网络中间节点几乎不感知路径状态，具备很高的扩展性。

3 . 可编程性好。Segment Routing 中的Segment非常类似于计算机的指令， 通过对Segment 的编排可以实现类似于计算机指令的功能。具备非常好的灵活性，可以非常灵活地建立满足不同需求的路径，释放网络的价值。

4.更可靠的保护。Segment Routing能提供100%网络覆盖的快速重路由保护，解决了IP网络长期面临的技术难题，能够在高可扩展性的前提下，又可以达到完全的可靠性保护。

### SRv6优势

Segment Routing转发层有两种封装格式，一种是MPLS即SR MPLS，另一种是IPv6即SRv6。

SRv6在SR MPLS的基础上，还具有如下优势：

去MPLS，协议简化。SRv6彻底去标签化，隧道及业务均通过SRv6 SID统一承载。

无缝部署IPv6业务。SRv6完全融入IPv6，部署VPN业务，中间设备只要保证IPv6可达即可。利用IPv6的路由可达性的天然优势，易于大规模、跨网络端到端部署业务。MPLS网络，如果要建立隧道，需要整网支持MPLS。对于SRv6，只需要支持IPv6就可以建立端到端的隧道；

可编程能力强。可以实现网络路径可编程和业务可编程。

SRv6不仅继承了SR的优点，还具备标签空间数量无限、全网唯一、任意点可达的优点。

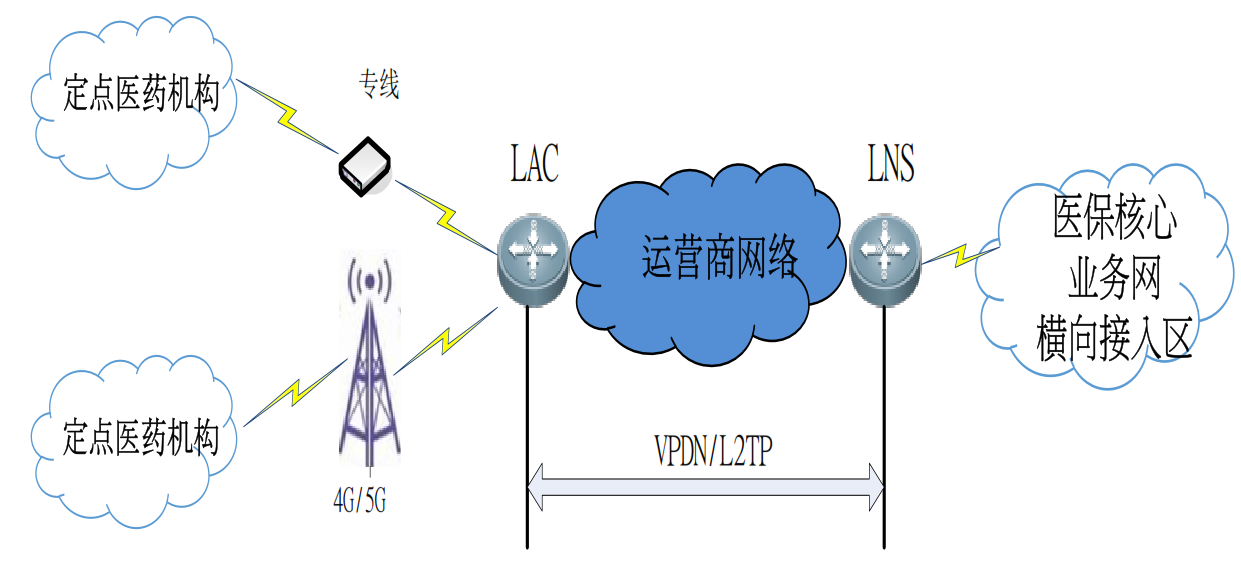
### SRv6应用效果

目前河南省医疗保障业务专网建设主要依托于电子政务外网+办公资源网，选择GRE穿越电子政务外网的部署方式。GER隧道方式配置繁琐，部署也不够灵活，开通新的业务需要部署新的GRE隧道。当电子政务外网完成IPv6改造，可以切换到使用SRv6穿越电子政务外网方案，电子政务外网可以达到和专线类似的效果，实现业务灵活部署，链路状态感知的效果。

## 无线接入VPDN设计

### VPDN组网方式

医疗保障局的无线接入终端利用运营商的4G/5G网络，接入运营商VPDN平台，通过运营商与客户的互联专线，实现无线接入终端与企业之间的数据传输。VPDN组网拓扑如下所示：



所有无线终端设备都处于医疗保障局专用网络内，终端设备获得的是内网的IP地址，节省日渐紧张的公网IP资源。同时，客户私网和医保专网完全隔离，数据保密性好。客户专网不会受到来自医保专网上的黑客及病毒的侵袭，能够有效保证稳定的传输速率和带宽。下面分别对上图中各个设备进行介绍。

**终端**：可以是手机、笔记本、无线Modem等，根据客户不同的需求选用不同的终端。

**运营商PGW**：网关支持节点, 客户通过4G接入到PGW，PGW判断是VPN用户，向指定的LNS发起L2TP/GRE连接。

**专线**：通常采用运营商的100M以太网专线，此专线将运营商的4G网关和客户的LNS设备连接起来。

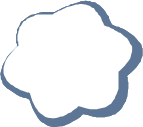
**客户侧路由器（LNS）**：需支持L2TP/GRE协议，要与PGW建立L2TP/GRE隧道。

### 国密加密算法

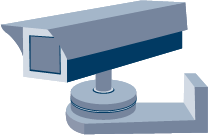
为进一笔保障数据安全，两定机构与省级平台之间建立IPSec VPN，并在对“敏感”数据进行加密时，密码算法应选用国密算法，确保业务安全。



4G/LTE



**总部**



L2TP over IPSec(国密)

国密算法能够实现商用密码算法的加密、解密和认证等功能的技术。（包括密码算法编程技术和密码算法芯片、加密卡等的实现技术）。商用密码技术是商用密码的核心，国家将商用密码技术列入国家秘密，任何单位和个人都有责任和义务保护商用密码技术的秘密。

## 网络可靠性设计

网络的可靠性由多个因素构成，主要包括设备可靠性、链路可靠性、网络可靠性、故障检测、业务保护等方面。充分利用设备的软硬件特性及网络拓扑，可使网络的可靠性达到最优。

线路的备份主要解决了网络互通路径的问题，而节点设备的可靠则解决网络的有效运转。要保证网络的可靠性，必须要选用具备电信级可靠性的网络设备进行组网，才能使网络具有自动恢复能力、降低人工维护工作，达到电信级的可靠运行。

### 设备可靠性

设备的高可靠性从硬件、软件、保护机制等几个方面体现：

1. **采用分布式体系结构**

分布式体系设备将管理、路由转发、接口处理等功能分配在不同的部件上，协同工作，分布式体系可以分散故障风险、隔离故障、提供冗余配置，提高系统的自动恢复能力。

1. **关键部件冗余**

设备的所有关键部件都有冗余设计，主控板1:1冗余备份、交换网板N+M冗余备份、电源模块N+M冗余备份、风扇模块冗余备份，完善的告警功能，保证系统在运行中不会失效。

1. **实时热备份机制**

在系统软件及硬件的支持下，关键部件在发生故障能自动启动备份系统，主备系统之间实时热切换，运行中即使发生设备故障切换也不会对网络业务造成影响。

1. **热插拔特性**

设备任意单板需要支持热插拔特性，保证系统出现故障需要维护或系统需要升级扩展时，不需要停机处理，保证网络的7×24小时不间断运行。

1. **散热系统**

散热系统使设备长时间运行而不至因为系统升温过高出现故障，冗余风扇等散热装置可以增加设备的运行时间及减少故障发生。

1. **硬件异常保护**

设备具备异常情况下的保护、告警、纠错能力。

1. **不间断转发、路由和升级**

NSF、GR、NSR和ISSU等业务不中断技术用于使得在主控板1:1冗余备份的设备上，主控板主备倒换或软件升级期间，保证数据转发不中断、路由处理不中断。

### 链路可靠性

在单链路组网接入时，租用运营商的链路时，应尽量租用双线接入的链路，以提高网络的可靠性。在双节点双链路接入时，可以采用单线接入的链路，利用网络的可靠性机制保证业务不发生中断。

对物理链路可靠性的要求应至少需要满足99.99%可靠性的服务质量要求。

对于节点间的主备链路，要求主备两根物理裸光纤布放在不同物理管线中（比如从不同运营商租用），要求主备链路部署在不同物理裸光纤中（租用链路时明确提出避免主备链路共风险要求）。

### 故障检测

1. **硬件BFD通断检测**

为了提高IP/MPLS层的故障检测时间和效率，需要使用检测速度快、支持各种协议的故障检测机制。BFD已经被广泛应用于各种链路、协议的故障检测。

1. **误码检测**

网络设备在入接口方向通过CRC校验算法来检测误码，并计算相应的误码率。如果该误码率超过了当前接口的误码告警阈值，则设备认为该接口发生了误码故障，通知上层业务，进而触发保护倒换。如果在后续的检测中，接口的误码率降低到了告警恢复阈值以下，则设备认为该接口误码故障已恢复，通知上层业务，进而触发业务回切。

## 骨干网流量设计

### 骨干网流量分析

根据国家医保局下发《全国医疗保障系统核心业务区骨干网络建设指南》及《地方医疗保障信息平台建设指南》，结合河南省实际情况，分析河南省医疗保障业务专网内流量流向主要为以下几种：  
 1、外部接入区→河南省医保云平台  
 人社、卫健、民政、公安、税务、其他信息资源共享部门，以及定点医院、定点药店、商业银行、保险公司等外部用户等经办类流量。  
 2、内部办公区→河南省医保云平台  
 医保办公人员办公业务流量  
 3、外部接入区→安全管理区  
 对外部接入数据样本采集流量  
 4、河南省医保云平台→国家局医保云平台  
 跨省业务流量

### 骨干网流量Qos划分

根据上一章节，可以将流量划分为医保业务流量和办公流量两大类。  
 1、办公流量  
 办公流量可以更细划分为语音类业务，视频类业务，普通办公类业务。这三类业务流量，对时延敏要求由高到低为：视频类业务＞语音类业务＞普通办公类业务。因此要优先保证视频类业务。  
 2、医保业务流量  
 医保业务流量根据《地方医疗保障信息平台建设指南》，根据云平台不同子系统划分为：公共服务子系统流量、药品和医用耗材招采管理子系统流量、基础信息管理子系统流量、医保业务基础子系统流量、跨省异地就医管理子系统流量、支付方式管理子系统流量、医疗服务价格管理子系统流量、信用管理评价子系统流量、内部统一门户子系统流量、内部控制子系统流量、医疗保障智能监控子系统流量、运行监测子系统流量、宏观决策大数据应用子系统流量、基金运行及审计监管子系统流量。  
 针对以上子系统流量，建议优先级较高的子系统流量为：公共服务子系统流量、药品和医用耗材招采管理子系统流量和跨省异地就医管理子系统流量。  
 公共服务子系统包含医疗即时结算、结算对账等结算类业务。药品和医用耗材招采管理子系统包含实时查询，价格管理等业务。跨省异地就医管理子系统包含收付款确认、收付款查询等业务。因以上子系统业务对时延要求较高，因此要优先保证该子系统业务流量。

应用分类是QoS实现的基础，下面以常用的业务为例，说明针对应用的QOS分类：

关键类应用：如银行的核心的柜面业务，自助终端等应用，企业的核心定单业务对带宽需求量稳定，需要保证数据的优先传输。

语音类应用：VoIP类应用，对延时和抖动要求较高。

视频类应用：视频会议类应用，对延时和抖动要求较高。

交互类应用：需要双向交换信息，对实时性要求较高，数据流量变化不大的非办公业务；例如基于WEB的信息查询等。

决策和批量类应用：与交互类业务相独立的，对实时性要求不高，单向数据传输量大且数据流量变化很大的非办公业务。

办公类应用：所有办公类的应用，例如邮件等。

根据各类应用系统的特点，对其重要性、实时性、时延、带宽和优先级，进行描述。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 应用类别 | 重要性 | 实时性 | 时延 | 带宽需求 | 优先级 |
| 关键类应用 | 高 | 高 | 高 | 中 | 高 |
| 语音类应用 | 中 | 高 | 高 | 中 | 高 |
| 视频类应用 | 中 | 高 | 高 | 高 | 高 |
| 交互类应用 | 中 | 高 | 中 | 中 | 高 |
| 办公类应用 | 中 | 中 | 低 | 高 | 中 |
| 决策和批量类应用 | 中 | 低 | 低 | 高 | 中 |
| 其他 | 低 | 低 | 低 | 高 | 低 |

采用 DSCP对数据包进行标记，DSCP采用IPv4报头中的 6位来定义服务水平，其中：

EF：表示 Expedited Forwarding，为最高服务级别

AF：表示 Assured Forwarding，可以根据不同服务要求，定义不同的服务级别

BE：表示 Best Effort，一般用于缺省的服务级别

基于上述的应用分类和分析，数据包标记如下：

|  |  |  |
| --- | --- | --- |
| 应用类别 | 优先级 | DSCP标记 |
| 关键类应用 | 高 | EF |
| 语音类应用 | 高 | AF41 |
| 视频类应用 | 高 | AF42 |
| 交互类应用 | 中 | AF31 |
| 办公类应用 | 中 | AF21 |
| 决策和批量类应用 | 中 | AF11 |
| 其他 | 低 | BE |

## 网络性能和质量监测设计

用户对网络智能运维的需求越来越迫切，及时检测流量微突发和流量调优，需要更加实时更高精度地监控数据，同时监控过程要对设备功能和性能影响小。在医疗保障业务专网建设中，推荐使用telemetry技术实现网络性能和质量监测。

Telemetry是一项远程的从物理设备或虚拟设备上高速采集数据的技术，支持亚秒级数据采集频率，适用于7\*24小时的周期性持续不间断监控。设备通过推模式（Push Mode）周期性的主动向采集器上送设备状态数据，提供了更实时更高速更精准的数据采集功能。

Telemetry技术可以支持智能运维系统管理更多的设备、监控数据更高精度和更加实时、监控过程对设备自身功能和性能影响小，为网络问题的快速定位、网络质量优化调整提供了很重要的大数据运维基础，将网络质量分析转换为大数据分析，有力的支撑了智能运维的需要。

# 安全体系设计

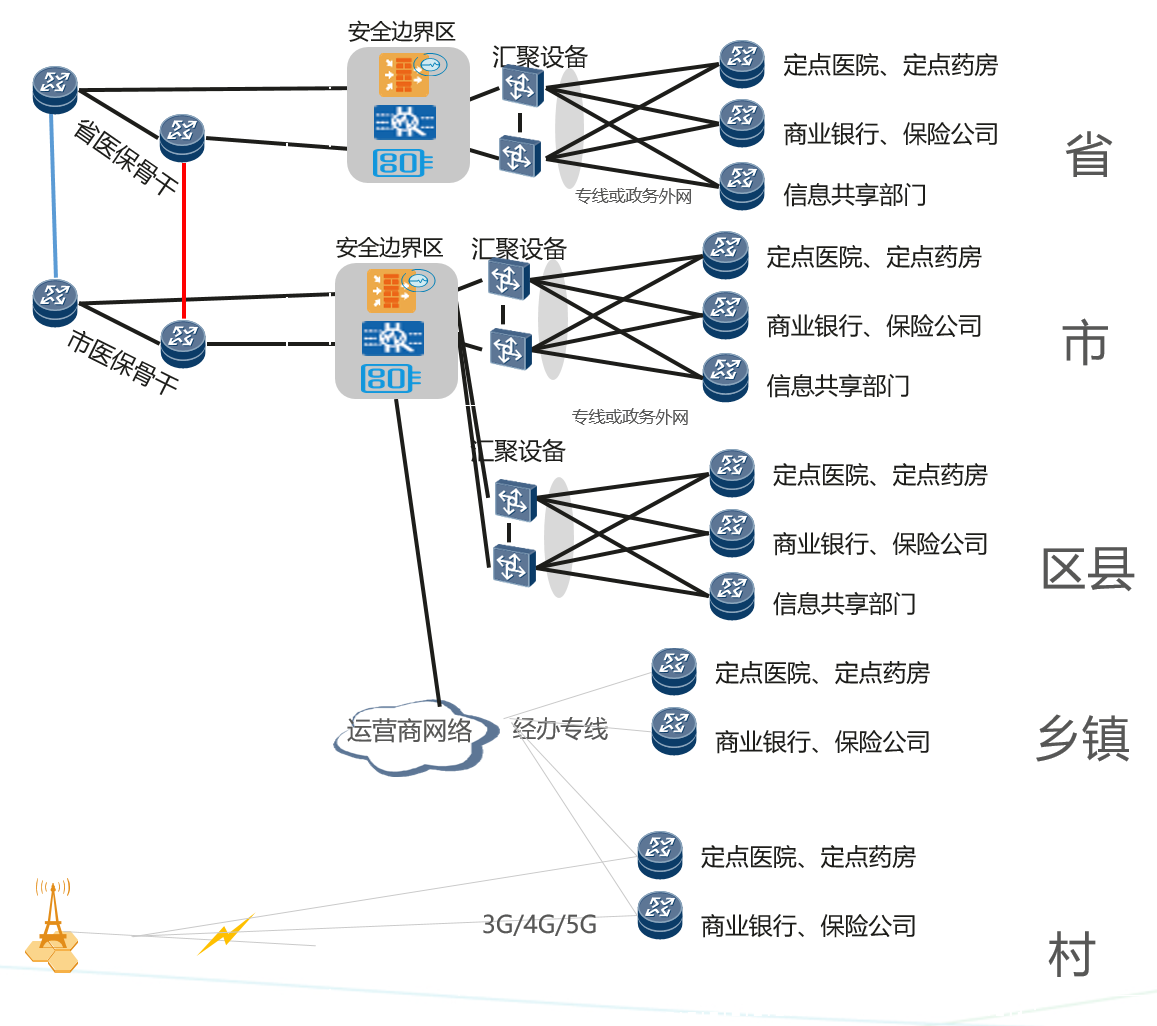
## 安全保障体系建设

医保项目涉及民生工程，系统稳定性、数据安全性非常重要，要严格把关安全，建设立体的安全保障体系，包括网络安全技术体系、网络安全管理体系、三重防护体系、网络安全运营体等，要加强安全态势感知能力建设，要加强安全管理中心职责与能力建设，并且通过信息系统安全等级保护测评来保障等保3级。业务网络要结合大数据局做好安全管理，终端接入、应用系统、互联网系统、定点医药机构接入等要联合使用单位，共同建设完善安全保障体系。

## 网络建设的安全性要求

### 横向接入区安全

横向接入区通过专线或政务外网方式与人社、卫健、民政、财政、税务、公安以及医院、药店、商业银行、保险公司等单位互联互通，外部接入单位较多，核心业务系统面临来自横向外部接入单位的安全威胁相对来自互联网的安全威胁较小，但是作为重要业务系统仍不可忽视来自横向单位的安全威胁。



（1）通过部署横向边界防火墙保证跨越边界的访问和数据流通过防火墙提供的受控接口进行通信，实现对边界交换数据流基于应用协议和应用内容的访问控制，实现对边界数据流中恶意代码的检测和清除、垃圾邮件的检测和防护。

（2）通过部署入侵防御系统或日志审计系统防止或限制从外部和内部发起的网络攻击行为；当检测到攻击行为时，记录攻击源IP、攻击类型、攻击目标、攻击时间,在发生严重入侵事件时进行报警。

（3）通过运营商专线或政务外网方式连接同级资源共享部门及外部关联单位，避免信息在横向网络传输过程中被窃听，对于两定、商业公司等可以通过IPSEC技术进行密文传输，防止传输过程中被窃听。

（4）基于大数据分析，精准识别恶意文件传输，黑客入侵，数据泄露等威胁，并实现威胁的自动化威胁阻断。

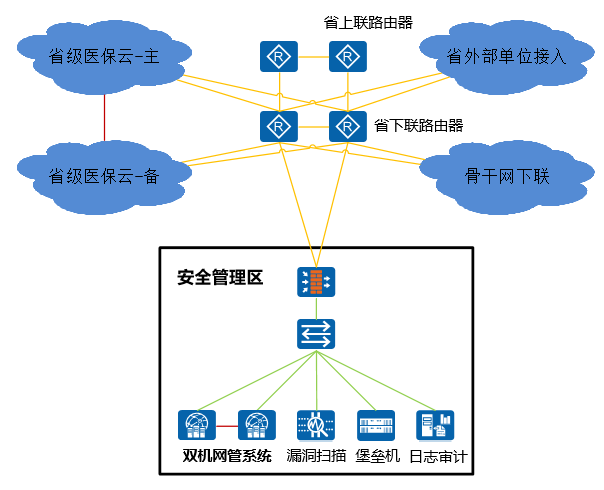
### 安全运维区

安全服务管理安全域为对医保骨干网的软/硬件系统提供统一运维资源环境，部署堡垒机、网管系统等设备；为了保证安全服务管理安全域的安全，对该安全域也同步在网络中配置安全隔离和安全防护措施。

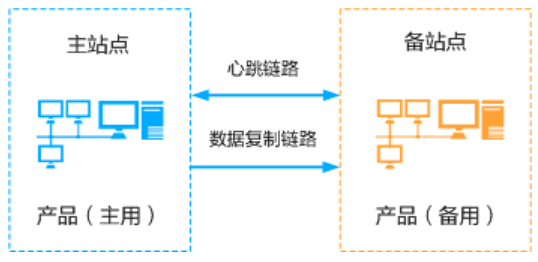
安全管理域对业务专网的所有设备提供高效、可信的安全运维管理，部署堡垒机、网管系统、漏洞扫描系统等设备，包括设备以及系统的日志审计，设备统一管理与配置。通过丰富的报表将业务状态、网络环境、安全态势、用户行为等进行可视化展现，让用户全方位感知，安全运营。

河南省医保业务专网依托专业SDN控制器网管平台Network Cloud Engine进行统一运维管理，实现资产管理、拓扑管理、告警管理、大屏监控、报表管理、自动化部署、流量调优等功能。

网管平台部署于省安全管理区，并通过电子政务外网VPN通道实现对医保业务专网全网路由、交换、安全设备的统一纳管。为确保运维管理工作的有序与安全，网管平台采用分权分域管理的原则，可设置超级管理员、省级管理员和地市管理员三级权限，分别负责账号权限分发，全省设备管理和地市设备管理。



网管平台采用双机部署方案，实现业务系统的高可靠性。通过远程热备份技术，实现主、备站点数据实时同步，并动态监视网络管理系统的运行状态。当主服务器发生硬件故障、操作系统故障、网管关键应用故障或心跳线路故障时，系统会自动倒换到备份服务器。主备业务系统都是双活状态，无切换时间。



1、所需资源如下：

主站点：物理服务器1台

备站点：物理服务器1台

客户端：可网页登录，如需要可添加PC客户端。

2、核心安全设备如下：

**防火墙：**

通过部署安全管理区域防火墙设备进行域间访问控制，对不同安全域的业务进行有效的隔离和防护。

**统一运维审计：**

通过部署运维审计系统，对医保骨干网中网络设备的帐号、认证、授权和审计的集中管理和控制，可有效解决IT运维管理问题，满足相关法规、标准要求，完善IT管理体系，实现了IT核心资源的统一接入管理和运维审计。

对所有运维过程的控制和记录审计：实现对所有运维操作过程的文本记录和视频记录，同时支持细粒度查询，避免恶意运维操作，实现责任定位，确保运维可见可控可查。

**漏洞扫描系统：**

通过部署漏洞扫描系统，定期对骨干网中网络设备和安全设备进行漏洞扫描，明确漏洞修复优先级，以确保最危险的漏洞最早修复。

**综合日志管理系统：**

采用日志管理系统实现骨干网网络设备和安全设备的统一日志采集、格式化和关联分析、告警及审计和报告服务。

**杀毒软件：**

省级统一部署杀毒软件控制中心，各级单位办公电脑安装杀毒软件客户端。杀毒软件需具有智能升级功能，定时检查病毒库的最新版本，发现最新版本后首先升级控制中心的病毒库，然后自动将升级包分发至局域网内的各个客户端，实现统一升级实现所有防病毒软件病毒库的及时更新。

## 平台管理的安全性要求

根据国家医保局要求，国家医保局负责建立全国统一的安全接入管理平台（以下简称管理平台），河南省管理平台依据国家局管理平台现有基础进行建设。

河南省安全接入管理平台采用省市两级部署模式。定点医药机构通过各运营商网络接入各级管理平台，同时管理平台通过运营商提供的API 接口对接入终端使用情况进行监控。管理平台须具备角色管理、发放管理、设备管理、联网管理、应用管理、监控管理、入库管理、下载管理等功能。

省级平台部署省级身份认证相关模块、服务器密码机、目录服务系统LDAP、身份认证网关。无线VPDN 方式部署AAA 鉴权设备、LNS 接入设备等；有线VPN 方式部署VPN 网关设备。

市级平台部署证书综合管理系统FCMS、服务器密码机、目录服务系统LDAP、身份认证网关。无线VPDN 方式部署AAA 鉴权设备、LNS 接入设备等；有线VPN 方式部署VPN网关设备。

定点医药机构接入终端须使用国家局CA 身份认证系统颁发的数字证书，接入时须进行基于数字证书的强身份鉴别。

## 网络接入安全

接入安全体系包括终端安全、链路安全、边界安全、认证安全和应用安全等方面。安全产品原则上应采用国产自主可控产品。

### 终端安全

接入终端按照用户属性，分为内部用户终端和外部用户终端两类：

1、内部用户终端指各级医疗保障部门等医疗保障系统内部用户使用的终端，包括在医疗保障核心业务区网络内部通过局域网方式接入的终端以及医疗保障内部用户通过VPDN方式远程接入医疗保障核心业务区网络的终端。

2、外部用户终端指人社、卫健、民政、公安、税务、其他信息资源共享部门，以及医院、药店、商业银行、保险公司等医疗保障系统外部用户使用的终端，包括点对网模式接入终端和网对网模式接入终端。

#### 内部用户终端要求

**内部用户局域网终端要求**

医疗保障局域网内部用户应严格遵守国家各项信息安全法律法规，遵守医疗保障内部各项信息安全管理规定。医疗保障内部用户使用终端时，应采取以下措施：

（1）接入终端应专机专用，不得连接互联网及其它网络，严禁处理涉密信息。

（2）终端应安装医疗保障部门统一的客户端安全管理软件，实现实名制注册严格准入，防范违规外联，及时进行补丁升级，提升系统安全性。

（3）终端应安装医疗保障部门统一的杀毒软件，并确保病毒库及时更新，防范恶意代码。

（4）加强移动存储介质管理，严控数据输入输出，防止数据泄漏。

**内部用户远程办公接入终端要求**

医疗保障内部用户远程终端包括便携计算机、平板电脑或手机等设备。

对于便携计算机，应采取以下措施：

（1）采取共享限制、强制锁屏、密码强度控制等措施和必要的加固技术，保证终端安全。

（2）采用VPDN方式接入，4G/5G上网卡应与用户绑定，并采取相应技术措施，确保终端只能访问医疗保障核心业务区网络。

（3）终端应安装医疗保障部门统一的客户端安全管理软件，实现实名制注册严格准入，防范违规外联，及时进行补丁升级，提升系统安全性。

（4）终端应安装医疗保障部门指定的杀毒软件，并确保病毒库及时更新，防范恶意代码。

（5）加强移动存储介质管理，严控数据输入输出，防止数据泄漏。

（6）终端接入时应使用医疗保障颁发的数字证书进行用户身份认证。

（7）应采用符合国密算法的加密技术对数据传输和存储进行保护，防止数据泄漏。

对于平板电脑或手机终端，应采取以下措施：

（1）应使用专用的APP 访问医疗保障核心业务区网络。

（2）应采用符合国密算法的加密、沙盒等技术对数据传输和存储进行保护，防止数据泄漏。

（3）采用VPDN 方式接入，4G/5G 上网卡应与用户绑定，并采取相应技术措施，确保终端只能访问医疗保障核心业务区网络。

（4）终端接入时应使用医疗保障颁发的数字证书进行用户身份认证证书介质可采用SIM 卡、SD卡、耳机接口的USBKEY、蓝牙接口的USBKEY 等硬件方式。

（5）禁止私自提升终端权限，如获取root 权限、越狱等。

（6）终端一旦发生遗失，应有相关技术手段防范数据泄露，如远程擦除手段。

#### 外部用户终端

**点对网模式接入终端要求**

接入终端要符合医疗保障部门的安全规范，并采取以下措施：

（1）接入终端应专机专用，不得连接互联网及其它网络，严禁处理涉密信息。

（2）接入终端应通过客户端安全监控和管理软件、符合国密算法的加密或沙盒等技术手段进行安全管理，严格网络准入，及时进行补丁升级，简化相关软件的安装和使用，降低运维成本。

（3）接入终端应安装医疗保障部门统一的杀毒软件，并确保病毒库及时更新，防范恶意代码。

（4）应使用医疗保障部门颁发的医疗保障数字证书进行用户身份认证。

（5）加强移动存储介质管理，严控数据输入输出，防止数据泄漏。

**网对网模式接入要求**

接入单位网络须符合等保三级要求，接入医疗保障核心业务区网络应采取访问控制、数据加密、身份认证等安全防护措施。在访问医疗保障业务应用时，须使用医疗保障部门颁发的数字证书进行用户身份认证。

### 身份认证安全

应对医疗保障核心业务区网络接入对象进行身份认证。接入用户使用医疗保障部门统一的医疗保障数字证书进行身份认证，接入设备可通过IP/MAC 地址、设备码、设备证书等进行身份认证。

### 防火墙接入安全

#### 4.4.3.1 远程接入安全配置要求

防火墙设备必须配置合法登录声明，保护组织对入侵行为进行法律追究的权利，登录声明中禁止包含有助于攻击者的信息（软件版本，设备型号等）。

防火墙登录空闲超时时间不超过15分钟，对于超时的会话，只有在用户重新认证后方可继续访问。

网络中的Internet、Extrenet防火墙Untrust口不可作为管理口，防火墙设备要求使用专用的管理接口管理。

防火墙应限制远程管理的地址范围，除AAA服务器地址外，地址范围限定为网络维护人员日常维护所需网段。

#### 4.4.3.2认证、授权安全配置要求

防火墙设备必须纳入AAA管理系统管理。

防火墙管理用户，除网关监控、配置采集只读用户、临时性变更静态用户和统一版本网络自动化读写用户外，用户密码需采用一次性动态口令。

防火墙设备必须设置本地特权用户及动态密码，本地特权用户具有设备最高管理权限。

AAA管理系统中，针对防火墙的管理用户，至少分为两种权限类型，读写权限和只读权限，读写权限管理用户应授权到个人。

防火墙设备，用户账号在6次无效尝试后，应对该账户进行锁定，在锁定后必须延迟至少30分钟或由管理员进行解锁。

#### 日志服务安全配置要求

防火墙日志必须发送到专用日志存储服务器，日志包括设备日志和包转发日志。设备日志需记录设备登录认证信息及用户对设备的配置、状态修改的操作记录。

防火墙流量日志保存3个月。防火墙设备日志（不包括流量日志）要求保存1年以上，3个月内的日志要求立即可查。

## 等级保护建设规划

### 行业安全等保建设背景

为贯彻落实国家信息安全等级保护制度，规范和指导全国卫生行业信息安全等级保护工作，按照公安部《关于开展信息安全等级保护安全建设整改工作的指导意见》（公信安〔2009〕1429号）要求，原国家卫生部结合卫生行业实际，研究制定了《卫生行业信息安全等级保护工作的指导意见》（卫办发〔2011〕85号）。意见指出，国家、省、地市三级卫生信息平台的安全保护等级原则上不低于3级。

医疗机构作为涉及国计民生的重要组成部分，其安全保障事关社会稳定，必须全面实施信息安全等级保护。

### 等级保护要求

按照国家信息安全等保保护要求，重要业务系统需要按照三级等保要求来建设。

三级系统安全保护环境的设计目标是：落实 GB/T 22239-2008 对三级系统的安全保护要求，在二级安全保护环境的基础上，通过实现基于安全策略模型和标记的强制访问控制以及增强系统的审计机制，使得系统具有在统一安全策略管控下，保护敏感资源的能力。

通过为满足物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全四个方面基本技术要求进行技术体系建设；为满足安全策略和管理制度、安全管理机构和人员、安全建设管理、安全运维管理四个方面基本管理要求进行管理体系建设。使得网络系统的等级保护建设方案最终既可以满足等级保护的相关要求，又能够全方面为业务系统提供立体、纵深的安全保障防御体系，保证信息系统整体的安全保护能力。

信息系统安全保护级别，分为5个等级：

第一级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。

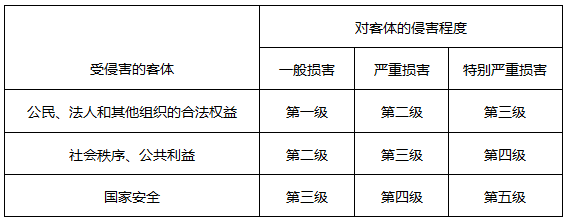
第二级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。

第三级，信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。

第四级，信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害。

第五级，信息系统受到破坏后，会对国家安全造成特别严重损害。

信息系统的安全保护等级由两个定级要素决定：等级保护对象受到破坏时所侵害的客体和对客体造成侵害的程度，定级要素与安全保护等级的关系如下：



### 等级保护流程

等级保护五个标准流程：

* 定级：现网格局梳理、初步等级确定
* 备案：组织专家评审
* 整改：梳理当前网络安全与等保要求之间的差距，根据差距进行安全整改
* 测评：联合专业测评资质的测评公司进行等保测评
* 检查: 安全运维检查。

# 机房建设规划

按照国家医疗保障局网络安全和信息化领导小组办公室下发《全国医疗保障系统核心业务区骨干网络建设指南》文件要求，医疗保障核心业务网络采用树形网络结构，结合河南省电子政务网络现状，河南省医疗保障业务专网建设采用“政务外网链路+办公资源网”方式。按照核心业务省集中模式建设，业务专网按照省、市两级节点模式建设。

本次机房建设充分遵循集约建设的原则，需向同级主管信息部门申请具体机柜位置及相关配电照明系统。

省级医保中心核心机房采用托管模式，主要放置省级骨干网络核心设备、内部办公局域网、河南医保安全接入管理平台、省级身份认证相关模块等核心设备，以及相关的语音、配线架、电源、空调等设备。根据目前所用设备，上下联主备路由器需要放置在不同的机房，按照设备情况以及预留空间预估，包含4个网络机柜，2个接入机柜，2个安全管理区设备机柜，共计约8个机柜。

市级医保中心核心机房同样采用托管模式，主要放置市级骨干网络核心设备、市县级安全接入设备，以及相关的语音、配线架、电源、空调等设备。按照实际设备情况以及未来业务增长需求，地市核心机房需求4个网络机柜，2个接入机柜，共计约6个机柜。

# 方案组件与选型建议

## 省级方案组件与选型建议

省级医保核心业务专网分为骨干路由区，外部接入区，安全管理区，省级内部办公区和云平台接入区。

**骨干路由区：**

骨干路由区的组成为两台核心上联路由器，两台核心下联路由器。上联路由器负责与国家医保局对接，统一由国家医保局管理。国家医保局部署SDN，实现跨省医保结算业务快速发放。下联路由器负责连接各市以及省级骨干网其他区域。

**外部接入区：**

外部接入区是实现省级人社、卫健、民政、公安、税务、其他信息资源共享部门以及定点医院、定点药店、商业银行、保险公司等机构的接入。

外部接入区部署两台防火墙作为接入区安全边界，开启入侵防御，防病毒等功能。对进入骨干网流量进行安全过滤。外部接入区部署2台LNS（L2TP网络服务器）和1套AAA系统。LNS设备负责对政务外网、专线链路、有线VPN、无线VPDN实行统一接入，AAA认证系统对非政务外网接入方式的链路进行统一认证。

**安全管理区：**

安全管理区主要负责对整张骨干网络的告警管理、性能检测。

安全管理区部署一台防火墙作为安全边界。部署一台接入交换机作为安全边界防火墙的端口扩展，同时可以对安全设备采集的流量进行复制，起到分流器的作用。省上统一部署网管，采用带内管理方式，不用部署单独交换机采集设备信息。部署SDN控制器，实现对医保骨干网流量调优。安全设备部署日志管理，漏洞扫描，堡垒机，杀毒软件等。

**省级内部办公区：**

省级内部办公区为省级医保局工作人员办公网。

省级内部办公区部署两台出口防火墙，开启入侵防御，防病毒等功能。部署两台核心交换机，负责省级医保局内部办公数据交换。接入交换机负责连接各办公设备的有线接入。

**云平台接入区：**

云平台接入区路由器不在本次骨干网建设范围内。

省级设备配置列表：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 区域 | 设备 | 数量 | 预算单价 | 功能 | 建议配置 |
| 骨干路由区 | 上联路由器 | 2 | 390,000 | 省级上联至国家局 | 一、基本要求：  1.三层路由：静态路由、RIP、OSPF、BGP4、IS-IS；  2.VPN技术：MPLS严格遵循相关标准，支持L3的MPLS VPN，实配GRE、IPSEC、NAT、L2TP、国密等多业务功能；  3.网络管理：SHELL、SNMP V1/V2/V3、Telnet、Rlogin、FTP、TFTP，支持流量监控功能。  二、核心性能要求：  1.硬件要求：设备支持主控卡、交换板卡、业务板卡完全物理分离，主控槽位≥2，独立交换槽位≥2；子卡槽位≥16；设备电源槽位数≥4，支持N+N冗余；  2.交换容量：交换容量≥110Tbps，包转发率≥24000Mpps；  3.支持全面的快速重路由TE FRR功能,支持基于硬件的BFD故障探测技术，支持单臂BFD。  三、最低配置要求：配置双主控，双交换板卡，冗余电源，10GE光口≥4，千兆SFP光口≥8，SRv6功能。 |
| 骨干路由区 | 下联路由器 | 2 | 450,000 | 省级下联至地市 | 一、基本要求：  1.三层路由：静态路由、RIP、OSPF、BGP4、IS-IS；  2.VPN技术：MPLS严格遵循相关标准，支持L3的MPLS VPN，实配GRE、IPSEC、NAT、L2TP、国密等多业务功能；  3.网络管理：SHELL、SNMP V1/V2/V3、Telnet、Rlogin、FTP、TFTP，支持流量监控功能。  二、核心性能要求：  1.硬件要求：设备支持主控卡、交换板卡、业务板卡完全物理分离，主控槽位≥2，独立交换槽位≥2；子卡槽位≥16；设备电源槽位数≥4，支持N+N冗余；  2.交换容量：交换容量≥110Tbps，包转发率≥24000Mpps。  3.支持全面的快速重路由TE FRR功能,支持基于硬件的BFD故障探测技术，支持单臂BFD。  三、最低配置要求：配置双主控，双交换板卡，冗余电源，10GE光口≥6，千兆SFP光口≥8，SRv6功能。 |
| 外部接入区 | 防火墙 | 2 | 150,000 | 省级横向同级资源共享部门及两定机构安全边界 | 一、基本要求：  1.支持防火墙、应用特征、防病毒、入侵防御、URL、IPSEC VPN等功能；  2.能够实现与接入网关设备联动，安全网关检测到病毒攻击，威胁攻击时主动切断接入端设备。  二、核心要求：整机防火墙吞吐≥20Gbps；HTTP并发连接≥400万；HTTP新建连接≥10万/秒。  三、最低配置要求：配置万兆（SFP+）接口数量≥4，配置千兆光口数量≥6，配置千兆电口数量≥6；配备500GB硬盘。配置三年IPS,AV,URL license。 |
| 外部接入区 | LNS | 2 | 420,000 | 省级单位实现与运营商无线核心网对接 | 一、基本要求：  1.三层路由：静态路由、RIP、OSPF、BGP4、IS-IS；  2.VPN技术：MPLS严格遵循相关标准，支持L3的MPLS VPN，实配GRE、IPSEC、NAT、L2TP、国密等多业务功能；  3.网络管理：SHELL、SNMP V1/V2/V3、Telnet、Rlogin、FTP、TFTP，支持流量监控功能。  二、核心要求：  1.硬件要求：设备支持主控卡、业务板卡完全物理分离，主控槽位≥2，子卡槽位≥8；设备电源槽位数≥2，支持N+N冗余；每子卡槽位可支持100G线速转发；  2.设备性能：交换容量≥110Tbps，包转发率≥24000Mpps。  3.支持全面的快速重路由TE FRR功能,支持基于硬件的BFD故障探测技术，支持单臂BFD。  三、最低配置要求：  配置双主控，冗余电源，10GE光口≥8,千兆SFP光口≥10, 并配置4000认证license，SRv6功能。 |
| 外部接入区 | AAA认证系统 | 1 | 160,000 | 省级单位非专线形式下两定机构接入认证 | 一、基本要求：  1.支持PAP认证，CHAP认证，EAP-MD5认证，AD代理认证，LDAP代理认证，Radius代理认证；  2.支持4G终端接入要求进行SIM卡绑定认证，认证的时间控制，针对接入终端或者用户名判断下发固定的IP地址。  二、核心要求：  1.支持基于TACACS的用户设备操作命令授权、用户Shell属性授权，确保不同用户，对设备拥有不同操作权限  2.支持对用户分组进行管理，可指定用户所属分组，便于策略配置和授权；  3.支持对用户设备操作命令审计，方便记录跟踪；  4.支持将用户上、下线信息，外发到其它上网行为管理服务器，完成基于用户账号的实名审计功能；  5.系统角色支持按组织机构进行分级分权管理，即不同用户拥有不同区域、不同权限。  三、最低配置要求：  1.配置4000 license接入授权。含配套硬件。 |
| 外部接入区 | 国密证书系统 | 1 | 150,000 | 省级单位非专线形式下两定机构国密认证 | 一、基本要求：  1.支持证书模板，提高签发各类证书的灵活性；  2.数据库、配置文件中的敏感数据采用加密方式保存。  二、核心要求：  内置目录服务器，直接提供证书及CRL查询，方便应用系统直接进行证书状态验证及证书下载。  三、最低配置要求：  采用软硬一体化设计，1U，2个千兆电口，支持RSA和国密SM2算法证书的颁发，含配套硬件。 |
| 安全管理区 | 防火墙 | 1 | 110,000 | 安全管理区安全边界，实现安全设备整网信息管控 | 一、基本要求：  1.支持防火墙、应用特征、防病毒、入侵防御、URL、IPSEC VPN等功能；  2.能够实现与接入网关设备联动，安全网关检测到病毒攻击，威胁攻击时主动切断接入端设备。  二、核心要求：  吞吐量≥12Gbps，最大并发连接数≥600万，每秒新建连接数≥20万。  三、最低配置要求：  配置万兆（SFP+）接口数量≥4，配置千兆光口数量≥6，配置千兆电口数量≥6；配备500GB硬盘。 |
| 安全管理区 | 交换机 | 1 | 36,000 | 安全管理区端口扩展，同时对安全设备采集的流量进行复制，起到分流器的作用 | 一、基本要求:  1.支持静态路由、RIP、OSPF、BGP等动态路由协议，支持RIPng、OSPFv3、IS-ISv6、BGP4+，支持MPLS VPN；  2.支持Telnet、Console、SNMP等管理方式。  二、核心要求:  1.最小交换容量≥2Tbps，最小包转发率≥1600Mpps。  三、最低配置要求：  1.双电源、SFP+光口≥48端口，40GE QSFP+≥4端口。 |
| 安全管理区 | 统一网络管理系统 | 1 | 400,000 | 整网设备管理、性能统计、告警监控、SDN功能 | 一、基本要求：  支持在统一的界面上对业务进行360度监控，集中展示包括业务分层路径拓扑，业务相关资源的状态集中呈现，告警与业务自动关联等。  二、核心要求：  采用分布式架构，可以满足五万网元的超大规模网最大100个终端在线操作视图管理设备，实现不同厂商网络、安全设备统一管理，提供IP设备健康检查功能，实现网络和设备健康状态批量自动检测。  三、最低配置要求：  实配≥1000个网元，含配套硬件。 |
| 安全管理区 | 堡垒机 | 1 | 150,000 | 实现对各类帐号、认证、授权和审计的集中管理和控制 | 一、基本要求：  1.支持字符型并发≥1500，图像型并发≥400；  2.支持B/S、C/S两种不同方式的运维接入；  3、支持双机热备部署，实现配置和审计日志实时同步，保证数据高可靠性。  二、核心要求：  1.端口≥6个GE电口；  2.支持图形会话下的文件传输控制。  三、最低配置要求：  实配100个设备管理license，3年维保。 |
| 安全管理区 | 日志审计系统 | 1 | 150,000 | 通过分布式架构提供企业日志的采集、存储和审计 | 一、基本要求：  1.支持在线日志、转储日志二级存储的海量存储；  2.支持异步查询和细粒度的查询。  二、核心要求：  1.最大支持100日志源授权；  2.支持流量实时统计、基础流量分析、应用流量分析、接口流量分析、P2P流量分析；  3.支持对攻击、病毒等威胁事件的统计和分析。  三、最低配置要求：  1.1个console口，存储容量6T，6千兆电口,3年维保。 |
| 安全管理区 | 漏洞扫描 | 1 | 150,000 | 负责各类设备的漏洞扫描和修复 | 一、基本要求：  支持系统扫描、Web扫描、数据库扫描、安全基线检测、弱口令扫描在内的五大扫描能力。  二、核心要求：  支持60000条以上系统特征库。  三、最低配置要求：  6个10/100/1000BASE-T接口、2个SFP插槽，无限扫描IP 授权。 |
| 安全管理区 | 电脑主机杀毒软件 | 1 | 150,000 | 省级统一部署杀毒软件控制中心，负责各级单位办公电脑杀毒 | 一、基本要求：  具备二次开发能力，防止产品后门和用户敏感信息外泄等隐患。  二、核心要求：  防病毒+补丁管理+运维管控+移动储存介质管理。  三、最低配置要求：  统一管理平台和1000 Windows客户端管理授权。 |
| 安全管理区 | APT未知威胁 | 1 | 500,000 | 负责全网流量监测、分层防御，提供一流的针对未知威胁的反躲避能力 | 一、基本要求：  2U服务器结构；固态硬盘250GB，机械硬盘12TB。  二、核心要求：  1.安全沙箱检测能力库升级服务3年License，3年维保；  2.支持多种格式图像文件的检测；  3.支持应用层协议的流量还原；  4.支持与防火墙联动部署。  三、最低配置要求：  标配双电源；包含7个10/100/1000BASE-T管理接口(其中2个管理接口，4个数据接口，1个BMC接口)，4个SFP插槽，2个万兆SFP插槽。 |
| 安全管理区 | 等保测评服务 | 1 | 150,000 | 实现医保业务专网等保三级测评服务 | 等保三级测评服务 |
| 办公区 | 防火墙 | 2 | 32,000 | 省级内部接入区安全边界，开启入侵防御，防病毒等功能 | 一、基本要求：配置三年IPS,AV,URL license，支持USB口。  二、核心要求：吞吐量≥2Gbps，最大并发连接数≥300万，每秒新建连接数≥7万。  三、最低配置要求：千兆接口≥6，万兆光口≥2，冗余电源。 |
| 办公区 | 核心交换机 | 2 | 120,000 | 负责省级医保内部办公人员数据交换 | 一、基本要求：  1.支持静态路由、RIP、OSPF、BGP等动态路由协议，支持RIPng、OSPFv3、IS-ISv6、BGP4+，支持MPLS VPN；  2.支持Telnet、Console、SNMP等管理方式。  二、核心要求：  1.业务槽位≥6，主控槽位≥2，电源槽位数≥2，风扇≥2；  2.最小交换容量≥19Tbps，最小包转发率≥1600Mpps。  三、最低配置要求：  双主控、双电源、10/100/1000M电口≥48端口，SFP千兆光接口≥12端口，SFP+光口≥12端口。 |
| 办公区 | 接入交换机 | 6 | 7,000 | 负责省级医保内部办公人员的有线接入 | 一、基本要求：支持静态路由、RIP路由协议，支持Telnet、Console、SNMP等管理方式。  二、核心要求：最小交换容量≥336Gbps；最小包转发率≥140Mpps。  三、最低配置要求：48个10/100/1000Base-T电接口、4个SFP+光口，冗余电源。 |
| 安全管理区 | 态势感知（可选） | 1 | 1,000,000 | 基于大数据安全分析平台采集丰富的网络数据，实现发现威胁的同时阻断恶意流量 | 一、基本要求：  能够通过态势感知系统跟防火墙、入侵防御设备联动。  二、核心要求：  实现对防火墙和入侵防御系统阻断策略下发，能够在态势感知系统上驱动漏洞扫描设备，并将扫描结果直接在态势感知平台上进行分析和展示。  三、最低配置要求：  3年升级服务。含配套硬件。 |
| 培训服务 | 培训服务（可选） | 1 | 150,000 |  | 含25天培训（两人班），学习课程：路由器、交换机、安全 |

预算规划：

|  |  |  |
| --- | --- | --- |
|  | 金额（万） | 备注 |
| 设备采购 | 527.2（必选部分） | 硬件包含三年维保 |
| 100（可选部分） | 态势感知 |
| 培训服务 | 15 | 含25天培训（两人班），学习课程：路由器、交换机、安全 |
| 设备总计 | 642.2 | |
| 骨干网线路 | 0 | 电子政务外网线路每年（2条/1000M） |
| 骨干网线路 | 0 | 办公资源网线路每年（2条/1000M） |
| 合计 | 642.2 | |

## 市级方案组件与选型建议

市级医保核心骨干网分为骨干路由区，外部接入区和内部办公接入区。

**骨干路由区**

骨干路由区的组成为两台核心上联路由器，两台核心下联路由器。上联路由器负责与省级医保局对接，由河南省医保局管理。河南省医保局部署SDN，实现跨市医保结算业务快速发放。下联路由器负责连接市级骨干网其他区域。

**外部接入区**

外部接入区是实现省级人社、卫健、民政、公安、税务、其他信息资源共享部门以及定点医院、定点药店、商业银行、保险公司等机构的接入。

外部接入区部署两台防火墙作为接入区安全边界，开启入侵防御，防病毒等功能。对进入骨干网流量进行安全过滤。外部接入区部署需部署2台LNS（L2TP网络服务器）和1套AAA系统。LNS设备负责对政务外网、专线链路、有线VPN、无线VPDN实行统一接入，AAA认证系统对非政务外网接入方式的链路进行统一认证。

**内部办公接入区**

内部办公区为市、县（区）级办公网络统一接入区。

市级内部办公区部署一台出口防火墙，开启入侵防御，防病毒等功能，部署两台接入交换机，负责连接各办公设备的有线接入。

市级配置列表：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 区域 | 设备 | 数量 | 预算单价 | 功能 | 建议配置 |
| 骨干路由区 | 路由器 | 4 | 250,000 | 市级上联至省级需2台路由器，市级下联至横向接入区需2台路由器，实现医保业务跨市交互 | 一、基本要求：  1.三层路由：静态路由、RIP、OSPF、BGP4、IS-IS；  2.VPN技术：MPLS严格遵循相关标准，支持L3的MPLS VPN、SRv6,实配GRE、IPSEC、NAT、L2TP等多业务功能；  3.网络管理：SHELL、SNMP V1/V2/V3、Telnet、Rlogin、FTP、TFTP，支持NetFlow或IPFIX流量监控功能，SDN控制器集中管理。  二、核心要求：  1.硬件要求：主控槽位≥2、子卡槽位≥8，2个电源槽位，每子卡槽位可支持100G线速转发；  2.交换容量≥9Tbps,最小包转发率≥800Mbpss。  3.支持全面的快速重路由TE FRR功能,支持基于硬件的BFD故障探测技术，支持单臂BFD。  三、最低配置要求：  1.配置双主控，冗余电源，10GE光口≥6,千兆SFP光口≥4，SRv6功能。 |
| 外部接入区 | 防火墙 | 2 | 150,000 | 市级横向同级资源共享部门及两定机构安全边界 | 一、基本要求：  1.支持防火墙、应用特征、防病毒、入侵防御、URL、IPSEC VPN等功能；  2.能够实现与接入网关设备联动，安全网关检测到病毒攻击，威胁攻击时主动切断接入端设备。  二、核心要求：整机防火墙吞吐≥20Gbps；HTTP并发连接≥400万；HTTP新建连接≥10万/秒。  三、最低配置要求：配置万兆（SFP+）接口数量≥4，配置千兆光口数量≥6，配置千兆电口数量≥6；配备1000GB硬盘。配置三年IPS,AV,URL license。 |
| 外部接入区 | LNS | 2 | 450,000 | 市级单位实现与运营商无线核心网对接 | 一、基本要求：  1.三层路由：静态路由、RIP、OSPF、BGP4、IS-IS；  2.VPN技术：MPLS严格遵循相关标准，支持L3的MPLS VPN，实配GRE、IPSEC、NAT、L2TP、国密等多业务功能；  3.网络管理：SHELL、SNMP V1/V2/V3、Telnet、Rlogin、FTP、TFTP，支持流量监控功能。  二、核心要求：  1.硬件要求：设备支持主控卡、业务板卡完全物理分离，主控槽位≥2，子卡槽位≥8；设备电源槽位数≥2，支持N+N冗余；每子卡槽位可支持100G线速转发；  2.设备性能：交换容量≥110Tbps，包转发率≥24000Mpps。  3.支持全面的快速重路由TE FRR功能,支持基于硬件的BFD故障探测技术，支持单臂BFD。  三、最低配置要求：  配置双主控，冗余电源，10GE光口≥8,千兆SFP光口≥10, 并配置4000认证license，SRv6功能。 |
| 外部接入区 | AAA认证系统 | 1 | 170,000 | 市级单位非专线形式下两定机构接入认证 | 一、基本要求：  1.支持PAP认证，CHAP认证，EAP-MD5认证，AD代理认证，LDAP代理认证，Radius代理认证；  2.支持4G终端接入要求进行SIM卡绑定认证，认证的时间控制，针对接入终端或者用户名判断下发固定的IP地址。  二、核心要求：  1.支持基于TACACS的用户设备操作命令授权、用户Shell属性授权，确保不同用户，对设备拥有不同操作权限；  2.支持对用户分组进行管理，可指定用户所属分组，便于策略配置和授权；  3.支持对用户设备操作命令审计，方便记录跟踪；  4.支持将用户上、下线信息，外发到其它上网行为管理服务器，完成基于用户账号的实名审计功能；  5.系统角色支持按组织机构进行分级分权管理，即不同用户拥有不同区域、不同权限。  三、最低配置要求：  1.配置5000 license接入授权，含配套硬件。 |
| 外部接入区 | 国密证书系统 | 1 | 150,000 | 市级单位非专线形式下两定机构国密认证 | 一、基本要求：  1.支持证书模板，提高签发各类证书的灵活性；  2.数据库、配置文件中的敏感数据采用加密方式保存。  二、核心要求：  内置目录服务器，直接提供证书及CRL查询，方便应用系统直接进行证书状态验证及证书下载。  三、最低配置要求：  采用软硬一体化设计，1U，2个千兆电口，支持RSA和国密SM2算法证书的颁发，含配套硬件。 |
| 办公区 | 防火墙 | 1 | 32,000 | 市级内部接入区安全边界，开启入侵防御、防病毒等功能 | 一、基本要求：配置三年IPS,AV,URL license，支持USB口。  二、核心要求：吞吐量≥2Gbps，最大并发连接数≥300万，每秒新建连接数≥7万。  三、最低配置要求：千兆接口≥6，万兆光口≥2，冗余电源。 |
| 办公区 | 交换机 | 4 | 7,000 | 负责市级医保内部办公人员的有线接入 | 一、基本要求：支持静态路由、RIP路由协议，支持Telnet、Console、SNMP等管理方式。  二、核心要求：最小交换容量≥336Gbps；最小包转发率≥140Mpps。  三、最低配置要求：48个10/100/1000Base-T电接口、4个SFP+光口，冗余电源。 |
| 安全管理区 | 堡垒机  （可选） | 1 | 150,000 | 实现对各类帐号、认证、授权和审计的集中管理和控制 | 一、基本要求：  1.支持字符型并发≥1500，图像型并发≥400；  2.支持B/S、C/S两种不同方式的运维接入；  3、支持双机热备部署，实现配置和审计日志实时同步，保证数据高可靠性。  二、核心要求：  1.端口≥6个GE电口；  2.支持图形会话下的文件传输控制。  三、最低配置要求：  实配100个设备管理license，3年维保。 |
| 安全管理区 | 杀毒软件（可选） | 1 | 0 |  | 与省级平台共用 |

预算规划：

|  |  |  |
| --- | --- | --- |
|  | 金额（万） | 备注 |
| 设备采购 | 258（必选部分） | 硬件包含三年维保 |
| 15（可选部分） | 安全管理区（堡垒机） |
| 设备总计 | 273 | |
| 骨干网线路 | 0 | 电子政务外网线路每年（2条/100M） |
| 骨干网线路 | 0 | 办公资源网线路每年（2条/100M） |
| 线路总计 | 0 | |
| 合计 | 273 | |

## 县（区）级方案组件与选型建议

县（区）级主要为县（区）级医保局办公网，根据各级医保局工作人员数量，确定园区网接入交换机数量。园区网的出口路由器，负责出口路由链路选择。园区网的出口部署防火墙，开启入侵防御，防病毒等功能。接入交换机负责各办公设备的有线接入，两台交换机采用堆叠技术，实现县（区）级医保局办公数据内部交换。

办公网设备可以直接部署在办公室楼层弱电间内机柜，无需单独建设机房。

配置列表：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 区域 | 设备 | 数量 | 预算单价 | 功能 | 建议配置 |
| 办公区 | 出口路由器 | 1 | 10000 | 负责县（区）级医保内部办公人员的出口路由 | 一、基本要求：  1.三层路由：静态路由、RIP、OSPF、BGP4、IS-IS；  2.VPN技术：MPLS严格遵循相关标准，支持L3的MPLS VPN，配置GRE、IPSEC、NAT、L2TP等多业务功能；  3.网络管理：SHELL、SNMP V1/V2/V3、Telnet、Rlogin、FTP、TFTP，支持流量监控功能。  二、核心要求：  1.最小包转发率≥9Mpps。  三、最低配置要求：  1.千兆电口≥4个，千兆光口≥4个，扩展插槽≥4，冗余电源。 |
| 办公区 | 出口防火墙 | 1 | 12000 | 负责县（区）级医保内部办公人员的出口管控，开启入侵防御、防病毒等功能 | 一、基本要求：  1.支持扩展AI应用识别、IPS入侵防御及AV防病毒功能。  二、核心要求：  1.防火墙吞吐800M，并发连接30万，每秒新建连接3000，IPSEC VPN吞吐20M。可扩展SSL VPN模块。  三、最低配置要求：  1.5个千兆电口，1个Combo口，含IPSEC VPN模块。 |
| 办公区 | 接入交换机 | 2 | 4000 | 负责县（区）级医保内部办公人员的有线接入 | 一、基本要求：  1.支持静态路由、RIP路由协议，支持Telnet、Console、SNMP等管理方式。  二、核心要求：  1.交换容量≥336Gbps，包转发率≥80Mpps。  三、最低配置要求：  1.48个千兆电口，4个千兆SFP，提供三年维保服务。 |

预算规划：

|  |  |  |
| --- | --- | --- |
|  | 金额（万） | 备注 |
| 设备采购 | 3 | 硬件包含三年维保 |
| 设备总计 | 3 | |
| 骨干网线路 | 0 | 20M电子政务外网或办公资源网 |
| 线路总计 | 0 | |
| 合计 | 3 | |

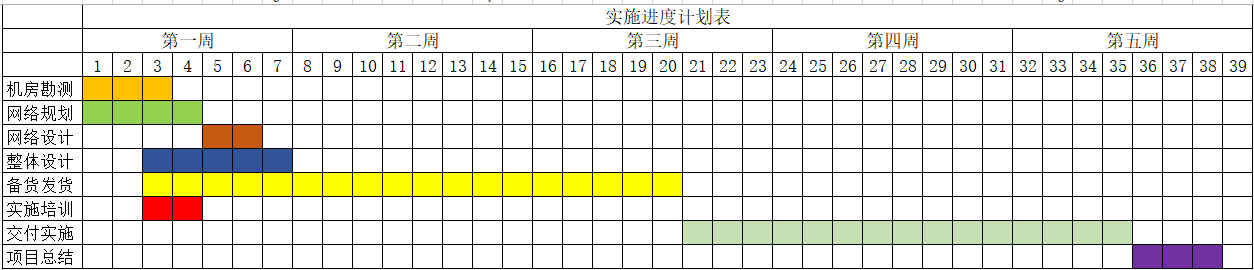
# 项目实施方案

针对本工程质量要求高、工程体量大、专业系统复杂、工期紧迫等特点，参考类似项目交付经验，结合本工程的具体内容和特点，按照“结构合理、精干高效、分工协作”的原则，项目组设项目经理、项目技术负责人等项目领导岗位并配备数量足够、专业齐全、大型项目施工管理经验丰富、年富力强、高素质的施工管理及技术人员，对项目施工实施全过程、全方位的“四控制”（即进度、质量、成本、安全控制）、“三管理”（即现场（要素）、信息、合同管理）和“一协调”（即组织协调），确保实现项目管理的各项目标。

## 实施计划与内容

根据要求应在设备到货后两周内完成项目实施，包括需求分析与规划设计、设备到货、硬件安装、布线调试、测试等工作，具备试运行条件。

整体计划：



由于工期紧张，设备量大，施工人员计划多组分不同区域进行实施。项目进展由专业的项目经理和技术负责人全天次跟踪，统筹协调到货、机房、人员。通过最优化项目进度安排，保证项目在自到货之日起两周内完工。

备注：本计划是根据客户需求制定，具体时间需要根据实际的合同签署确定，最终计划可以根据客户要求调整或者增加资源投入，以满足客户实际工期要求。

## 项目建设实施方案

### 系统架构设计

1、总体架构：骨干网分省、市二级架构，每一级架构包含骨干路由器，安全边界区和接入区。骨干网为内部用户和外部接入单位提供访问省中心的通道。省-市之间通过电子政务外网+办公资源网实现互联。

2、路由方案设计：以GRE穿越电子政务外网方案为例。IGP 协议使用ospf为例，政务外网 MCE 与政务外网 PE 间协议使用 EBGP。医保各路由器配置ospf进程 100，各直连接口地址宣告进ospf，在政务外网MCE设备上 BGP 和 ospf 做路由互引。

3、IP规划设计：本次IP地址主要分为接入地址、设备互联地址、loopback地址、数据中心地址等。接入地址用于各单位的接入；设备互联地址用于路由器、防火墙等三层设备之间的互联；loopback地址用于设备管理以及路由协议的router ID。数据中心地址用于数据中心内部。

总体IP规划如下表：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **类别** | **地址数量** | **地址段** |
| 1 | 接入地址 | 768个C | 10.82.0.0-10.84.255.254 |
| 2 | 设备互联地址 | 64个C | 10.85.0.0-10.85.63.254 |
| 3 | loopback地址 | 32个C | 10.85.64.0-10.85.95.254 |
| 4 | 数据中心地址 | 160个C | 10.85.96.0-10.85.255.254 |

### 安装实施服务

**1 现场实施条件勘查**

根据系统架构和应用系统需求，在设备上架前对供电及机柜等信息进行工勘，输出机柜和设备的详细设计，包括LLD（解决方案详细设计文档）和机柜设计图。

**2 安装实施：**

根据解决方案详细设计及相关产品安装调测指导书，完成设备的部署和配置，主要包括如下内容：

1、制定实施计划；

2、硬件部署：包括工前机房环境检查，设备搬运、开箱验货、机柜安装、设备上架、信号线缆布放、标签制作和粘贴、设备上下电检查等；

3、网络部署和配置

配置路由器、防火墙和交换机：包括版本升级、管理配置、路由配置、vlan配置、互联配置、安全配置等；

|  |  |
| --- | --- |
| **软件安装调测一览表** | |
| **编号** | **任务** |
| **1.1** | **软件督导** |
| 1.1.1 | 提供软件安装技术指导 |
| **1.2** | **测试工具及仪表准备** |
| **1.3** | **单机调测** |
| 1.3.1 | 设备硬件运行状况检查 |
| 1.3.2 | 设备告警信息检查处理 |
| 1.3.3 | 开局软件版本加载 |
| 1.3.4 | 设备版本运行状态检查 |
| 1.3.5 | 软件调试 |
| 1.3.6 | 基本数据配置 |
| 1.3.7 | 单机基本功能测试 |
| **1.4** | **单机数据配置** |
| 1.4.1 | VLAN配置 |
| 1.4.2 | 二层VPN配置 |
| 1.4.3 | 用户认证计费方式配置 |
| 1.4.4 | IP业务配置(DNS、NTP、ACL、NAT等） |
| 1.4.5 | 路由协议配置(OSPF、IS-IS、BGP协议) |
| 1.4.6 | 组播配置 |
| 1.4.7 | MPLS配置 |
| 1.4.8 | VPN配置 |
| 1.4.9 | Qos配置 |
| 1.4.10 | 网络管理配置 |
| 1.4.11 | 网络安全性配置 |
| 1.4.12 | 网络特性、可靠性配置 |
| 1.4.13 | 软硬件问题处理 |
| 1.4.14 | 单机软件自检 |
| 1.4.15 | 非本次工程设备的单机数据配置 |
| **1.5** | **全网联调** |
| 1.5.1 | 设备间链路调测 |
| 1.5.2 | 全网IP业务配置联调 |
| 1.5.3 | 全网路由协议配置联调 |
| 1.5.4 | 全网组播配置联调 |
| 1.5.5 | 全网MPLS配置联调 |
| 1.5.6 | 全网VPN配置联调 |
| 1.5.7 | 全网Qos配置联调 |
| 1.5.8 | 全网网络特性、可靠性配置联调 |
| **1.6** | **配置正确性、规范检查** |
| **1.7** | **输出过程文档** |

**4 网络系统联调测试服务内容：**

测试用例设计：根据合同、技术规范书等内容，设计网络系统的测试用例，主要分为单机基础调试、目标网络联网调测、网络迁移/割接、业务验证。

1) 单机基础调试

设备基础调试时，工程师需配带以下材料和工具，测试单机运行状态。

a. 在官方网站上下载需要升级的软件版本

b. PC机，具有以太网卡和终端仿真软件(如CRT)

c. 控制口的串行线

d. 以太网双绞线和多模(LC-LC)和多模SC-SC各一对

e. 螺丝刀一套

f. 标准标签纸，标签用标准的标签纸打印（本端端口+对端接口描述写）

2) 目标网络联网调试

目标网络联网调试准备以下工具和输出材料

a. PC机，具有以太网卡和CRT软件

b. 串口线缆

c. 设备互联和管理地址

d. 最终配置文件

目标功能联网调测需要验证局域网互联互通，冗余链路和设备的可靠性，达到全网互通，目标流量按照规划走向达到目标网络。联网验收输出主备线路和设备切换操作日志。

3) 业务验证

业务验证主要验证网络的互联互通，验证流量走向按照预定规划流动。

### 项目实施保障

合同签定后至验收前，将根据项目采用的服务方式及工程技术服务要求提供项目实施周期内的项目实施和管理服务，并保证自签订合同之日起30个工作日完成项目实施工作。

实施方案在施工开工前必须复核完毕，且实施方案的复核由项目经理、售后工程师负责，必须明确复核内容，复核人员及复核方法，复核结果汇总项目团队，发现问题，及时上报项目经理，其结果作为技术资料归档。

技术、质量的交底工作是施工过程基础管理中一项不可缺少的重要工作内容，质量管理团队需要制定项目整体质量管理流程，流程内容交底必须采用书面签证确认形式，同时提供中间形成的记录与报告。在验收环节，需要客户参与进来。

### 应急预案及措施

应提高工程实施安全、质量、进度管理水平，加强工程实施应急体系建设，积极做好工程实施日常管理工作，开展应急教育和培训工作，建立完善的工程实施应急管理制度，提高应对工程实施过程中突发事件的能力。

建立工程实施应急预警和事件快速反应机制，建立高效的事件汇报渠道，强化人力、物力、财力储备，增强应急处理能力。保证对工程实施应急事件做到早发现、早报告、早处理、早恢复等环节的紧密衔接，一旦出现影响工程实施事件，快速反应，及时准确处置。

明确工程实施应急响应工作的角色和职责，保证各项工作责任到人，建立应急响应各项工作的处理流程，实现应急响应工作的规范化、制度化和流程化。

为保证应急行动的能力，以提高处理应急事件的能力，检验物资器材的完好情况。

首先，由应急领导小组确定应急响应演练的目标和应急响应演练的范围；

按领导小组的要求，信工作小组制定应急响应演练的方案，并调配应急响应演练所需的各项资源。在必要时，由信息安全领导小组协调应急响应演练过程中涉及的部门和单位；

工作小组组织相关部门和单位进行应急响应演练；

领导小组对应急演练进行评估，并通报应急响应演练结果；

领导小组总结经验，根据演练结果对应急预案的更新，并对本单位的应急工作进行整改；

在每次应急响应过程结束之后，领导小组应针对应急响应工作过程中遇到的问题，分析应急响应预案的科学性和合理性，针对预案中的问题向信息安全领导小组提出修改建议。信息安全领导小组组织人员对修改意见进行评估，修改后的预案应经评估通过后，发布实施。

# 网络运维设计

网络管理系统统一管理全省设备，为方便地市管理员使用，系统要能提供分权分域管理方式，实现不同权限管理员管理不同区域的设备。

网络管理系统需要支持异地灾备功能，实现业务系统的高可靠性。主备业务系统间的数据可以实时同步，主机出现故障，可以自动切换到备机系统，主备业务系统都是双活状态，无切换时间。

## 网管基本功能设计

从两个方面进行网管基本功能设计，一方面是对设备的管理，另一面是针对业务的管理，对VPN等业务的管理能力是更为关注的特性。

1、拓扑集中监视

提供统一拓扑发现功能，全网监控，可以实时监控所有设备的运行状况，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，拓扑功能包括：拓扑自动发现、拓扑业务状态显示、拓扑告警显示、时钟视图功能。

2、精确故障管理

部署Telemetry技术，满足大规模、高性能的网络监控需求，支持智能运维系统管理更多设备、监控数据拥有更高精度和更加实时、监控过程对设备本身功能和性能影响小，为网络问题的快速定位、网络质量优化调整提供了重要的大数据基础，将网络质量分析转换为大数据分析，有力的支撑了智能运维的需要。

支持对全网设备的故障、运行状态进行实时监控、历史统计并提供协助排障的手段，故障管理功能支持如下功能：支持多种告警级别、告警多种通知方式、支持告警相关性分析、告警屏蔽、告警统计、告警转储、告警同步、告警跳转。

3、设备配置文件管理

提供网络设备丰富的配置管理能力，网络管理员需要定期备份设备的配置文件，跟踪设备配置变化，从而保证一旦发生网络故障时，可以使用历史配置备份将网络设备立刻恢复正常。

设备配置文件的批量备份和恢复等集中管理设备配置变化，主动备份配置文件 灵活的设备配置文件比较功能，包括指定设备的运行配置和启动配置的比较、不同设备间的配置文件比较等，管理员能够快速查看设备配置差异，迅速定位导致问题的配置命令。

4、管理数据可靠

网管服务器数据库存储文件有两种，一种用来存储数据，另一种用来存储该数据库运行的日志信息。为保证数据安全，应定期进行数据库的备份。

网管与设备的数据一致性，网络管理系统需要提供多种功能来保证网元配置数据安全和一致性。包括上载、下载、一致性校验、同步、复制、预配置和初始化网管侧网元数据等。

5、网管业务管理设计

通过网管软件提供端到端的VPN专线运营的可视化业务管理能力，简化业务管理，提供业务配置、管理效率。跨域管理，从VPN到IP承载，到物理层快速定位 ，以及网络级的可视化管理，故障定位等功能。

6、VPN业务端到端快速发放

医疗保障专网通过VPN承载业务，对于VPN来说，如果采用传统的手工方法需要配置命令行，建立tunnel隧道，配置VRF实例等过程，不仅对人的要求高而且容易因为人为因素配置错误影响客户单位的业务。数据承载网的统一网管，必须简化这个过程，降低对人的要求：

VPN的创建图形化，参数模板化，通过层次化、可视化网络管理，提供完善的多层管理能力，实时获取网络承载关系，可视化操作，无须记忆命令行端到端可视化VPN及传输业务发放，利用业务模板创建业务，提升业务发放效率。

提供模板配置功能，在配置VPN的业务时，可以选择之前预定义的模板，快速设置业务参数，提高配置效率。

提供Tunnel和VPN等业务导入功能，可以从excel中配置业务参数，直接导入到管理系统中，进行业务参数检查后可以直接进行业务下发。

提供批量部署Tunnel的功能，选择网元和组网规则后，自动计算所有的Tunnel业务并统一下发配置，提高Tunnel部署效率。

提供端到端的业务管理，可以查看整个业务的业务状态，可以查看业务的路由信息，可以对路由进行调整。可以查看VPN业务的承载关系，了解资源使用情况。

7、VPN业务端到端故障定定位功能

通过部署IFIT，直接对业务报文进行测量，从而得到IP网络的真实丢包率、时延等性能指标，IFIT部署方便、统计精度高，有效提高了业务端到端故障定位能力。

同时医疗保障专网需要网管能够支持MPLS VPN跨域业务管理，实现VPN路径可视，用户可以通过图形界面了解业务的流量分布，做到底层链路的快速故障定位。

层次化展现“VPN路径”的承载关系，显示各层次业务路径的告警状态，协助用户实现Tunnel层，IP层，链路层业务的故障定界。

8、SDN技术实现网络流量可视和调优

医疗保障专网网络建设时，要求网络带宽资源使用最优，同时兼顾业务的差异化管理，保证优先满足高优先级业务的需求。同时提供全网业务约束条件和拓扑链路属性信息的集中管理，集中分配全网带宽资源，方便和强化用户对业务和拓扑的查询、规划及维护。

9、智能化故障管理

在网管的告警方面，通过告警管理功能，能够统一查看所有设备的告警信息，包括接入和IP的故障信息，可以查看告警影响的业务，支持故障定位。为了提高维护效率，还需要提供以下特性，提高告警诊断效率。

以业务为中心故障诊断。可以通过告警查看告警所影响的业务和影响的用户范围，快速了解到告警所影响的范围，做出轻重缓急的判断。

告警过滤，聚焦关键告警。并且关联同类告警，减少告警数量，使运维人员能聚焦主要问题。

## 运行维护建设要求

### 运维服务概览

维护团队将严格按照服务流程，提供维保合同规定的各项服务，做到逐项落实，并根据实施细则认真履行，确保业务的顺畅运行。考虑网络地位非常重要，为了更好的向医保局提供维护技术支持服务，为医保局提供如下服务方案：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 类别 | 服务内容 | 服务内容描述 |
| 1 | 服务团队 | 服务团队 | 对于医保局客户，成立售后服务团队，并设置服务代表，负责服务的统一接口，受理用户提出的相关服务问题，制定服务计划，定期与用户沟通以监控服务质量，并在服务实施中负责相关协调，安排团队成员定期对用户系统及设备运行情况进行讨论评估以便提前发现并消除运行隐患。对于用户的故障申告，服务代表将立刻组织技术支持团队，帮助用户恢复业务，排除故障。 |
| 2 | 保修期限 | 免费保修服务期限 | 满足本项目产品提供的三年免费保修服务。 |
| 3 | 技术支持服务 | 7X24小时技术支持服务热线 | 7×24覆盖，实时响应。 |
| 4 | 远程问题处理 | 7×24覆盖，实时响应。 |
| 5 | 在线技术支持 | 技术信息共享和补丁下载。 |
| 6 | 备件先行 | 省局与地市7×24×4，实时响应。县级  7×10×ND送达 |
| 7 | 现场工程师硬件更换 |
| 8 | 现场问题处理 |
| 9 | 驻场服务 | 驻场服务是安排专家与客户工程师一起在客户现场工作，深入地理解客户网络运营、日常维护、人员培养等方面的现状，致力于提供网络产品咨询和主动运维服务，可协助客户优化网络系统和预防重大故障的发生，并在发生故障时可以快速解决故障。 |
| 10 | 故障管理服务 | 故障管理服务是当客户网络系统出现故障时，客户可直接联系专属技术专家参与故障处理。 |
| 11 | 软件版本管理 | 提供软件战略管理、软件版本推荐、软件主动预警分析服务。 |
| 12 | 重大事件保障服务 | 重大活动、重要节假日安保期间以及产品安装、系统变更和迁移、系统升级等的现场支持保障服务。 |
| 13 | 巡检服务 | 对于部署的产品，提供对系统和设备进行全面检查的巡检服务。 |
| 14 | 培训服务 | 产品技术培训 | 产品技术、故障处理等技术培训。 |

### 运维服务内容

“运维”是运行维护的简称，包括运行和维护两方面。对于运行管理来说，主要是面向网络承载的业务，侧重监视、控制、调度；对于维护管理来说，主要是面向网络设备（路由器、交换机、服务器等），侧重软硬件的维护、测试、管理。网络必须在面向业务和面向网络两个层面开展各项维护服务工作。

从工作内容角度衡量，网络必须开展运行监控、设备维护、配置管理、故障管理、变更管理、资源管理、信息管理、安全管理、业务开通、故障响应等项工作，才能保证全网的稳定运行及对已承载的业务提供有力支撑。

运行监控：包括对链路、设备状态的实时监测，网络流量的实时监控，安全事件的实时监控及面向部委业务应用的实时监控等。

设备维护：包括设备的定期检测、保养，数据备份，配置检查，主备功能的倒换测试等。

配置维护：管理网络的配置参数，按要求完成路由、访问控制、策略控制、设备端口等数据的配置、修改和删除。

故障管理：包括制定故障管理办法，建立故障资料库，故障发生时快速定位故障，调度全网进行解决，控制故障的影响等。

资源管理：包括资源数据库的建立，定期进行资源数据的整理、核对、统计等，备品备件的使用管理，资源使用的请求响应等。

安全管理：包括安全策略的制订与变更，安全配置检查，安全事件响应，安全日志的分析、审计，以及定期的安全预警等工作。

变更管理：指设备、资源、配置的变更管理工作，以及业务的割接管理工作，包括制定变更管理办法、提出变更申请、变更的审核与实施，以及变更的响应等。

信息管理：通过网络运行情况的统计和分析，为领导、其他相关部门提供准确的网络运行数据。

故障响应：实时响应客户网络故障申告，全程跟踪、协调处理并反馈信息；对故障处理信息进行统计和分析，向客户提供故障处理报告、网络运行分析报告。

业务开通：按照相关接口部门（如工程技术部门、客户服务部门等），制定的网络、业务开通方案，完成具体的设备配置、尾纤跳接、开通测试等工作。

### 驻场服务工作内容

负责客户所有购买原厂服务的设备及产品的技术服务支持，并输出运营周报/月报。

负责客户所有购买了原厂服务的设备的例行检查服务及报告输出。

客户界面例行检查监控项目请参考各产品维护指南并根据项目具体情况定制例行检查计划，并通过客户审核。

按照相关服务条款，负责在第一时间尽快处理客户设备重大故障及疑难故障；负责重大故障处理时的问题单升级、问题单跟踪，及收集问题单相关信息。

### 质保内容

与设备同步提供3年的原厂维保服务。

维保期间提供7×24小时热线受理，7×24小时远程问题处理和7×24小时在线技术支持。

1、远程问题处理

工程师在接到网络或系统故障申报后，将首先进行远程故障分析与处理，及时排除故障。远程问题处理包括电话支持和远程接入。

2、备件先行服务

备件先行服务旨在满足您的紧急要求，提高响应速度，为您提供更快速服务。

备件先行服务是指在通过您的备件服务申请后，提前提供更换件给您，而您只需要在收到提供的更换部件后的30自然日内将故障件返回指定接收点即可，故障件送达的物流费用需要您承担，邮寄返回过程中发生损坏和遗失由您承担相关责任；逾期未返回的将视为您购买，将于下一个收款周期开具发票；并且在超期备件未核销前，会将服务降为备件更换服务，即收到您返回的坏件后在约定时间内将可用备件送达指定收货点。

### 培训内容

可以提供20人的用户现场技术培训、不少于10人天的原厂课程集中培训（包括产品使用培训、各项产品操作技能等）；提供相关软件说明文档、管理和配置指南手册、使用手册和故障定位/排除指南手册。

提供全面、详细的培训方案和培训计划，提供有经验的授课教师和标准化的培训课程。

培训内容如下：

路由器，防火墙，交换机产品硬件介绍，VRP快速入门，IP路由等相关知识。

# 域名规划

域名规划参照《全国医疗保障系统很业务区骨干网络建设指南》内域名规划原则，采用：省级行政区域名+市级简拼+“.”+hsip. gov.cn。详细内容如下：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 市级节点名称 | 行政区域名 | 域名 |
| 1 | 郑州市 | zz | henzz.hsip.gov.cn |
| 2 | 开封市 | kf | henkf.hsip.gov.cn |
| 3 | 洛阳市 | ly | henly.hsip.gov.cn |
| 4 | 平顶山市 | pds | henpds.hsip.gov.cn |
| 5 | 安阳市 | ay | henay.hsip.gov.cn |
| 6 | 鹤壁市 | hb | henhb.hsip.gov.cn |
| 7 | 新乡市 | xx | henxx.hsip.gov.cn |
| 8 | 焦作市 | jz | henjz.hsip.gov.cn |
| 9 | 濮阳市 | py | henpy.hsip.gov.cn |
| 10 | 许昌市 | xc | henxc.hsip.gov.cn |
| 11 | 漯河市 | lh | henlh.hsip.gov.cn |
| 12 | 三门峡市 | smx | hensmx.hsip.gov.cn |
| 13 | 南阳市 | ny | henny.hsip.gov.cn |
| 14 | 商丘市 | sq | hensq.hsip.gov.cn |
| 15 | 信阳市 | xy | henxy.hsip.gov.cn |
| 16 | 周口市 | zk | henzk.hsip.gov.cn |
| 17 | 驻马店市 | zmd | henzmd.hsip.gov.cn |
| 18 | 济源市 | jy | henjy.hsip.gov.cn |

# IP地址规划

IP地址配置思路如下：

本次IP地址主要分为接入地址、设备互联地址、loopback地址、数据中心地址等。接入地址用于各单位的接入；设备互联地址用于专网各路由器之间以及专网路由器与电子政务外网MCE路由器之间的互联；loopback地址用于设备管理以及路由协议的router ID。数据中心地址用于数据中心内部。

总体IP规划如下表：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **类别** | **地址数量** | **地址段** |
| 1 | 接入地址 | 768个C | 10.82.0.0-10.84.255.254 |
| 2 | 设备互联地址 | 64个C | 10.85.0.0-10.85.63.254 |
| 3 | loopback地址 | 32个C | 10.85.64.0-10.85.95.254 |
| 4 | 数据中心地址 | 160个C | 10.85.96.0-10.85.255.254 |

## 接入地址分配

每个地级市分配32个C类地址用于各单位接入骨干网。由于郑州市规模较大，分配64个C类地址。省核心单独分配64个C类地址用于接入。省直管市分配8个C类地址，考虑到未来5年的业务扩展，预留40个C类地址。

|  |  |  |
| --- | --- | --- |
| **序号** | **用途** | **接入地址段** |
| 1 | 省端 | 10.82.0.1 - 10.82.63.254 |
| 2 | 郑州 | 10.82.64.1 - 10.82.127.254 |
| 3 | 开封 | 10.82.128.1 - 10.82.159.254 |
| 4 | 洛阳 | 10.82.160.1 - 10.82.191.254 |
| 5 | 平顶山 | 10.82.192.1 - 10.82.223.254 |
| 6 | 安阳 | 10.82.224.1 - 10.82.255.254 |
| 7 | 鹤壁 | 10.83.0.1 - 10.83.31.254 |
| 8 | 新乡 | 10.83.32.1 - 10.83.63.254 |
| 9 | 焦作 | 10.83.64.1 - 10.83.95.254 |
| 10 | 濮阳 | 10.83.96.1 - 10.83.127.254 |
| 11 | 许昌 | 10.83.128.1 - 10.83.159.254 |
| 12 | 漯河 | 10.83.160.1 - 10.83.191.254 |
| 13 | 三门峡 | 10.83.192.1 - 10.83.223.254 |
| 14 | 南阳 | 10.83.224.1 - 10.83.255.254 |
| 15 | 商丘 | 10.84.0.1 - 10.84.31.254 |
| 16 | 信阳 | 10.84.32.1 - 10.84.63.254 |
| 17 | 周口 | 10.84.64.1 - 10.84.96.254 |
| 18 | 驻马店 | 10.84.96.1 - 10.84.127.254 |
| 19 | 济源 | 10.84.128.1 - 10.84.135.254 |
| 20 | 巩义 | 10.84.136.1 - 10.84.143.254 |
| 21 | 兰考 | 10.84.144.1 - 10.84.151.254 |
| 22 | 汝州 | 10.84.152.1 - 10.84.159.254 |
| 23 | 滑县 | 10.84.160.1 - 10.84.167.254 |
| 24 | 长垣 | 10.84.168.1 - 10.84.175.254 |
| 25 | 邓州 | 10.84.176.1 - 10.84.183.254 |
| 26 | 永城 | 10.84.184.1 - 10.84.191.254 |
| 27 | 固始 | 10.84.192.1 - 10.84.199.254 |
| 28 | 鹿邑 | 10.84.200.1 - 10.84.207.254 |
| 29 | 新蔡 | 10.84.208.1 - 10.84.215.254 |
| 30 | 预留 | 10.84.216.1 - 10.84.255.254 |

## 设备互联地址分配

设备互联地址分为专网内部互联地址、专网与电子政务外网MCE路由器互联地址和电子政务外网互联地址3类。

每个地级市分配1个C类地址用于专网内部互联以及专网与电子政务外网MCE路由器互联，1个C类地址用于电子政务外网互联。由于郑州市规模较大，分配2个C类地址用于专网内部互联以及专网与电子政务外网MCE路由器互联，2个C类地址用于电子政务外网互联。省核心单独分配4个C类地址用于互联。每四个省直管市共用一个C类地址用于专网内部互联以及专网与电子政务外网MCE路由器互联，1个C类地址用于电子政务外网互联。考虑到未来5年的业务扩展，预留18个C类互联地址。

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **用途** | **专网互联地址段** | **电子政务外网互联地址段** |
| 1 | 省端 | 10.85.0.1 - 10.85.1.254 | 10.85.32.1 - 10.85.33.254 |
| 2 | 郑州 | 10.85.2.1 - 10.85.3.254 | 10.85.34.1 - 10.85.35.254 |
| 3 | 开封 | 10.85.4.1 - 10.85.4.254 | 10.85.36.1 - 10.85.36.254 |
| 4 | 洛阳 | 10.85.5.1 - 10.85.5.254 | 10.85.37.1 - 10.85.37.254 |
| 5 | 平顶山 | 10.85.6.1 - 10.85.6.254 | 10.85.38.1 - 10.85.38.254 |
| 6 | 安阳 | 10.85.7.1 - 10.85.7.254 | 10.85.39.1 - 10.85.40.254 |
| 7 | 鹤壁 | 10.85.8.1 - 10.85.8.254 | 10.85.40.1 - 10.85.40.254 |
| 8 | 新乡 | 10.85.9.1 - 10.85.9.254 | 10.85.41.1 - 10.85.41.254 |
| 9 | 焦作 | 10.85.10.1 - 10.85.10.254 | 10.85.42.1 - 10.85.42.254 |
| 10 | 濮阳 | 10.85.11.1 - 10.85.11.254 | 10.85.43.1 - 10.85.43.254 |
| 11 | 许昌 | 10.85.12.1 - 10.85.12.254 | 10.85.44.1 - 10.85.44.254 |
| 12 | 漯河 | 10.85.13.1 - 10.85.13.254 | 10.85.45.1 - 10.85.45.254 |
| 13 | 三门峡 | 10.85.14.1 - 10.85.14.254 | 10.85.46.1 - 10.85.46.254 |
| 14 | 南阳 | 10.85.15.1 - 10.85.15.254 | 10.85.47.1 - 10.85.47.254 |
| 15 | 商丘 | 10.85.16.1 - 10.85.16.254 | 10.85.48.1 - 10.85.48.254 |
| 16 | 信阳 | 10.85.17.1 - 10.85.17.254 | 10.85.49.1 - 10.85.49.254 |
| 17 | 周口 | 10.85.18.1 - 10.85.18.254 | 10.85.50.1 - 10.85.50.254 |
| 18 | 驻马店 | 10.85.19.1 - 10.85.19.254 | 10.85.51.1 - 10.85.51.254 |
| 19 | 济源 | 10.85.20.1 - 10.85.20.63 | 10.85.52.1 - 10.85.52.63 |
| 20 | 巩义 | 10.85.20.65 - 10.85.20.127 | 10.85.52.65 - 10.85.52.127 |
| 21 | 兰考 | 10.85.20.129 - 10.85.20.191 | 10.85.52.129 - 10.85.52.191 |
| 22 | 汝州 | 10.85.20.193 - 10.85.20.254 | 10.85.52.193 - 10.85.52.254 |
| 23 | 滑县 | 10.85.21.1 - 10.85.21.63 | 10.85.53.1 - 10.85.53.63 |
| 24 | 长垣 | 10.85.21.65 - 10.85.21.127 | 10.85.53.65 - 10.85.53.127 |
| 25 | 邓州 | 10.85.21.129 - 10.85.21.191 | 10.85.53.129 - 10.85.53.191 |
| 26 | 永城 | 10.85.21.193 - 10.85.21.254 | 10.85.53.193 - 10.85.53.254 |
| 27 | 固始 | 10.85.22.1 - 10.85.22.63 | 10.85.54.1 - 10.85.54.63 |
| 28 | 鹿邑 | 10.85.22.65 - 10.85.22.127 | 10.85.54.65 - 10.85.54.127 |
| 29 | 新蔡 | 10.85.22.129 - 10.85.22.191 | 10.85.54.129 - 10.85.54.191 |
| 30 | 预留 | 10.85.22.193 - 10.85.31.254 | 10.85.54.193 - 10.85.63.254 |

## Loopback地址分配

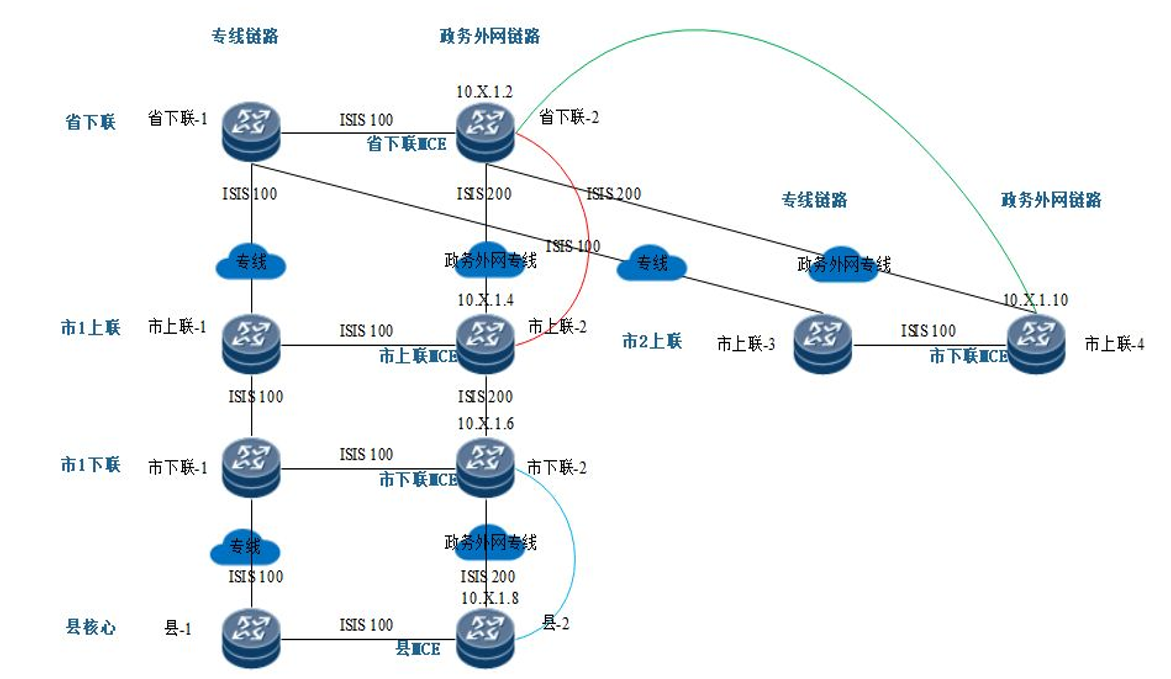
每个地级市分配1个C类地址用于设备loopback地址。由于郑州市规模较大，分配2个C类地址。省核心单独分配2个C类地址用于接入。每四个省直管市共用一个C类地址用于接入。考虑到未来5年的业务扩展，预留9个C类地址。

|  |  |  |
| --- | --- | --- |
| **序号** | **用途** | **loopback地址段** |
| 1 | 省端 | 10.85.64.1 - 10.85.65.254 |
| 2 | 郑州 | 10.85.66.1 - 10.85.67.254 |
| 3 | 开封 | 10.85.68.1 - 10.85.68.254 |
| 4 | 洛阳 | 10.85.69.1 - 10.85.69.254 |
| 5 | 平顶山 | 10.85.70.1 - 10.85.70.254 |
| 6 | 安阳 | 10.85.71.1 - 10.85.71.254 |
| 7 | 鹤壁 | 10.85.72.1 - 10.85.72.254 |
| 8 | 新乡 | 10.85.73.1 - 10.85.73.254 |
| 9 | 焦作 | 10.85.74.1 - 10.85.74.254 |
| 10 | 濮阳 | 10.85.75.1 - 10.85.75.254 |
| 11 | 许昌 | 10.85.76.1 - 10.85.76.254 |
| 12 | 漯河 | 10.85.77.1 - 10.85.77.254 |
| 13 | 三门峡 | 10.85.78.1 - 10.85.78.254 |
| 14 | 南阳 | 10.85.79.1 - 10.85.79.254 |
| 15 | 商丘 | 10.85.80.1 - 10.85.80.254 |
| 16 | 信阳 | 10.85.81.1 - 10.85.81.254 |
| 17 | 周口 | 10.85.82.1 - 10.85.82.254 |
| 18 | 驻马店 | 10.85.83.1 - 10.85.83.254 |
| 19 | 济源 | 10.85.84.1 - 10.85.84.63 |
| 20 | 巩义 | 10.85.84.65 - 10.85.84.127 |
| 21 | 兰考 | 10.85.84.129 - 10.85.84.191 |
| 22 | 汝州 | 10.85.84.193 - 10.85.84.254 |
| 23 | 滑县 | 10.85.85.1 - 10.85.85.63 |
| 24 | 长垣 | 10.85.85.65 - 10.85.85.127 |
| 25 | 邓州 | 10.85.85.129 - 10.85.85.191 |
| 26 | 永城 | 10.85.85.193 - 10.85.85.254 |
| 27 | 固始 | 10.85.86.1 - 10.85.86.63 |
| 28 | 鹿邑 | 10.85.86.65 - 10.85.86.127 |
| 29 | 新蔡 | 10.85.86.129 - 10.85.86.191 |
| 30 | 预留 | 10.85.86.1 - 10.85.95.254 |

# 路由配置方案

## GRE穿越政务外网实施方案

二级及以下纵向骨干网部署以其中一个省、两个市、一个县部署为例，整体配置过程如下（以华为路由器配置举例）。



配置思路如下：

IP地址规划（IP 地址为示例，实际 9-16 位以全国 IPV4 地址规划为准），接口IP地址规划同动态路由协议。

本例 GRE 隧道地址省下联与市 1 上联/市 2 上联地址 10.X.101.1/30 10.X.101.2/30、10.X.201.1/30 10.X.201.2/30；市下联到县核心地址 10.X.102.1/30；政务外网 LoopBack 接口地址省下联侧 10.X.1.2、市 1 上联侧 10.X.1.4、 市下联侧 10.X.1.6、县核心侧 10.X.1.8、市 2 上联侧 10.X.1.10。

路由协议规划：本例 IGP 使用 ISIS 协议，也可使用 OSPF 协议，政务外网设备与政务外网 PE 间使用 ISIS 协议。 各路由器部署 ISIS 进程 100，MCE 部署 ISIS 100，政务外网 PE 部署私网 ISIS 200，政务外网设备使能 ISIS 200（GRE 源和目的使用 Loopback 地址，Loopback 接口地址发布在 ISIS 200 内）政务外网 PE 上 ISIS 200 和 BGP 间通过策略控制做路由互引保证 Loopback 口路由可达，其余发布在 ISIS 100 中。

省核心 MCE 上通过 display isis 200 route 查看，包含各 核心 loopback 地址。

以省下联侧政务外网 MCE 路由器为例（关键配置）：

IPV4：

isis 100

is-level level-2

cost-style wide

network-entity 10.0000.0000.1000.0002.00

bfd all-interfaces enable

is-name Province-2

frr

loop-free-alternate level-1

loop-free-alternate level-2

isis 200

is-level level-2

cost-style wide

network-entity 10.0000.0000.2000.0002.00

bfd all-interfaces enable

is-name Province-2

frr

loop-free-alternate level-1

loop-free-alternate level-2

interface LoopBack0

ip address 10.X.1.2 255.255.255.255

binding tunnel gre

isis enable 200

interface Eth-Trunk0.1

vlan-type dot1q 1

ip address 10.X.168.14 255.255.255.252

isis enable 100

interface Tunnel101

ip address 10.X.101.1 255.255.255.252

tunnel-protocol gre

source 10.X.1.2

destination 10.X.1.4

isis enable 100

isis cost 20

interface Tunnel201

ip address 10.X.201.1 255.255.255.252

tunnel-protocol gre

source 10.X.1.2

destination 10.X.1.10

isis enable 100

isis cost 20

display isis 100 route // 查看 ISIS 路由表

display isis peer //查看 ISIS 邻居，与省上联、市上联政务外网设备 GRE、政务外 网 PE 间邻居状态为 Up

display bfd session //查看检测 ISIS BFD 状态为 UP

医保各核心设备到其他核心设备接入接口路由存在备份。

**GRE 隧道规划**

各省下联政务外网 MCE 设备与各市上联政务外网 MCE 设备、各市下联政务外网 MCE 设备 和各区县政务外网 MCE 设备间建立 GRE 隧道。

具体配置见第 2 点路由协议规划。

Interface Tunnel 101

display this interface //隧道状态为 UP

display isis peer //隧道间 ISIS 邻居状态为 UP

链路保护机制

a) 省下联和市上联间正常数据转发走专线链路，专线链路故障后，切换到 省下联 -1<==>省下联-2<==>GRE(省下联-2<=>市上联-2)<==> 市上联-1；省下联与市下联间类似。

b) 省下联和县核心间正常数据转发走专线链路，省下联与市上联间专线链路故障后， 切换到 省下联-1<==>省下联-2<==>GRE(省下联-2<=>市上联-2)<==> 市上联-1<==> 市下联 -1<==>县-1；省下联与市上联间专线、市下联与县核心间专线均故障后，切换到 省下联 -1<==>省下联-2<==>GRE(省下联-2<=>市上联-2) <==>市上联-2<==>市下联-2<==>GRE(市下 联-2=>县-2)<==> 县-1。

c) 市1上联与市2上联间正常数据转发走专线，省下联与市上联1间专线链路故障后， 切换到 GRE(省下联-2<=>市上联-2)转发，省下联与市 1 上联间、省下联与市 2 上联间专线 链路均故障后，切换到 GRE(省下联-2<=>市上联-2) GRE(省下联-2<=> 市上联-4)转发。