

开标一览表

供应商名称	中国移动通信集团河南有限公司濮阳分公司
项目名称	濮阳市行政审批和政务信息管理局濮阳市市直电子政务外网线路租赁服务项目第一标包
投标总报价 (人民币)	大写：肆拾叁万贰仟元整 小写：432000 元
投标有效期	自投标截止之日起 90 日历天
服务期限	合同签订后 15 日历天完成
质量要求	满足国家相关法律规定和现行行业标准与规范和招标文件要求
备注	我方完全响应招标文件要求，租赁期一年

供应商名称（盖单位公章）：中国移动通信集团河南有限公司濮阳分公司

法定代表人或授权委托人（签字）： 尹玲

2024 年 04 月 09 日



三、技术偏差表

序号	采购文件章节及条款号	响应文件章节及条款号	偏差说明
1	第二章 招标项目基本内容及要求， 2.1 总体要求	十二、技术方案及服务方案 12.1.1 总体要求	无偏离
2	第二章 招标项目基本内容及要求， 2.2 管理要求	十二、技术方案及服务方案 12.1.2 管理要求	无偏离
3	第二章 招标项目基本内容及要求， 2.3 保密要求	十二、技术方案及服务方案 12.2 保密要求	无偏离
4	第二章 招标项目基本内容及要求， 2.4 网络安全要求	十一、商务部分 11.3 网络安全 十二、技术方案及服务方案 12.1.9 网络安全要求	无偏离
5	第二章 招标项目基本内容及要求， 2.5 建设方案和编制依据	十二、技术方案及服务方案 12.1.7 政策依据、 12.1.8 技术标准	无偏离
6	第二章 招标项目基本内容及要求， 2.6 采购内容参数要求	十二、技术方案及服务方案 12.1.10 采购内容参数	无偏离
7	第二章 招标项目基本内容及要求， 2.7 建设工期及进度要求	十二、技术方案及服务方案 12.1.11 建设工期及进度	无偏离
8	第二章 招标项目基本内容及要求， 2.8 售后运维要求	十二、技术方案及服务方案 12.5 售后服务	无偏离

注：

1. 供应商需按文件第二章要求应答，列出所投服务的具体应答。偏差说明一栏中对偏差予以详细说明（“正偏离”“无偏离”或“负偏离”）。
2. 投标者可根据其投标内容进一步细化上述表格，并可增添其它表格或说明以便进一步明确投标内容。

供应商名称(盖单位章)：中国移动通信集团河南有限公司 阳分公司
法定代表人或其委托代理人(签字)： 
日期：2024 年 04 月 09 日





十二、技术方案及服务方案

12.1 实施方案

12.1.1 总体要求

我公司负责建设电子政务外网骨干线路并提供相应设备。负责满足省市电子外网对接规范，上联省级电子政务外网，横向兼容其他供应商骨干网络。负责提供电子政务外网核心标准机房，该机房由电子政务外网管理机构管理使用，我公司负责进行维护。提供电子政务外网线路多速率带宽服务供使用方选择。为市级核心节点提供千兆互联网带宽服务，线路支持 IPv6 协议，并提供不少一个 1C 的互联网 IP。

1. 网络互联互通

电子政务网平台建立后，纵向上实现上连国家、省、市电子政务外网平台，下连各乡镇电子政务外网平台，在横向上能够方便连接市委、市人大、市政府、市政协以及政府各组成部门、直属机构、办事机构、事业单位等。同时，网络具备高度的可靠性和稳定性，具备可伸缩、可管理、可扩展的能力，以应对业务数据的快速增长，满足网络平台平滑升级的要求。

2. 互联网接入

外网平台提供整个网络统一的安全的互联网接入。

3. IPV6 升级

我公司建设的电子政务外网支持国家关于电子政务外网 IPV6 升级的基本需求。

4. 政务云对接

我公司建设的电子政务外网能够实现互联互通，并对接本地现有政务云，并实现政务系统互联互通。

12.1.2 管理要求

采购人负责政务外网的统筹管理，并按照统一规划、统筹管理、平均分配的原则，分配政务外网 IP 地址。

我公司负责端到端的物理设备及链路的故障定位和排除、管理设备配置。未经采购方许可，

所有设备不能与其它网络并用，从物理到逻辑均为单一独立的局域网络。我公司明确一个负责人或团队对电子政务外网线路进行运行维护，因特殊原因需更换负责人或团队，及时告知电子政务外网管理员。我公司提供网络运维管理、安全监测服务，并交于采购方使用。

1. 传输质量要求。

我公司提供的线路满足以下条件：默认 PING 传输时延上限值为 10ms；PING 带 2000 字节包，上限值为 20ms；（省市设备间延时上限值为 100ms；市县设备间延时上限值为 50ms）

2. 故障处置。

我公司提供 7×24 小时呼叫服务专线：从用户报障开始计算人员，到场时间 ≤1 小时，故障恢复时限 ≤4 小时。除不可抗力及市政施工等原因以外，一年内发生不超过 5 次线路故障在 48 小时内未能及时修复。

3. 日常巡检。

我公司建立光纤巡查机制。派专人就提供的光纤运行质量状态进行巡查。每季度巡查不少于一次，并做好巡查登记记录和通知维修记录。

12.1.3 实施计划

12.1.3.1 实施计划原则

➢ 总体原则：提前计划；合理安排；及时调整。

在具体实施前作好各种计划。对于进度要有全面的考虑，需要对于各阶段的具体日期，变更风险等方面有清楚的认识，完成《进度计划表》、《进度变更表》、《风险控制表》。

为了保证交付期，实施过程中将根据客户条件的具备来安排整体施工。实现分步实施，单独初验、统一终验的原则执行，确保按时保质保量的完成网络开通。

环境特殊的节点在实施之前要确认具体的实施方案并确认详细具体步骤。

实施之前确认实施前期的准备工作状况，充分考虑实施过程中有可能存在的问题，及时与将要开始实施的分支节点取得充分的沟通，及时提出相应的要求。根据具体的情况及时调整进度计划。

➢ 实施调度计划

公司项目组负责监督和指导各小组的工作进程，负责各小组的调度和人员安排；

项目实施负责人要填写工程实施日志

实施采购组负责设备的订货、接收、设备托运等。

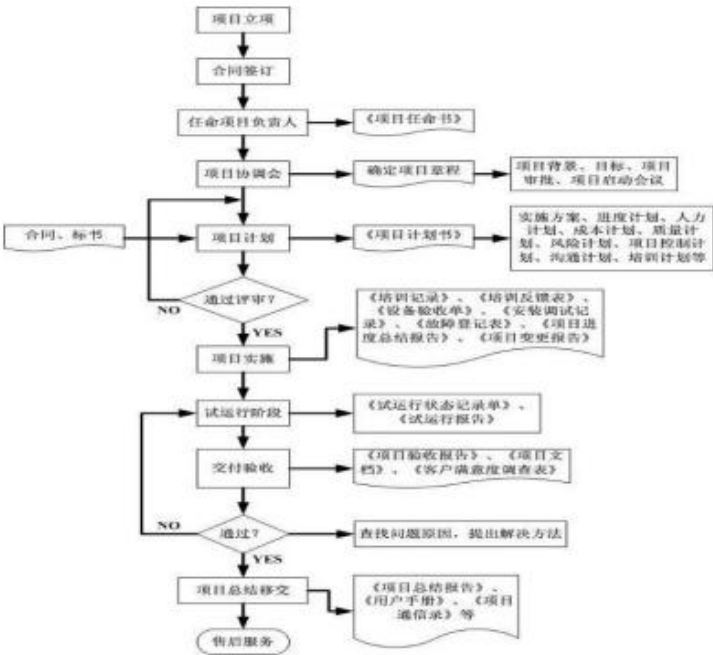
运维部负责接收并处理各分支节点实施完成以后的技术支持与培训。

项目进度按照《规定》的各项资料保证规定监督各小组实施工作情况；

各阶段确定计划

项目进度的合理安排是保证项目顺利交付的关键。根据濮阳市电子政务外网项目的复杂性和网络规模，我公司实施进度安排建议，整个项目过程包括以下阶段：项目准备阶段、设备到货验收阶段、线路施工、调试实施阶段及项目验收阶段。

具体内容包括：合同签订、设备购货、工程实施协调会、设备交付及验收、施工准备、工程施工、全网测试及试运行、集中培训、全网验收、竣工总结、工程验收后的系统维护等。



12.1.3.2实施内容计划

针对本次项目实施内容如下：

1. 对机房现场进行勘查，提供机房环境需求，协调用户按工程进度完成现场准备工作。
 2. 完成设备验收。
 3. 进行设备安装上架、上电验收、测试。
 4. 进行网元管理软件和硬件的安装、调试和投产。
 5. 按用户的技术进行现场单机调试工作。
 6. 协助用户进行初验。
 7. 安装地用户运维培训。
 8. 按照招标人要求制定详细网络设计方案和项目实施计划，完成本项目所有网络设备的调试工作。
 9. 按照详细测试、切换和迁移方案，完成本项目所有网络设备的测试、切换和迁移工作。
 10. 如涉及第三方网络产品、部分原有网络设备，编制相应的集成计划。
 11. 提交下列文档：
 - 网络设备订货清单
 - 机房现场勘察报告
 - 更新的项目计划
 - 网络设备开箱验收报告
 - 网络设备软件、固件版本文档
 - 网络设备网络端口连接表
 - 网络设备详细配置文档
 - 网络实施报告
 - 网络测试报告
 - 网络验收报告
- 明确双方接口人

在合同签订后项目实施前，本投标方将与用户领导和技术专家成立联合项目组，进行项目工程施工。

工前准备

本期项目内容主要在用户现有网络系统和设备的基础上，进行新购网络系统软、硬件安装、集成和调试，完成网络的改造。在完成货物运作、线路申请等工作后，进入各项目点的网络工程的具体实施阶段。由相关项目经理负责，进行前期准备，主要内容如下：

1. 掌握合同信息。合同中的设备类型数量、技术、软件版本，如果有新产品和新功能，是否有产品、软件版本等满足项目实施。
2. 了解货物、责任和到货信息。
3. 与用户沟通，了解工期和用户准备情况。
4. 若有扩容和设备改造部分，要了解原有设备情况。
5. 根据情况准备制作《实施技术方案》，组网图。《实施技术方案》要经过技术负责人的审核。

工前协调会

在开工前，项目经理及相关人员和用户相关部门一起召开开工协调会，其主要内容如下：

1. 与用户协商并确定《实施技术方案》，作为实施中的技术文件。
2. 与用户商定进度计划及配合事宜，按照进度用户完成安装环境准备。
3. 确认用户是否对硬件安装等工艺方面有特殊。签订《备忘录》，模板见附件。
4. 明确用户的总负责人和接口人。建议用户派一至两名技术水平较高的工程师随工，建议为机房维护人员。
5. 确定验收项目和验收方案，明确完工标志。

机房环境检测

在开始具体的工作之前，为保证设备能够安全工作，减少由于安装环境导致的网络通信问题，需要对机房状况进行检查。机房检测可以依照设备手册，参考标准机房的考察如下几个方面：

1. 电气参数：电压 220V—380V，频率 50HZ
 2. 静电接地：为保证及时泄掉各种设备产生的静电，防止因静电造成的损害，直流接地电阻要小于 1 欧姆，交流接地电阻小于 4 欧姆。
 3. UPS 输出：测试 UPS 输出是否满足设备需求。
 4. 机房温度：夏季保持在 22 ± 2 摄氏度，冬季保持在 20 ± 2 摄氏度
 5. 机房湿度：保持在 45%-65%
 6. 干扰：没有强电/磁干扰。
 7. 其他物质：无其他腐蚀性化学物质。
 8. 机房其他条件：地下网络综合布线是否合理可用、局域网以及广域网线路是否可用。
- 根据检查结果，填写附录：《安装环境检查表》。

责任和界面划分

依据国家通信行业惯例制订如下责任和界面划分，如果合同中有明确说明，按合同条款执行。如有疑问，客户与友好协商，在开工前以备忘录的形式确定。

设备材料责任划分：

客户准备：

1. 机房建筑、到机房的接地排、空调；
2. 传输设备、MDF/ODF/DDF 配线架及端子；
3. UPS 电源、直流和交流电源柜；
4. 电源线：电源柜到设备之间的电源线和接头；
5. 接地线：机房内接地排到设备之间的地线和接头；
6. 安装设备的机柜等。

设备厂家：

1. 按合同配置清单提供设备和相关配套物料；
2. 合同配置中含有机架时，配套发货安装底座（支撑支架组件 II，适用于 256~345mm 高的防静电地板）；
3. 按照合同规定的时间、地点到货。

集成商/代理商：是客户选择的集成商或者是本投标方的合作伙伴，根据客户与集成商的合同情况决定，一般情况下提供如下安装材料：

1. 信号线：配线架到设备间的连线和接头，如网线、尾纤、E1 电缆等。DDF 架端子（BNC、SMB 等接头）由 DDF 厂家提供。

安装责任和工程界面划分

机房接入侧：

1. 设备安装位置符合通风和空间等环境；
2. 完成电源柜和 UPS 的安装；
3. 电源线施工：完成电源柜到设备之间的电源线布放和连接；
4. 接地线施工：机房内接地排到设备之间的地线布放和连接；
5. 完成机房接地排安装和连线，接地电阻符合设备运行，一般小于 1 欧姆；
6. 确定设备的安装位置和相的柜子；
7. 提供必要的设备配置所需数据（如 IP 地址段）；

8. 设备调试配合；

9. 测试验收；

设备提供：

1. 对集成商、合作伙伴提供技术支持；

2. 成立项目支持组，由工程项目经理协调公司内部相关资源进行重大保障。

集成商/代理商：是客户选择的集成商或者是本投标方的合作伙伴，根据客户与集成商的合同情况决定，一般情况下完成如下内容：

1. 设备开箱验货；

2. 设备硬件安装；

3. 信号线施工：配线架到设备间的连线布放和连接，如网线、尾纤、E1 电缆等；

4. 数据配置、调试等，使设备能满足合同的技术指标正常运行；

5. 配合测试和验收；

6. 项目管理：协调人力资料，进度控制符合客户要求，项目质量符合项目要求，提供项目进展周报和实施文档。

7. 机房维护热线挂牌：在完工前在主要机房张贴机房维护热线标牌，标牌中有服务指南、合作伙伴的售后服务热线电话、厂家的售后服务热线电话等信息。

	本投标方责任	集成商	客户责任
设备提供、发货	√		
技术支持	√		
场地勘测		√	√
场地资料提供			√
机房准备			√
开箱验货		√	√
设备安装		√	
设备开通		√	
系统调试		√	
系统调试协助			√
初验测试			√

初验测试协助		√	
试运行			√
试运行协助		√	
终验测试			√
终验测试协助		√	

人员配置

为保证项目按时、保质完成，本投标方将为本项目配备了充足的人员，所派技术人员在用户技术代表的领导和管理下工作，按照组织人上级主管部门的技术标准，进行网络的设计、规划和项目督导（实施）等工作，并在实施过程中形成符合 ISO9000 和 ITIL 规范的技术档案文件。

12.1.3.3 上线部署计划

实施计划

1. 设备加电，刷配置脚本
2. 记录现网网络信息表
3. 骨干环网新增路由器
4. 新增路由器对接上下行站点
5. 新增特性业务
6. 测试业务是否正常
7. 业务运行若干小时即可认为业务割接上线成功

实施步骤

1. 设备升级版本，预加载配置脚本，查看设备状态信息
2. 查看现网设备运行状态和路由信息，记录网络信息表
3. 新增路由器对接政务外网、部署双向 NAT，测试业务，确保业务正常，查看现网设备运行状态和路由信息，符合预期之后，记录网络信息表
4. 业务运行若干小时即可认为业务割接上线成功

回退计划如下

骨干环网回退

1. 如果新增路由器上行至骨干环网业务或路由异常，立刻断开新增路由器与骨干环网路由器的连接，检查新增路由器配置，排查梳理完毕后再上联骨干环网，否则割接放弃，恢复骨干环网至正常。
2. 如果新增路由器下行业务或路由异常，立刻断开新增路由器下行的连线，排查新增路由器配置，排查梳理完毕后再上联骨干环网。

12.1.3.4 试运行方案计划

试运行方案与客户单位确认后，最终决定试运行方案，试运行操作可初步参考如下条件进行：

1. 设备安装调试完成并通过初步验收后，进入不超过6个月的连续试运行。如果由于本投标方或设备原厂商的原因使系统在6个月内达不到规范指标，则在修复之后由用户、本投标方及设备原厂商等共同确定再一次连续试运行开始日期。
2. 在试运行期间，本投标方或设备原厂商使任何故障或问题都能在收到故障通知后4小时内（节、假日也不例外）被修复和解决，并给出详细修复细节报告。
3. 所有试运行期间设备的修改和软件变化都在试运行结束后写入操作手册和维护手册中。

12.1.3.5 质量保障措施计划

项目组将制定科学、严谨的施工质量技术措施，严格执行公司的施工质量管理体系，推行PDCA循环质量控制方法，实现施工质量的“事前-事中-事后”控制。

（1）坚持“质量第一，客户至上”，把公司的质量方针和质量目标贯穿于整个工程的实施当中，把我们的服务态度和服务意识与网络的发展联系起来，促进我公司的质量保证体系不断完善。

（2）遵循PDCA中的计划、执行、查核、改善行动四个步骤的方法，对维护中的每个节点进行严格的监控。

（3）我公司项目组将严格执行公司安全质量部下发的“事前-事中-事后”三层循环质量保证措施，通过对每个环节的严格把控，提早发现施工过程中出现的各种质量问题，针对不同质量问题进行分析并提出解决方案，及时整改和纠正，做到“事前预防，事中避免，事后分析”，

保证整个项目质量

工程质量控制实施的三个阶段：
(1) 准备阶段：(2) 施工阶段：(3) 验收阶段：



项目涉及网络传输设备安装、调测等工作，工期短，任务急，涉及的工作细节繁多、设备材料众多、施工现场环境复杂多变等特点。只有把每一项工作细化分解，通过长期的实践才能形成规范化标准化的工作模式和工作效果，制定相关的工作流程，使每项工作形成制度化、流程化。对设备工程工作的管理需要贯彻到每一项工作细节，因此我公司针对本项目要求制定相关的制度规范，确保项目实施质量。

(1) 项目组在工程交底时要求全体施工人员牢固树立“质量第一”的观念，强化质量意识、服务意识，并实行公司满意度考评制度。

(2) 项目组在工程开工前召开技术交底会，加强员工上岗前的培训工作。对施工人员进行质量、安全、技术交底，认真审阅施工图设计和工程投标文件中我公司对公司的承诺，掌握工程全部内容，并及时填写“工程交底记录表”。

项目组技术负责人对施工队进行安全技术交底

(3) 现场施工人员不得擅自修改工程设计，对设计需变更的地方及时向项目组负责人反馈，由项目组负责人向建设单位提出修改建议，经建设方和设计部门同意后方可施工，并填写“工程变更单”。

(4) 项目组组建专门的质量管理小组，监督检查各施工队的工程质量，要求施工人员严格按照公司的标准施工。

(5) 工程队要认真组织落实施工检查工作，贯彻施工“三检”制度，各道工序严把质量关，出现问题，立即分析原因，及时返工、返修，确保工程质量。

(6) 各工程队要严格按施工图设计、会审纪要、工程验收指标及标准和规范进行施工，项目组将督促工程队具体实施及时下达工程各工序技术要求，各队应积极执行，并制定相应的施工技术交底，以便统一工艺和质量标准。

(7) 严格执行规范和设计要求的原则下，要虚心听取现场监理方的意见，在不违背设计原则的情况下，尽量协商解决好施工中的问题。

(8) 每周日向本公司工程管理部门上报“工程周报”表及工程施工情况，每周一向公司建设部门汇报工程进度及本周工作计划。

(9) 各工程队在工程施工中如发现技术问题，应及时上报项目组，项目组将随着工程的展开，协调建设单位、监理单位制定和发布相应的施工技术补充要求。

(10) 工程中涉及到高空作业和电工作业，必须是通过专业培训的持证人员进行操作。

(11) 对施工过程中的重要工序，施工现场负责人必须向作业人员进行现场交底，加强对重要工序的检验，确保重要工序的质量过关。

质量负责人进行关键工序现场培训

(12) 相关设备安装和布放各类线缆要严格按照技术规范和公司操作手册相关要求进行，一定要做好技术交底，与随工代表、监理现场沟通，确保运行设备和电路的安全运行，严格按照要求做好有关标识。

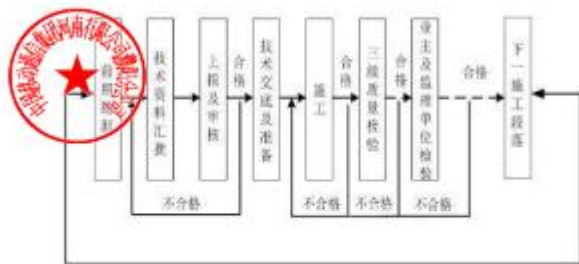
(13) 光缆测试和设备调测过程中，必须使用经过计量合格的仪表，按照本工程验收指标规定的项目和数量严格调测。

(14) 项目组组织人员在工程验收前要加强重要工序的检验，确保重要工序的质量过关。

(15) 按规定办理各种工序签证手续，做到及时、齐全和清楚，并妥善保管，以备编制工程竣工资料。

12.1.3.6 质量管理流程计划

质量是企业的生命线，完善、可靠的质量保证体系是项目顺利完成的根本保证。我公司一贯尊崇这种严谨的、科学的管理理念，为此公司专门成立了质量监督部和质检小组对每一个项目的实施过程和实施情况进行全程监控，并形成了一套完整的质量保障体系。严格和完善的质量管理是项目顺利优质完成的保障。



12.1.3.7 施工质量保证与改进措施

➤ 施工前

编制可行的组织设计。

设置合理的施工管理机构。

参与设计会审，对设计中不合理的地方及时提出。

工程开工前召开技术交底会，熟悉建设单位的质量规范和相关操作流程。

制定本项目的施工守则、质量考核评分细则和相应的激励制度。

对施工过程中容易出现的质量难点进行预测，并制定出相应的解决措施。

工程开工前，对全体参与施工人员进行技术培训和上岗考核，提高全员的素质，增强员工的质量意识。

确保车辆、仪表、仪器、工具处于良好的待命状态。

工程全面开工前，进行标准站点的安装，确定统一的安装标准。



采用专人负责制，施工队长负责施工现场的质量控制，公司项目管理人员不定期对施工现场进行检查。

线路施工现场作业前，施工队长督促施工人员明确工作目的、操作规范和质量目标。

施工队长确保现场每道工序都符合操作规范。

施工队长做好现场施工安装记录。

施工中如发现设计图纸与现场不符时，须立即停工同时与勘测设计工程师汇报，施工人员不得擅自更改设计。

➤施工后

对施工中出现的品质问题进行阶段总结并制定出相关的预防措施，向全员推广，杜绝再出现同种问题。

➤品质改进措施

当项目的结果未达到质量标准时，就要查明原因，消除产生品质缺陷的因素，实现品质的改进。

优化过程。工程品质第一次就做好会节省大量的时间和资源。因此我们的项目团队是不断努力改进和优化过程并减少返工时间作为基本原则。

持续改进。品质又是一个持续改进的过程，我们坚决抛弃“没有出现问题就不管”的观点，推行持续改进思想。

全员培训。我们从以前的对管理层和精英进行培训转化为对施工人员全员进行教育和培训。我公司项目组对当地区的网络情况已经相当了解，我们要利用这个优势，将线路网络施工实际情况与我们的品质保证体系更紧密地结合起来，并将本期工作量及以后网络的发展联系起来。

充分授权。我们本次派出的是经过充分授权的团队，能够根据客户的期望执行和改进项目，以使客户满意。

12.1.3.8 施工器具与材料品质保证措施

➤施工器具品质保证措施

进场前对施工中需要使用的工具、仪表进行检查和保养，保证运行良好，有检定合格的

“合格证”，能完全满足本项目的需求和工程进度的要求。

检查进场的安全帽、工作鞋等安全防护用品是否符合施工安全标准。

进场的所有车辆进行检修，确保车辆状态良好，杜绝“病”车上路。

保证车辆和日常工具的数量和质量，避免因车辆及工器具质量而影响质量。

➤施工材料质量保证措施

项目负责人在施工期间配合仓管部门对设备及安装材料配件等的库存定期进行清点，提前做好须添补的材料准备，保证施工质量。

施工时检查工具、材料是否放置安全，防止高空坠物，施工结束时，要带走所有的工具和剩余材料。

工程用材料必须符合相关质量标准（含甲供材料），材料管理员需对材料进行严格检验，确保材料合格。发现缺、坏件等质量问题，应及时退换，并向建设单位汇报。由我公司自购的材料，需与厂家协商好供货速度问题，确保供货速度达到施工需要。

在设备材料搬运前对设备进行外表检验，如发现外表损伤，应及时向建设单位提出，以便办理材料退货。

12.1.4项目实施人员

12.1.4.1实施人员配备

序号	姓名	联系电话	角色	备注
1	和鑫	13525606099	项目负责人	无
2	于士奇	19839386556	项目经理	无
3	钟建锋	13839291019	技术负责人	无
4	许光华	13939336527	技术员	无
5	李英杰	13781354080	技术员	无
6	柳亚鑫	19720379721	技术员	无

12.1.4 施工人员能力保证

随着市场经济的进一步发展,为了能在激烈的市场竞争中立于不败之地,在竞争中做到“人无我有,人有我强”,公司制定了“以管理取胜,以质量取胜,以技术取胜”的策略。

人是质量的创造者,质量控制必须“以人为核心”,把人作为控制的动力,调动人的积极性、创造性;增强人的责任感,树立“质量第一”观念;提高人的素质,避免人的失误;以人的工作质量保工序质量、促工程质量。

我公司除了对员工进行政治思想教育、劳动纪律教育、职业道德教育、专业技术培训,健全岗位责任制,改善劳动条件,公平合理地激励劳动热情以外,我们还根据工程特点,从确保质量出发,在人的技术水平、人的生理缺陷、人的心理行为、人的错误行为等方面来控制人的使用。如技术复杂、难度大、精度高的工序或操作,由技术熟练、经验丰富的施工人员来完成;对某些要求万无一失的工序和操作,我们深入地分析人的心理行为,控制人的思想活动,稳定人的情绪;对具有危险源的现场作业,控制人的错误行为,严禁吸烟、打赌、嬉戏、误判断、误动作等。

技术人员的素质永远是一个项目成败的关键性因素,为了保证项目实施的高质量,我公司实施持证上岗制度,严格禁止无技术资质的人员上岗操作。我们员工必须通过公司的技术考核,合格后才能获上岗证。我们反对“一劳永逸”,我公司实行不定期的考核以检验并保持施工人员的技能水平,保障技术人员能够了解和掌握移动通信最前沿、最先进的技术。

把好参与项目人员的质量关、数量关。人员上岗必须具有相应技术资质和条件,对于特殊工序必须具有相关资格证的人员进行操作,如登高作业、用电作业等。

做好实施人员上岗前技术培训及劳动、职业道德教育,保证实施人员明确其岗位技术要点和工程注意事项,组织对质量控制体系制度的学习。

对于参加实施人员的数量,将按照工程的规模进行合理的配备,确保工程有条不紊的进行,对于关键工序,指定关键点操作责任人。

提高人员素质,建立合理监控体系,明晰岗位职责,质量控制,人人有责。

在具体的质量控制中,我们采取层层监控,实时反馈的方式,及时做好工程质量的预防、控制工作。

12.1.5 部署方案

12.1.5.1 项目背景



为坚决贯彻落实党中央、国务院、国家电子政务外网管理中心决策部署，积极推动“一张网”重大项目工程，助力实现“互联网+政务服务”，促进“放管服”改革落地见效。大力推进信息化与经济社会各领域融合发展的广度和深度，打造濮阳市新一代电子政务外网体系，推动“数字政府”建设并以“数字政府”带动“数字濮阳”、“智慧濮阳”发展，进而把濮阳市打造成为“深度感知、移动互联、融合共享、云上善政”的电子政务创新标杆。

12.1.5.2 需求分析

12.1.5.2.1 现状分析

濮阳市电子政务外网建设按照“2+N”网络架构（1个互联网接入区、1个公用网络区和N个专用网络区），稳步推进纵向覆盖和横向接入。目前，濮阳市政务外网已覆盖市、县区、乡镇办所有政务部门和实体政务大厅，纵横网络体系贯通基本实现，全市三级政务部门基本实现网络贯通。

横向网：各政务单位通过租用运营商固定专线的方式将各自路由器与横向网核心连接，对于重要部门一般考虑本地与路由器双上联，完成各相关单位访问电子政务外网的横向流量。

纵向网：纵向网主要完成市、县（区）、乡镇各相关单位访问政务外网的纵向流量或者相关单位 VPN 流量，纵向网区域主要由纵向骨干路由器，构建冗余可靠的网络平台，负责整个网络的高速数据交换及转发；下行连接区县二级网广域网路由器，负责业务汇聚功能；县（区）层级配备广域网路由器，负责县乡层级的业务汇聚。

12.1.5.2.2 总体分析

➤链路带宽需求分析

本项目是一个全市承载网络的一体化服务，最主要的传输流量为纵向流量和互联网出入口流量。一些直连单位本应按照国家有关要求使用政务外网，却因政务外网整体承载能力还存在“短板”，无法满足业务部署需求等原因，未能依托政务外网建设，也反映出政务外网提升网

络承载能力的迫切需要。

网络架构统一需求

全市电子政务外网网络架构不统一，对于整个市电子政务外网来说，由于市数据中心无法第一时间感知所有事件，当应用出现故障时，会存在故障定位困难、排查时间过长的问题。另外，当发生安全事件时，溯源困难，无法做到精确定位，本次方案将对组网模式进行统一规划，以解决故障感知、故障处理时效的问题。

网络出口架构优化需求

现市直各单位均有自己的互联网出口，出口规范不统一。互联网出口安全防护有进一步提升空间。互联网访问区在木马程序、病毒程序、篡改软件等恶意代码的防范仍有不足，以及在防止用户访问互联网时误操作访问非法网站或反动网站的措施存在不足。服务器托管区的网站在网页防篡改方面仍然不能进行有效防御，并且还需完善区域的入侵防护服务功能，阻止来自互联网对托管服务器的入侵行为。因此，需要制定统一的互联网出口规范，统一市、县、乡、村四级的互联网出口。

IPv6 业务承载的需求

为贯彻落实党中央、国务院关于建设网络强国的战略部署，加快推进基于互联网协议第六版（IPv6）的下一代互联网规模部署（以下简称 IPv6 规模部署），促进互联网演进升级和健康创新发展，也满足国家电子政务外网管理中心分别《政务外网 IPv6 演进技术白皮书 2021》要求，电子政务外网建设需要实现政务外网 IPv4-IPv6、IPv6-IPv6 业务互访能力，具备网络从 IPv4 到 IPv4/IPv6 再到 IPv6 单栈的演进能力。

考虑到电子政务网现有服务基本已到期，并且不能很好的支持 IPv6 部署的需求，所以需要现电子政务网进行能力升级服务，保障电子政务网信息系统的全面可靠，充分保障网络系统的可靠性，保障政府部门内部各种应用的正常开展。只有稳定的政府信息系统，才能提供高效的政府部门内部办公的应用需要。电子政务网主要是提供政府内部的重要公文的传递，办公系统的开展，同时为公众、企业提供公开的信息服务。没有可靠的网络系统，不仅无法确保各种公文及办公系统的正常开展，极大的降低了政府部门内部的办公效率，同时，无法为公众、企业提供稳定的公开信息服务，严重的损害了政府部门的形象。

网络新技术支持的需求

为满足政务外网对新技术的支持，随着 IPv6 和 SDN 等新技术的不断发展，新技术不断地出现并被广泛使用。由于新技术通常具有优良的性能和新的功能，原有的网络能力无法满足这

些新技术的应用的功能和性能要求，导致网络必须升级。骨干网需全面支持 IPv6 协议，为政务部门 IP 地址应用提供网络支撑，同时部署 SDN 技术做全网的网络资源灵活调度管理。

1) 完善终端安全、网络安全、数据安全防护

当前我市安全基础设施难以全面覆盖终端安全、网络安全、数据安全三个维度，且防护手段较为单一，难以实现终端安全全面监控、网络安全多重防护和数据安全全流程防护。此外，从多重安全设备、系统获取到的日志和数据有助于提升我省各地市的安全威胁感知能力，同时有助于态势感知系统的安全事件发现能力。

2) 完善市直各部门协作与安全事件联动机制

由于我市政务外网具有覆盖范围大、涉及部门广的特点，一旦安全事件涉及到跨地市、跨部门，安全事件的协同调查、响应就会趋于繁琐，处置不及还可能使事件影响扩大，造成更大损失。所以在不断完善安全基础设施覆盖、提升态势感知能力的同时，还应建立安全事件联动响应机制。

➤运维服务需求

完善科学合理的平台运维管理体系，包括运维体系、队伍管理、运维管理、运维制度，运维工具等，保障平台正常运行。

1) 运维服务需求

运维体系主要包括组织机构、管理机制和管理措施，标准规范主要包括电子政务外网运维管理体系规范。运营维护体系，系统服务的同时，通过培训、制定信息系统规章制度等手段，按照 IT 服务管理理论、方法和标准，结合实际需要及 IT 运维服务体系服务要求，借鉴和参考成功经验和实践，逐步建立一套融合组织、制度、流程、人员、技术的 IT 服务管理体系，健全组织机构，明确职责分工，制定规章制度，规范管理流程，强化技术支撑，实现对网络及信息系统的综合管理监控和日常技术支持，快速响应和及时解决信息系统运行过程中出现的各种问题和故障，确保网络及信息系统安全、稳定、高效运行，最终达到符合 IT 运维服务体系标准要求。同时通过完善与加强应用系统研发规章制度和流程，全面提升信息化工作管理水平。

2) 运维工具需求

运维工具是运维组织保障高质量、高效率交付运维服务的关键技术手段。运维工具的需求目标是实现政务外网运维监控自动化、服务流程规范化，从而全面提升政务外网的运维服务水平，并提高各级运维单位的协同运维能力。

12.1.5.2.3 总体需求

1. 网络互联互通的需求

电子政务外网平台建设需在纵向上实现上述国家、省、市电子政务外网平台，下连各乡镇电子政务外网平台。在横向上能够满足连接市委、市人大、市政府、市政协以及政府各组成部门、直属机构、办事机构、事业单位等。同时，网络必须具备高度的可靠性和稳定性，应具备可伸缩、可管理、可扩展的能力，以应对业务数据的快速增长，满足网络平台平滑升级的要求。

2. 互联网接入的需求

外网平台应能够提供整个网络统一的安全的互联网接入。

3. IPV6 升级

电子政务外网需支持国家关于电子政务外网 IPV6 升级的基本需求。

4. 政务云对接需求

电子政务外网须实现互联互通，并对接本地现有政务云，并实现政务系统互联互通。

12.1.5.2.4 管理需求

政务外网需统筹管理，并按照统一规划、统筹管理、平均分配的原则，分配政务外网 IP 地址。

应做好端到端的物理设备及链路的故障定位和排除、管理设备配置。未经许可，所有设备不可与其它网络并用，从物理到逻辑均为单一独立的局域网络。加强对电子政务外网线路运行维护。

12.1.5.2.5 保密需求

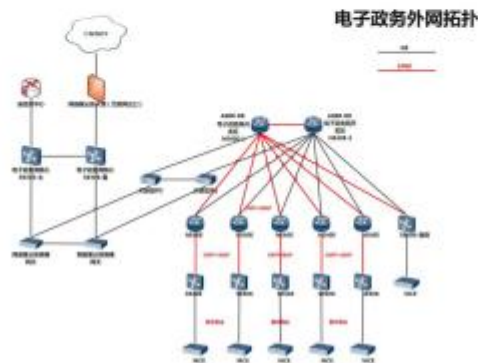
提供线路或相关工作人员应遵守保密原则，保证政务信息不因线路问题外泄。

12.1.5.2.6 网络安全需求

加强终端安全、网络安全、数据安全防护，建立各级部门协作与安全事件联动机制。

12.1.1 系统架构

12.1.2 技术架构



总体采用业务与网络分层构建、逐层保护的指导原则，在逻辑层次及业务的划分上，淮阳市电子政务外网核心架构为“一纵两横”结构，其中“一纵”为市、县、乡镇、村（社区）纵向广域网，“两横”为市、县（区）横向政务外网城域网。

12.1.5.3.2 整体目标

本次政务外网升级改造利用淮阳市公用基础通信设施，提供结构合理、边界清晰、技术先进、安全可靠的市电子政务外网网络平台，在组网架构方面充分利用运营商的大容量光纤链路升级改造政务外网网络，具备较高水平的安全监测、运维管理和服务保障能力。

➤扩大我市电子政务外网的网络覆盖范围，连通各市直单位政务外网。

➤提高我市电子政务外网的带宽和应用承载能力，真正实现“一张网”提供带宽保障。业务部门采用双线接入；通过构建 SDN 智能网络，搭建切片网络，实现市各级网络资源灵活分配、按需组网；推进政务外网、互联网和政务专网融合，整合互联网统一出口，通过 VPN 技术实现

与互联网的联接，打造云网融合一体化平台；适应 IPv6 发展趋势，满足中央 IPv6 部署要求，具备 IPv6 承载能力，构建支持 “IPv6+” 的先进网络；政务外网除可满足所有视频会议及应用系统外网传输需求，也可全面支持物联网、AI、大数据、区块链等新技术的应用创新。

►增强网络可靠性和安全性。建立与市级外网统一的安全保障体系，加强安全保障措施，建立政务外网安全管理和应急响应工作机制。

提升运维能力和服务能力。建立健全全市政务外网服务体系，市级核心区提供政务外网运维监管平台，进一步完善覆盖全市的网络监管机制，通过第三方网络监管服务，实时监管网络运行状态。

►推进全市电子政务规范化体系化建设。根据国家电子政务外网网络技术指南等相关要求，并结合我市实际情况，协助客户制定电子政务外网管理制度，编制我市电子政务外网技术规范、运行管理规范和安全管理规范等地方性标准规范文件。

►满足省市电子外网对接规范。上联省级电子政务外网，横向兼容其他供应商骨干网络。负责提供电子政务外网核心标准机房，该机房由电子政务外网管理机构管理使用，我公司负责进行维护。我公司提供电子政务外网线路多速率带宽服务供使用方选择。为市级核心节点提供千兆互联网带宽服务，线路支持 IPv6 协议，并提供不少一个 1C 的互联网 IP。

►实现网络互联互通。电子政务网平台建立后，在纵向上实现上述国家、省、市电子政务外网平台，下连各乡镇电子政务外网平台，在横向上能够方便连接市委、市人大、市政府、市政协以及政府各组成部门、直属机构、办事机构、事业单位等。同时，网络具备高度的可靠性和稳定性，具备可伸缩、可管理、可扩展的能力，以应对业务数据的快速增长，满足网络平台平滑升级的要求。

►实现互联网接入。外网平台能够提供整个网络统一的安全的互联网接入。

►IPv6 升级。建设的电子政务外网支持国家关于电子政务外网 IPv6 升级。

►实现政务云对接。建设的电子政务外网实现互联互通，并对接本地现有政务云，并实现政务系统互联互通。

12.1.5.4 IPv6改造

12.1.5.1 IPv6改造方案

IPv6 规模部署和应用是网络演进升级的必然趋势，是网络技术创新的重要方向，是网络强国建设的关键支撑。政务外网将以 IPv6 为基础，在基础设施集约化建设、业务高品质承载、安全精准管控方面深耕优化，提升政务治理的现代化水平。

政务外网基于 IPv6，构建集约高效的政务基础设施。通过为全网业务系统的服务器、终端等分配唯一的 IPv6 地址，实现政务非涉密业务通过统一的政务云、政务外网来承载，促进新业务的快速发展，实现政务资源的集约化。在每个服务器和终端具有唯一的 IPv6 地址后，对于数据大集中系统，以及跨层级、跨部门的视频会议等系统，可以实现扁平化的架构，不同层级的服务器和终端等可以直接通信，有效提升政务业务的处理效率。

政务外网通过 IPv6，实现高品质的政务体验。IPv6 技术体系是基于 IPv6、AI 的协议技术创新，在广联结、超宽、安全、自动化、确定性和低时延 6 个维度全面提升 IP 网络能力，可以为政务业务的差异化质量保障、自动化、智能化保驾护航。通过基于 IPv6+ 技术体系的网络切片技术，在一张物理网络上实现资源隔离的专网服务，可以为视频会议等重保业务提供独立的带宽资源，在其他业务出现拥塞时，不影响重保业务的质量，实现高品质的体验。结合 SRv6 VTN ID (Virtual Transport NetworkID, 切片 ID) 技术，多个网络切片平面可以共用一套接口 IP 地址和 IGP (Interior Gateway Protocol, 内部网关协议) 路由协议，降低网络协议的复杂性。基于 SRv6 Policy 技术和 SDN 架构，可实时采集整网链路的时延、丢包等质量信息，根据不同业务的要求，选择最佳的网络路径进行承载，并自动进行优化。通过 iFIT 随流检测技术，可以实时检测业务的质量，可视化呈现；在业务出现异常时，自动在业务路径上逐跳收集业务质量信息，定界故障位置，恢复业务，保障政务业务的连续性。同时结合 APN6 技术，可将视频会议等终端与网络深度协同，实现应用端到端可视和运维。

政务外网依托 IPv6 安全优势，提供精准的安全管控和溯源。全网终端具有唯一的 IPv6 地址，通过安全监测分析平台，实时检测网络威胁，当发现威胁后，可以通过 IPv6 地址精准溯源到终端位置，对异常终端进行阻断。使用 IPv6 地址后，部门政务终端接入政务外网时不需要进行 NAT 转换，不需要考虑 NAT 穿越的问题，可以通过免客户端的 Portal 认证方式进行准入认证，增加了认证的灵活性和便捷性。还可以利用 IPv6 地址丰富的扩展字段，可以携带

用户 ID 等信息。网络和安全设备通过用户 ID 等信息，对用户进行精准的认证和威胁防护。

IPv6 网络演进原则

政务外网采用统一规划、分级负责的模式，IPv6 演进是一个长期、分地域、分系统逐步升级的过程。演进过程遵循应用驱动、规划先行、分级分域、保障安全的原则统筹推进。各层级单位需要密切配合，充分利用沟通协调工作机制加强对接，合力破解具体困难和问题。

政务外网 IPv6 改造以部门业务需求为切入点和突破口，驱动网络演进，应用、网络互相促进，形成 IPv6 改造正循环。推进 IPv6 特色应用创新示范，尤其是对 IP 地址需求量大的应用，对存量应用实施分批分步的 IPv6 改造，改造一个，应用一个，最终实现 IPv6 规模部署。

演进过程中必须保障业务的可持续性 & 网络安全性，实现“业务不断，安全不乱”。在进行 IPv6 替换或者演进时，兼顾国产化战略，优选国产化产品或系统。尽快完善 IPv6 相关的等保测评体系，维护业务系统的安全运行。

政务外网 IPv6 演进需要政务云、网络平台、部门政务外网三方面协同发展，优先进行政务云互联网接入区改造，满足政策要求，应用逐步迁移到 IPv6；公用业务区按照“网络先行、应用逐步改造”策略，优先进行基础设施改造，打通政务外网 IPv6 访问通路，为 IPv6 应用上线奠定基础。

IPv6 演进原则

IPv6 演进迁移涉及到承载网络、业务系统、终端用户、支撑系统等各方面，适应电子政务外网实际情况，政务网络中 IPv6 演进遵循以下原则：

1) 优先改造政务云互联网区，满足国家门户网站 IPv6 改造要求

目前，政务云互联网区已经为公众提供 IPv6 访问服务，方案以 NAT 翻译技术为主，业务系统大多数仍然采用 IPv4 地址。互联网区的电子政务网、数据库、应用监测系统、身份认证管理系统、网络设备、安全设备等基础设施改造支持 IPv4、IPv6 双栈，具备双栈业务承载能力，过渡期内不支持 IPv6 的应用，通过 NAT64 (Network Address Translation IPv6-to-IPv4, IPv6 到 IPv4 的地址转换协议) 的方式支持 IPv6 用户访问。升级互联网区 DNS (Domain Name Server, 域名服务器) 系统，具备 IPv4/IPv6 域名递归解析能力。

应用系统需要支持 IPv4 和 IPv6 用户同时访问。对于网页中的外链 (网页包含其它网站内容的链接)，需要通过代理等方式解决，避免出现“天窗”问题 (用户访问网站时出现响应缓慢，部分内容无法显示，部分功能无法使用等情况)。随着 IPv6 改造的逐步深入，“天窗”问题会逐渐消失。

互联网出口与运营商对接，对外的 IPv6 业务地址建议采用运营商地址，政务外网地址和运营商地址分离，避免相互影响。

2) 电子政务外网 IPv6 改造，先试点，再推广，循序渐进

电子政务外网广域网/城域网 IPv6 改造建议采用 IPv6+ 方案，基于 SRv6 技术承载 IPv4、IPv6 业务，提升网络可编程能力，同步提升业务体验，全面实现网络和业务的可视、可管、可控、可维，满足持续演进要求。广域网/城域网 IPv6 改造整体按照“先评估，再规划”，“先试点，再推广”，“先核心，再边缘”，“先业务面，再管控面”的改造思路，循序渐进，平滑演进。

由于电子政务外网省、市采用分级建设的模式，改造计划、进度存在差异，建议改造时网络兼容 IPv4 和 IPv6 两种协议，对于未完成 IPv6 改造的网络，使用 IPv4 协议进行对接，保障现有 IPv4 业务不受影响。

电子政务外网广域网、城域网改造过程中，可采取循序渐进的原则，市级网络和各地市网络分步骤演进，推荐优先改造市级网络，市级网络采用新建方式支持 IPv4 和 IPv6 业务，全面向 IPv6+ 演进。地市网络可根据情况分步骤实施 IPv6+ 演进，市级网络与地市网络对接时，根据地市网络情况选择不同技术，如果地市网络采用 IP 方式承载，地市与市级可采用 CE、PE 方式进行对接，如果地市网络采用 MPLS 承载，地市与市级可采用路由重生成方式对接。地市网络不感知市级网络变化，无需做任何适配，市级网络兼容地市网络业务，已达到平滑演进。

存量设备改造时，改造前需要评估确认设备的升级、替换策略，关注开启双栈后性能变化，双栈功能可能会降低某些设备的可用资源，如路由表项，上线用户数等。

城域网的边界安全和准入认证系统，需要同时支持 IPv4 和 IPv6 用户和业务。网络管理运维系统，仅涉及内部管理，不涉及业务，可优先改造完业务面后，再进行改造。

3) 部门政务外网，按需改造，逐步演进

部门政务外网的网络和终端根据各部门需要进行改造。改造时，网络设备、安全设备、终端部署双栈。部门政务外网与城域网对接时，不需要 NAT 转换。终端访问政务外网时，采用终端准入控制机制，不允许终端同时访问互联网和政务外网，避免跳板攻击。

4) 政务外网区支撑系统改造（如 DNS、域名服务器），按需改造，试点先行

政务外网区应用不再采用 NAT64、DNS64 的过渡演进方式，直接向应用支持 IPv6 演进。首先在政务外网区改造支撑系统，例如 DNS 域名服务器，具备 IPv4/IPv6 域名递归解析能力，DHCP Server 动态地址分配服务器，具备 IPv4 和 IPv6 地址自动分配能力，其他如电子政务网、数

数据库、应用检测系统、身份认证系统、安全设备等基础设施支持 IPv6，以满足政务外网 IPv6 应用的部署。

5) 政务外网业务改造，按需进行，试点先行

新建的应用系统，要做好系统平台的架构规划，充分考虑系统对 IPv6 的支持，建议部署双栈，同时支持 IPv4 和 IPv6 用户的访问。面向未来，待终端 IPv6 普及后，双栈并行向 IPv6 单栈演进。

存量应用系统根据业务需要逐步进行改造。因存量系统一般重要性高，数据量大，可先选取部分应用系统进行改造，试点先行，并保证 IPv4 和 IPv6 双栈能力。

政务外网 IPv6 演进方案

目前政务外网主要以 IPv4、MPLS VPN 网络承载为主。从当前网络演进到 IPv6+网络，如下图所示主要是政务外网(广域网、城域网)的改造，无需改造政务云、委办园区内的服务器、应用系统、终端。

IPv6 演进上下文关系



根据现网的不同情况，政务外网的 SRv6 网络演进主要有三个场景：

替换：现网设备已到生命周期，全网替换支持 SRv6 能力的设备。

新建：现网设备未到生命周期，且不能通过升级具备 SRv6 能力，新建具备 SRv6 能力的网络平面。

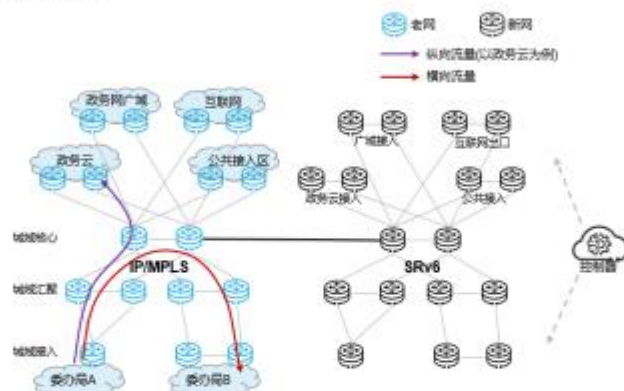
下面针对不同场景的 SRv6 演进给出规划建议。

场景一：平滑切换场景

替换完全新建 SRv6 网络，通过 SDN 网络控制系统对新建网络全网纳管，在割接过程中新老两网通过静态路由方式打通，逐步将业务切到新网络后，老网下线。详细过程（以城域网替换为例，广域网类似）如下：

一、割接准备

割接准备阶段示意图



完成新设备到位调试、网络搭建，并且内部连通性测试正常；

完成新网的各个业务 VPN 的部署，确保每个节点所有 VPN 业务的连通性正常；

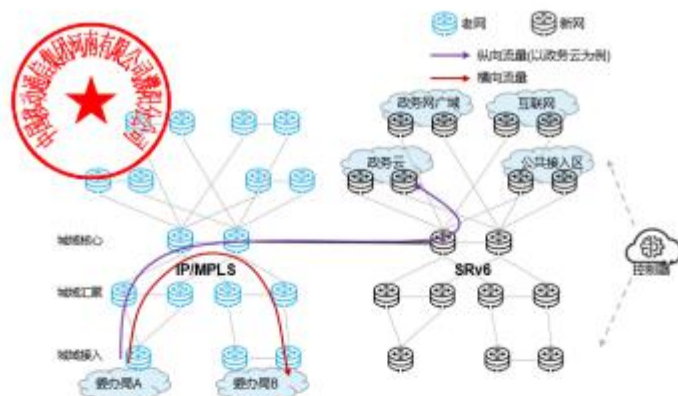
新网与老网的路由器的互联光纤部署完毕并完成连通性测试；新老网络核心互为 PE（老网非 MPLS VPN 时，新网做 PE，老网为 MCE），路由打通，确保所有业务路由成功传播至新网；

完成新老网络打通后的业务测试，确保新网具备各个业务 VPN 的承载能力。

以上步骤完成后网络纵向、横向业务流如上图所示。

二、业务系统割接

业务系统割接阶段示意图



完成业务梳理，将出口 PE 割接至新网，进行迁移割接后的业务测试，确保业务连通性正常；

完成互联网出口的业务梳理，将互联网出口 PE 割接至新网，进行迁移割接后的业务测试，确保业务连通性正常；

完成政务外网广域出口的业务梳理，将广域出口 PE 割接至新网，进行迁移割接后的业务测试，确保业务连通性正常；

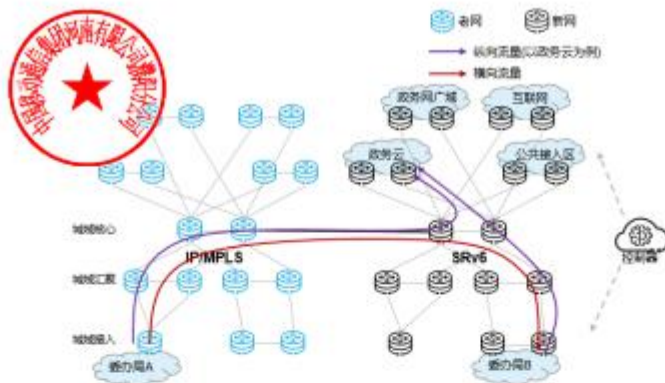
完成公共接入区的业务梳理，将公共接入区 PE 割接至新网，进行迁移割接后的业务测试，确保业务连通性正常；

完成其他网络业务区的业务梳理，将相应的 PE 割接至新网，进行迁移割接后的业务测试，确保业务连通性正常；

以上步骤完成后网络纵向、横向业务流如上图所示。

三、逐步完成政务单位割接

委办局逐步割接阶段示意图

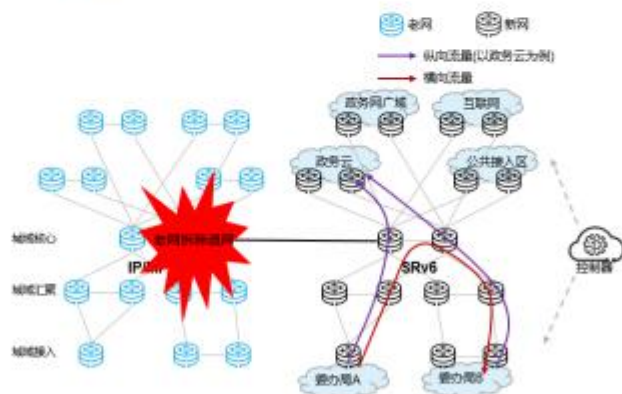


完成政务单位侧的业务梳理，将各单位业务逐步割接至新网，进行迁移割接后的业务测试，确保业务连通性正常。

以上步骤完成后网络纵向、横向业务流如上图所示。

四、替换完成，拆除老网

完成业务割接示意图



完成全网业务迁移割接，待网络运行稳定后老网逐步拆除退网。

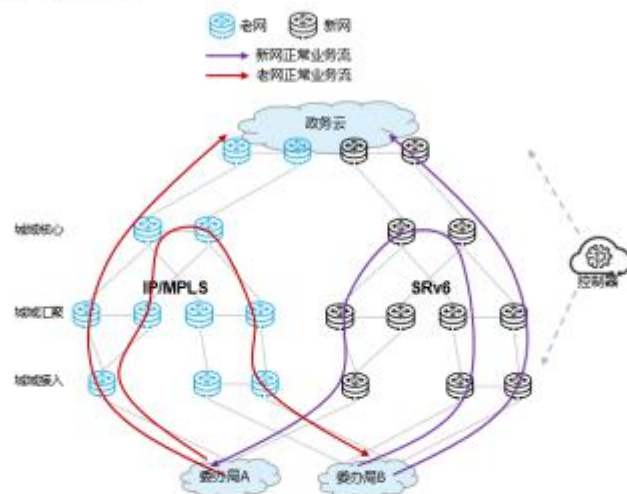
以上步骤完成后网络纵向、横向业务流如上图所示。

场景二：新建场景：

新建 SRv6 网络与原有政务外网形成双平面，一般此场景下新建平面会侧重承载特定业务，如新建视频业务平面，下网与老网互相备份，提升网络可靠性。详细过程(以城域网为例，广域网类似)如图 1-10 所示。

一、新建网络承载特定业务

双平面场景业务示意图



完成新设备到位调试、网络搭建，并且内部连通性测试正常，新、老网络两个平面横向不互联：

完成新网的各个业务 VPN 的部署，确保每个节点所有 VPN 业务的连通性正常：

政务单位新增链路接入新网络，此时新老网络均可访问业务系统，通过路由优先级控制选择网络平面，如视频业务承载在新网，数据业务承载在老网。

二、双平面互为备份，提升网络可靠性

双平面互备可靠性示意图



新网单点故障，通过 TI-LFA 等局部保护技术优先在自己网络平面内进行保护切换；

双平面任一网络出现多点故障，导致纵向网络不可达，政务单位接入侧路由收敛切换到另一个网络平面。

场景三：裸 IP 及大二层网络分步骤演进场景

部分政务外网运维管理单位运维能力薄弱，网络架构简单，现网老旧设备仍采用传统 OSPF 公网方式承载外网业务，甚至县城内采用二层组网，网关在汇聚或核心设备上。该场景下无法满足专网整合多业务承载、虚拟网络隔离要求，需要推动客户进行升级改造，建议采用场景二替换方式，先搭建新网，然后将业务逐步由老网割接到新网上。

步骤一：核心服务能力改造，核心网络具备 IPv6+能力

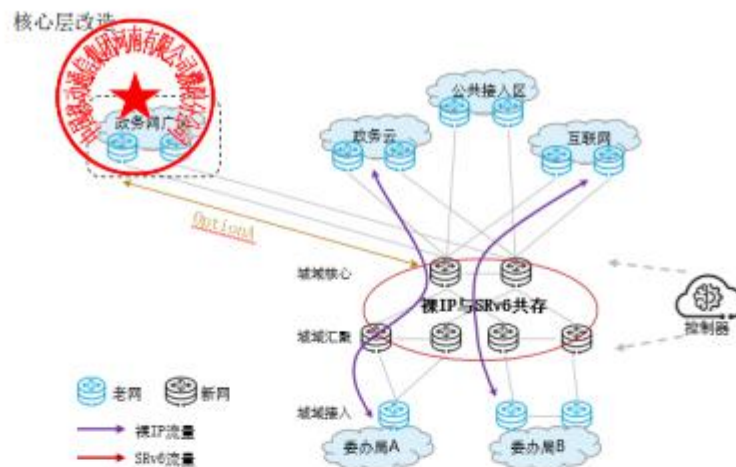
将核心层和汇聚层服务能力进行升级/替换，改造后设备移植原有传统 OSPF 或二层配置，保障原有网络业务不中断；

在核心、汇聚层部署 ISISv6 协议，用于通告 SRv6 Locator 以及 underlay 网络的 IPv6 路由，核心、汇聚设备支持 SRv6，但范围仅局限在核心和汇聚层；

核心设备兼做 RR，作为改造后业务的 MP-BGP 路由反射器，规划的 PE 设备与 RR 建立 MP-BGP IPv6 Peer，互相通告 EVPN 路由；

部署 SDN 网络控制系统对核心、汇聚设备进行统一纳管；

接入层仍然使用原有网络服务能力，网络承载方案保持不变。



步骤二：分区域改造，试点先行，部分业务通过 IPv6+承载

根据试点先行、按需改造原则，挑选部分委办局和政务云进行设备的升级/替换；

升级/替换后的接入层部署 ISISv6 协议，通告 SRv6 Locator 以及 underlay 网络的 IPv6 路由。作为 PE 角色的设备，与 RR 建立 MP-BGP IPv6 邻居关系；

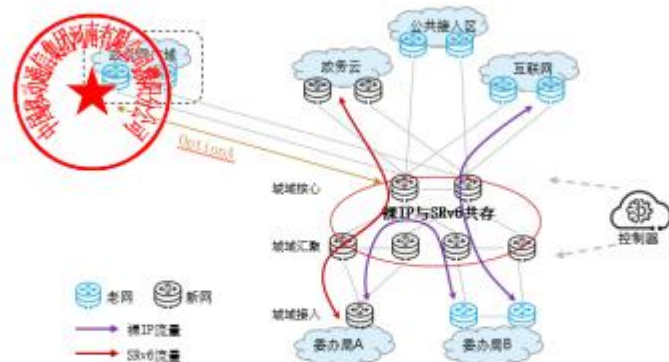
将升级/替换后的接入层纳入 SDN 网络控制系统管理范围，在该部分网络内可以实现业务快速发放、路径编排和流量调优；

升级/替换后的接入层和核心、汇聚层共同组成了 IPv6+网络区域，业务通过 SRv6 隧道承载；

升级/替换后的接入层仍然具备传统的 OSPF 以及二层 VLAN 能力，用于与存量网络之间的互联互通；

未升级/替换部分，以及与其之间的业务互通，仍然通过原有方式进行承载；

分区域按需改造

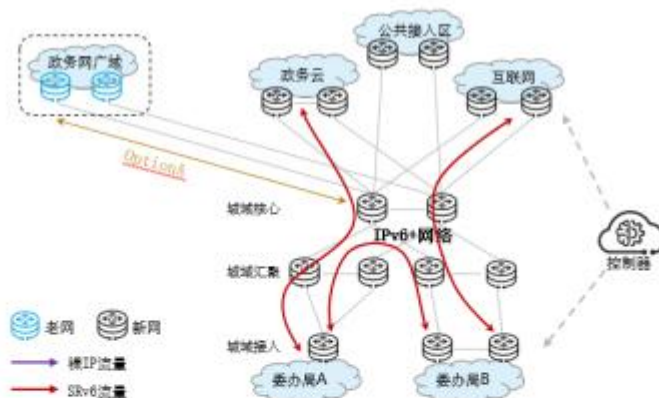


步骤三：按需推进，直至全网 IPv6+

逐步推进接入层升级/替换，已经完成改造后加入 IPv6+区域，未改造的仍然保持原有承载方式。最终实现全网改造完成，全网业务承载在 SRv6 隧道上。

待业务稳定后，删除原有裸 IP、vlan 配置，全网演进成 IPv6 单栈的先进网络。

全网完成 IPv6+改造



12.1.5.4.2 IPv6 地址规划与路由规划

IPv6 地址规划

IP 地址规划主要涉及到网络资源的利用的方便有效的管理网络的问题，IPv6 地址有 128 位，其中可分配为网络前缀的空间有 64bit。按照最新的 IPv6 RFC3513，IPv6 地址分为全球可路由前缀和接口 ID 部分，协议并没有明确的规定全球可路由前缀和子网 ID 各自占的 bit 数，目前 APNIC 能够申请到的 IPv6 地址空间为 /32 的地址。

IPv6 的地址使用方式有两类，一类是普通网络申请使用的 IP 地址，这类地址完全遵从前缀+接口标识符的 IP 地址表示方法；另外一类就是取消接口标识符的方法，只使用前缀来表示 IP 地址。

IP 地址的分配和网络组织、路由策略以及网络管理等都有密切的关系，IPv6 地址规划目前尚没有主流的规则，具体的 IP 地址分配通常在工程实施时统一规划实施，可以遵循一些分配原则：

地址资源应全网统一分配

地址划分应有层次性，便于网络互联，简化路由表

地址规划采用扁平化的规划思路，全网拓扑分为两个层次：骨干网和城域网。各个骨干网络或者特殊区域网络按照业务量需求，在骨干区域分配不同的地址段；对于城域网，考虑 IETF 对 IPv6 地址空间的 /48 的分配建议，结合大城域网的地址空间需求，划分为两级：城域区域和站点区域，其中城域区域划分为骨干区域到 /48 地址之间的地址空间，而站点区域，按照 IETF 的建议，使用 /48 到 /64 之间的地址空间。

IP 地址分配要尽量给每个区域分配连续的 IP 地址空间；在每个城域网中，相同的业务和功能尽量分配连续的 IP 地址空间，有利于路由聚合以及安全控制。

IP 地址的规划与划分应该考虑到网络的发展要求

地址使用兼顾到近期的需求与远期的发展以及网络的扩展，预留相应的地址段。IP 地址的分配需要有足够的灵活性，应考虑到现有业务、新型业务以及各种特殊的业务要求、满足各种用户接入（如，小区用户、专线用户，等）的需要。

充分合理利用已申请的地址空间，提高地址的利用效率。

IP 地址规划应该是网络整体规划的一部分，即 IP 地址规划要和网络层次规划、路由协议规划、流量规划等结合起来考虑。IP 地址的规划应尽可能和网络层次相对应，应该是自顶向下的一种规划。

CERNET2 分配给各个网络用户的 IPv6 地址空间会是一个或几个 /48 的 IPv6 地址前缀。

我们知道全球可聚集 IPv6 地址的前缀为 64 位，后 64 位为主机的 interface id。所以各

个网络用户用于分配的 IPv6 地址前缀空间的范围为/48 至/64 之间。

IPv6 地址分配规则同 IPv4 一样遵循 CIDR 原则。

IPv6 地址规划时主要分为三大类地址：

- 1、公共服务器地址，如 DNS，EMAIL，FTP 等。
- 2、网络设备互联地址和网络设备的 LOOPBACK 地址。

根据 IETF IPv6 工作组的建议 IPv6 网络设备互联地址采用/64 的地址块。IPv6 网络设备的 LOOPBACK 地址采用/128 的地址。

- 3、用户终端的业务地址。

此外由于目前网络设备的 IPv6 MIB 信息的获取和 OSPFv3 中 ROUTER ID 等均要求即使是一个纯 IPv6 网络也必须要求每个网络设备拥有 IPv4 地址。

所以一个纯 IPv6 网络也必须规划 IPv4 地址（仅需要网络设备互联地址和网络设备的 LOOPBACK 地址）。

IPv6 路由规划

路由协议分为域内路由协议和域间路由协议，目前主要的路由协议都增加了对 IPv6 的支持功能。从路由协议的应用范围来看，OSPFv3、RIPng 和 IS-ISv6 适用于自治域内部路由，为内部网关协议；BGP4+用来在自治域之间交换网络可达信息，是外部网关协议。

域内路由协议选择

支持 IPv6 的内部网关协议有：RIPng、OSPFv3、IS-ISv6 协议。从路由协议标准化进程看，RIPng、OSPFv3 和 IS-ISv6 协议已较为成熟。从协议的应用范围的角度，RIPng 协议适用于小规模的网络，而 OSPF 和 IS-IS 协议可用于较大规模的网络。

对于大规模的 IP 网络，为了保证网络的可靠性和可扩展性，内部路由协议（IGP）必须使用链路状态路由协议，只能在 OSPF 与 IS-IS 之间进行选择，下面对两种路由协议进行简单的对比。

目前在 IPv4 网络中大量使用的 OSPF 路由协议版本号为 OSPFv2，能够支持 IPv6 路由信息的 OSPF 版本称为 OSPFv3，能够支持 IPv6 路由信息交换的 ISIS 路由协议称为 IS-ISv6。

OSPFv3

OSPFv3 与 OSPFv2 相比，虽然在机制和选路算法并没有本质的改变，但新增了一些 OSPFv2 不具备的功能。OSPFv3 只能用来交换 IPv6 路由信息，ISISv6 可以同时交换 IPv4 路由信息和 IPv6 路由信息。

OSPF 是基于 IP 层的协议，OSPF v3 是为 IPv6 开发的一套链路状态路由协议。大体与支持 IPv4 的 OSPF v2 版本类似。

对比 OSPF v2 在 OSPF v3 中有以下区别：

虽然 OSPFv3 是为 IPv6 设计的，但是 OSPF 的 Router ID、Area ID 和 LSA Link State ID 依然保持 IPv4 的 32 位的格式，而不是指定一个 IPv6 的地址。所以即使运行 OSPF v3 也需要为路由器分配 IPv4 地址。

协议的运行是按照每一条链路（Per-link）进行的，而不是按照每个子网进行的（per-subnet）：

把地址域从 OSPF 包和一些 LSA 数据包中去除掉，使得成为网络层协议独立的路由协议：

与 OSPFv2 不同，IPv6 的地址不再出现在 OSPF 包中，而是会在链路状态更新数据包中作为 LSA 的负载出现：

Router-LSA 和 Network-LSA 也不再包含网络地址，而只是简单的表示拓扑信息：

邻居路由器的识别将一直使用 Router ID，而不是像 OSPFv2 一样在某些使用端口会将端口地址作为标识。

Link-Local 地址可以作为 OSPF 的转发地址。除了 Virtual link 必须使用 Global unicast 地址或者使用 Site-local 地址。

去掉了认证信息。在 OSPFv3 中不再有认证方面的信息。如果需要加密，可以使用 IPv6 中定义的 IP Authentication Header 来实现。

OSPF 数据包格式发生了一些变化：

OSPF 的版本号由 2 变成了 3；

Hello 包和 Database description 包的选项域增加到 24 位；

认证域去掉了；

Hello 信息中不再包含地址信息；

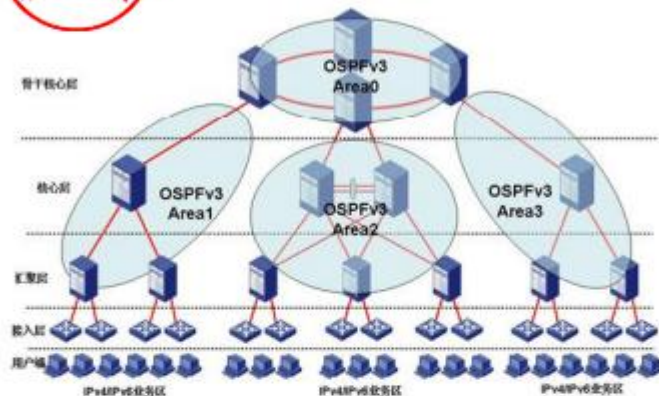
引入了两个新的选项：R 位和 V6 位；

为实现单链路上多 OSPF 进程的实现，在 OSPF 包头中加入了 Instance ID 域；

类型 LSA 3 名字改为：Inter-Area-Prefix-LSA，类型 LSA 4 名字改为：Inter-Area-Router-LSA

OSPF v2 和 OSPF v3 都使用最短路径优先算法，在 Area 划分、链路类型、LSA 传播等方面基本一致。

总的来说，由于 OSPF 发展成熟，厂商支持广泛，已经成为世界上使用最广泛的 IGP，尤其在企业级网络，也是 IETF 推荐的唯一的 IGP。其他路由协议所能适应的网络和具备的主要优点，OSPF 都能适应。



IPv6 网络的 IPv6 路由规划，需要考虑到现有用户的使用习惯和主流的应用模式。IPv6 的 IGP 可以选择 ISISv6 或者 OSPFv3，但是考虑到多数网络用户的习惯以及协议支持的广泛程度，部署 OSPFv3 可能更为实际。

同时 OSPFv3 域的设计可以沿用 OSPFv2 的思路。网络管理和路由规划等设计细节也可以参考原有的 OSPFv2 的原则。

改造后网络全网部署双协议栈，和原有网平滑对接。

在部署的核心、汇聚、接入（三层）交换机上同时运行 OSPFv2 和 OSPFv3 两个路由协议，尽管运行在同一个设备上，这两个路由是互相独立的，OSPFv3 的区域规划和 OSPFv2 可以完全不同。

IPv6 出口的路由规划：

通常来讲，按照国际上 IPv6 地址的分配规则，最终用户会分配到一块或几块 IPv6 PREFIX ::/48 的地址。对于单出口的情况，可能较为简单。接入路由器将指向其他网络的静态路由引入到 IBGP4+中宣告出去。

12.1.5.4.3 IPv6 安全防护

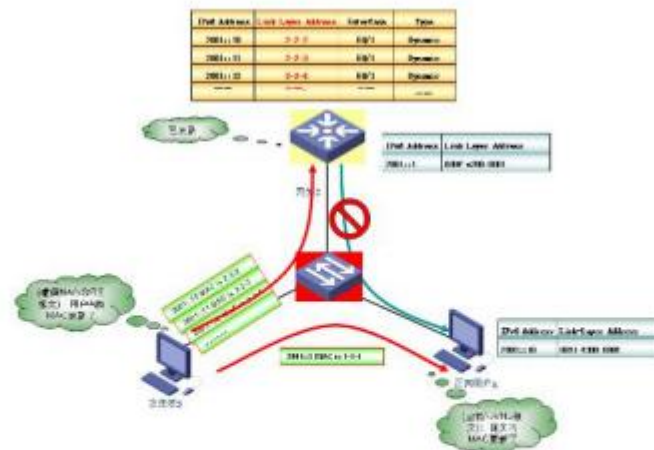
邻居发现协议 (Neighbor Discovery Protocol, 以下称 ND 协议) 是 IPv6 的一个关键协议, 可以说 ND 协议是 IPv4 某些协议在 IPv6 中综合起来的升级和改进, 如 ARP、ICMP 路由器发现和 ICMP 重定向等协议。当然, 作为 IPv6 的基础性协议, ND 还提供了其他功能, 如前缀发现、邻居不可达检测、重复地址检测、地址自动配置等。

在 IPv4 网络中, ARP 攻击问题已经为广大的网络管理者、设备厂商所认识, ARP 攻击能够造成大面积网络不能正常访问外网, 使得正常用户深受其害。针对 ARP 攻击, 大部分的网络设备厂商都推出了自己的 ARP 防攻击解决方案, 在很大程度上解决了 ARP 攻击的问题。而伴随着 IPv6 网络的建设, 在 IPv6 协议族中的 NDP 协议越来越被重视, 而在 ND 协议的设计与 ARP 协议一样并未提供认证机制, 导致网络中的主机是不可信的, 从而使得针对 ND 协议的攻击非常容易。

地址欺骗攻击

攻击者可以使用 RS/NS/NA 报文来修改受害主机或网关上受害主机的 MAC 地址, 造成受害主机无法与网络进行正常的通信。

如下图所示:



RS/NS/NA 仿冒攻击示意图

如上图所示，攻击者能够伪造 NS/NA 报文，发送给网关或受害主机，通过这种方式来对网关上受害主机的 MAC 地址或受害主机上的特定的 MAC 地址进行修改，这样就造成了受害用户无法接收到正常的网络报文。

DAD 攻击

当受害主机进行 DAD 查询的时候，攻击者通过 NS 或 NA 报文进行干扰，使得受害主机的 DAD 过程失败，无法获取到 IP 地址，这种攻击的概率和 NS/NA 的欺骗攻击相比，相对较少。见下图：

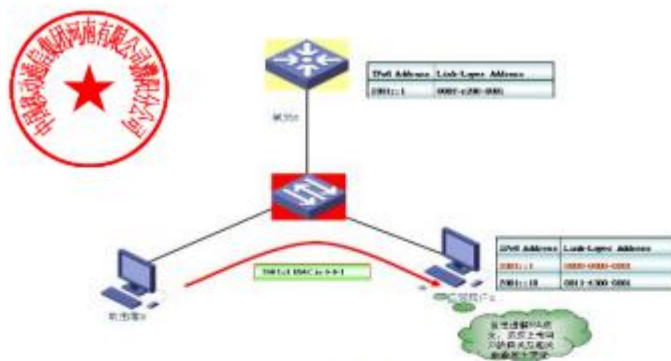


DAD 攻击示意图

如上图所示，在受害者进行 DAD 检测时，攻击者可以伪造 NS 报文，与受害者产生冲突，也可以伪造 NA 报文，应答受害者的 NS 报文。这两种情况，受害主机都无法获取地址，进行正常的网络通信。

RA 攻击

RA 能够携带很多网络配置信息，包括默认路由器，网络前缀列表，是否使用 DHCP 服务器进行有状态地址分配等网络配置的关键信息。如果受害者接收了虚假的 RA 信息，会造成网络配置错误，从而引发欺骗攻击。



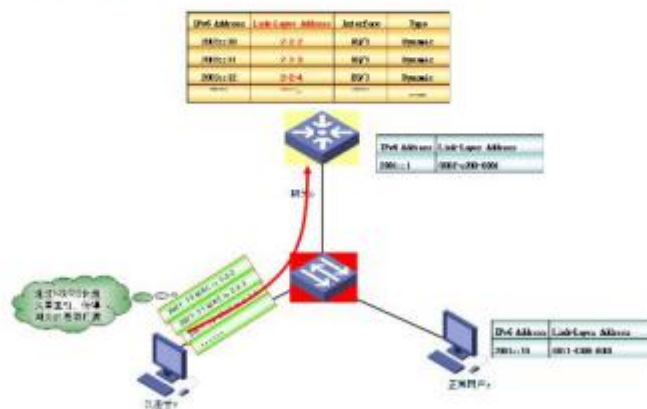
RA 攻击示意图

如上图所示，攻击者发送伪造的 RA 报文，其中可以造成多种攻击：

- 1) 伪造不存在的前缀，修改受害主机路由表。
- 2) 伪造网关的 MAC 及 lifetime，造成受害主机的默认网关改变。
- 3) 伪造 DHCP 服务器，同时伪造 RA 中的 M bit，造成受害主机使用 DHCP 服务器分配到虚假的地址。

针对网关的泛洪攻击

通过发送大量的 NS/RS 报文，造成网关的表项溢出。



泛洪攻击示意图

攻击者通过伪造大量的 NS/RS 报文，发送给网关，使得网关的表项溢出，造成网关无法提供正常的服务。

ND 防攻击解决方案

通过对上述的 ND 攻击类型的介绍。我们可以推出发现当前 ND 攻击防御的关键所在：如何获取到合法用户和网关的 IPv6 地址-MAC 对应关系，并如何利用该对应关系对 ND 报文进行检查，过滤掉非法 ND 报文。公司解决这一关键问题的思路是，通过自动的 ND 监控模式、DHCP 监控模式与手工配置的方式，获取到合法用户的 IP-MAC 对应关系。再配合 RA trust 与 DHCP trust 对 RA 报文与 DHCP 报文进行限制，从而解决不同环境下的 ND 防攻击问题。

同时，为了避免网关的 ND 表项被异常的 ND 报文打满溢出造成 DoS 攻击，在网关上能够针对端口配置最大的 ND 表项学习数量，能够缓解此类攻击。

信任表项与 ND Detection

从前文的描述，我们知道，在局域网中 ARP 或 ND 攻击的根本原因是无法对所交互的 ARP 或 ND 报文进行验证，从而无法得知正确的用户 IP、MAC、端口的绑定信息，所以无法对异常的 ND 报文进行过滤，使得网络中可能发生 ARP/ND 攻击。

通过 ND snooping、DHCP snooping、手工配置等手段在接入层交换机上建立的一张 IP、MAC、Port 的可信表项，获取可靠的用户 IP 地址与 MAC 地址的对应关系。通过这张表项，结合 ND Detection 技术，对异常的 ND 报文进行过滤，达到防止 ND 攻击的效果。

的 ND snooping 与 DHCP snooping 是一种动态获取用户 IP、MAC、Port 对应关系的技术，下面分别对这两种技术进行简要描述：

ND snooping：ND 协议报文的交互过程在上文已经进行了描述，在 ND snooping 中，监听 ND 协议的 DAD 交互过程，获取用户的 IP、MAC、Port 的对应关系。

DHCP snooping：通过监听 DHCP 的交互过程，获得用户的 IP、MAC、Port 的绑定表项。

手工绑定表项：手工绑定是一种常用的技术，在一些规模不大的网络中，或者对安全性要求较高且不经常变化的网络中，使用手工绑定来建立可信表项。

在建立了绑定表项之后，能够保证一个已经获取了 IP 地址的用户只能使用已获取的地址进行通信，过滤掉所有的不在绑定表项中的 IPv6 的非法用户发送的 IP 报文。

ND Detection 是在 ND 防攻击方面的创新技术，通过结合已经建立的绑定表项，这个绑定表项可以是使用 ND snooping，DHCP snooping，手工来进行配置的，通过比较已经获取到的可信表项中的 IP 与 MAC 地址，对 ND 报文进行过滤，丢弃异常的报文。相比单纯使用 ACL 进行

的用户绑定，ND Detection 技术结合绑定表项对 ND 报文进行过滤，能够较好的防御 ND 攻击。

RA Trust 与 DHCP Trust

RA Trust 与 DHCP Trust 的功能不同，但是思路是相同的，管理员可以在相应的连接 DHCP 服务器或网关的接口上配置，通过手工指定连接 DHCP 服务器与连接发送 RA 的设备的接口（通常是网关），能够避免网络中 DHCP 报文与 RA 报文的任意发送。当进行了 RA Trust 与 DHCP Trust 后，DHCP 的服务器端报文与 RA 报文只能从配置了 TRUST 的端口进入，避免了 DHCP 服务器欺骗与 RA 攻击，提升了局域网安全性。

综上所述，的 ND 防攻击解决方案，通过在网络设备学习可信的用户接入表项，同时配合 ND Detection 技术，对非法报文进行过滤，提高了用户侧 ND 报文的可信性及安全性。再配合 DHCP Trust 与 RA Trust 功能，禁止非法的 DHCP 报文与 RA 报文发送，从多方面提升了 ND 协议的安全性，解决了在 IPv6 网络中存在的 ND 攻击问题。

12.1.5.5 IPv6+

12.1.5.5.1 SRv6

随着数字政府建设的深入，传统的 MPLS 技术越来越难以满足业务发展需求。专网整合、数云网的融合需要更快速的业务部署；视频会议等重要业务需要更可靠的差异化的质量和路径保障；接入单位接入业务的多样性需要更加智能自动化的精细运维。

在 IPv6 时代，SRv6 是 IPv6 下 SDN 化的最佳实现方式。SRv6 是一个基于 IPv6 的分段路由转发技术，有效解决上述传统广域网技术的瓶颈；SRv6 技术作为 IPv6+ 技术体系的基石，天然和 SDN 技术适配，可作为智慧电子政务外网的坚实基座。

SRv6 技术价值

SRv6 技术主要优势包括：

（1）简化网络承载，降低运维难度，提升网络健壮性

不论是 IPv4 还是 IPv6 业务，不论是公网还是 VPN 私网业务都可以通过 SRv6 隧道承载，实现骨干承载 IPv6 单栈部署下各类业务全承载。

SRv6 不再使用 LDP、RSVP-TE 等协议进行标签分发，可通过 IGP 协议直接进行标签分发，消除 MPLS 网络中 LDP 和 IGP 的同步问题。

SRv6 可以和 L2VPN 相结合, 实现 L2VPN、L3VPN 业务的统一控制。

简化的电子政务外网可以在满足 VPN 业务承载基础上, 简化网络配置, 降低运维难度, 有效的提升业务的可靠性。

(2) 业务灵活编排, 重点按需保障, 业务随需而动

SRv6 基于源路由思想实现路径的编排。SRv6 报文头中封装 SID 列表, 每个 SID 标识沿途需要经过的节点或路径。通过和 SDN 控制器配合, 按照业务时延抖动等质量诉求, 给源点下发路径指令, 封装沿途路径列表信息, 实现网络的可编程、业务路径的灵活调度, 满足重保业务对网络的差异化服务需求。

视频会议是电子政务外网中的一项重要业务, SRv6+SDN 技术可以有效支撑视频会议对网络最佳路径, 最佳质量路径的业务诉求。

(3) 加速业务上云, 加速专网整合, 促进云网深度融合

SRv6 基于 IPv6 实现, 如果中间设备不支持 SRv6, 则报文按照传统 IPv6 路由方式转发, 因此只需要业务两端 PE 支持 SRv6, 中间设备支持 IPv6 即可。

专网整合时, 在开通新的 VPN 业务时, SRv6 可以减少中间设备配置及协调工作量, 加速业务整合下发。业务上云时, 中间设备配置无需变更, 业务可一跳入政务云。同时, 通过编排器, 整合广域网控制器、数据中心控制器, 园区控制器, 实现业务统一管控, 端到端拉通, 促进云网的深度融合。

(4) 简化跨域组网, 便捷互通兼容, 利网络平滑演进

和 MPLS 标签不同的是: SRv6 的 SID 以 128 位的 IPv6 地址形式表示, 继承了 IPv6 地址的可路由可聚合特性。由于 SRv6 SID 可路由, 全局规划后, 可以天然支持跨域传播, 同时通过层次化规划 SRv6 SID 后, 可以通过可聚合减少来标签的路由规模。当前, 省电子政务外网和国家电子政务外网之间, 省电子政务外网和地市电子政务外网之间, 电子政务外网和政务云之间多处存在跨域, SRv6 将很好的协助跨域间的业务开通。

SRv6 支持通过 SRv6 SID 和 MPLS 标签拼接, 跨域等技术, 实现 SRv6 网络和 MPLS 网络的兼容并存, 有效支持现存 MPLS 网络到 SRv6 的平滑过度。

(5) 高可靠性、故障快速恢复, 保业务稳定运行

SRv6 协议具备快速重路由能力, 在设备及链路故障产生时, 可实现路径快速自动收敛, 降低网络故障切换时间, 保障业务运行的可靠性。

SRv6 技术介绍

SR (Segment Routing, 段路由) 采用源节点路径选择机制, 预先在源节点封装好路径所要经过的 SID (Segment Identifier, 段标识), 当报文经过 SR 节点时, 该节点根据报文的 SID 对其进行转发。除源节点外, 其它节点无需维护路径状态。SRv6 是指在 IPv6 网络中使用 SR, 将 IPv6 地址作为 SID 对报文进行转发。

1、SRv6 基础原理

1) SRv6 SID 格式:

在 SRv6 中, 定义某种网络功能、代表网络指令的 SID。这种 SID 采用 IPv6 地址形式, 但不与任何设备上的接口地址对应。该 SID 被称为 SRv6 SID。如图所示, SRv6 SID 由 Locator、Function、Arguments 和 MBZ 四部分组成:

Locator: 标识 SID 所属的网段。Locator 在 SR 域内唯一。

Function: 标识与 SID 绑定的本地操作指令, SR 域内指定节点收到流量后, 根据 SRv6 SID 的 Function 字段执行相关操作。

Arguments: 定义报文的流和服务等信息。

MBZ (Must be zero): 当 Locator、Function 和 Arguments 的位数之和小于 128bits 时, 其他位使用 0 补齐。



图 SRv6 SID 格式

2) SRv6 报文格式:

SRv6 的报文封装格式为: 在原始三层数据报文前面添加新的 IPv6 基本头和 SRH (Segment Routing Header, SRv6 报文头)。SRH 是路由类型取值为 4 的一种路由扩展头。如下图所示, IPv6 基本头中 Next Header 取值为 43, 表明下一个报文头为路由扩展头。路由扩展头的路由类型字段取值为 4, 表明该路由扩展头为 SRH。SRH 主要包含以下几个部分:

Next Header: 8bits, 用来标识下一个报文头的类型。

Hdr Ext Len: 8bits, 表示以 8 个字节为单位的 SRH 头的长度, 不包括前 8 个字节。

Routing Type: 8bits, 路由类型字段, 取值为 4, 表示携带的是 SRH。

Segments Left: 8bits, 标识需要查看的下一个 SID 的编号, 初始取值为 n-1 (n 表示路由扩展头中 SID 的数目), 每经过一个节点减 1。

Last Entry: 8bits, SRH 头中报文实际转发路径的第一个 SID 的编号。

Flags: 8 bits, 标志位信息。

Tag: 8 bits, 用来标记具有相同特性的一组报文。

Segment List: SID列表。按照报文转发路径上节点从远到近的顺序进行排列, 即 Segment List [0]表示路径的最后一个 SID, Segment List [1]表示路径的倒数第二个 SID, 以此类推。

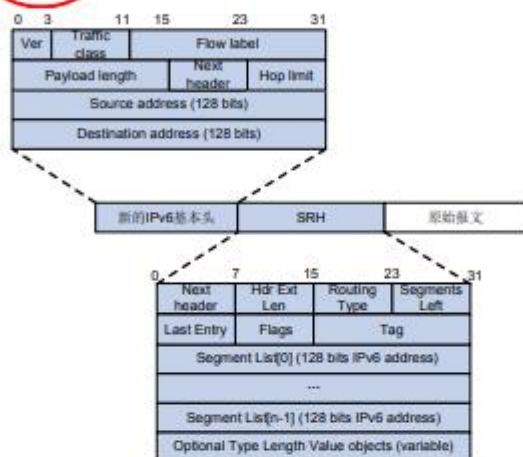


图: SRv6 报文格式

3) SRv6 设备角色

源节点: 负责在 IPv6 报文的 IPv6 头中插入 SRH 扩展头, 或者在报文外加上 IPv6 头和插入 SRH 扩展头的节点, 该节点将报文流引入 SRH 的 Segment List 定义的 SRv6 路径。如果 Segment List 中只包含一个 SID, 并且不需要在 SRH 中携带信息或 TLV, 则只需要将 IPv6 头的目的地址设置为这个 SID, 而不需要插入 SRH。源节点可以是产生 SRv6 报文的主机, 也可以是 SRv6 域的边缘设备。

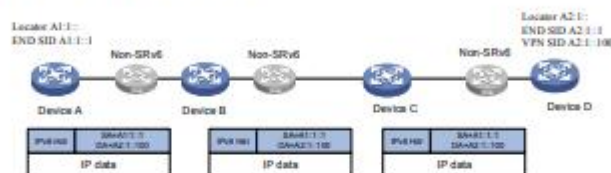
中转节点: 在报文的 SRv6 路径上, 不参与 SRv6 处理, 只执行普通 IPv6 转发报文的节点。节点收到 SRv6 报文, 如果 IPv6 目的地址不是本地配置的 SRv6 SID, 则将报文当作普通 IPv6 报文处理, 不处理 SRH。中转节点可以是支持 SRv6 的节点, 也可以是不支持 SRv6 的节点。

SRv6 Segment Endpoint 节点: 收到 SRv6 报文的节点, 如果 IPv6 目的地址是节点上配置的 SRv6 SID, 该节点需要按该 SID 绑定的指令进行处理, 并更新 SRH, 这个节点就是 SRv6 Segment Endpoint 节点。

4) SRv6 隧道技术:

SRv6 隧道分为两种: SRv6 BE (Best Effort) 和 SRv6 TE Policy (Traffic Engineering)。

SRv6 BE 基于 IGP 最短路径和 BGP 路由优选来指导流量转发。网络中仅需要部署 IGP, BGP 传递路由不需部署其他协议, 中间设备无需部署 SRv6, 只需要支持 IPv6 即可, 部署简单, 支持业务的快速开通。但是不支持基于路径的调度编排, 不支持流量按需调度。SRv6 BE 适用于链路带宽充足场景, 用于非关键业务承载。



SRv6 TE Policy 按照候选路径的显示路径进行转发, 结合 SDN 控制器可根据丰富的 SLA 策略进行路径计算, SLA 策略可包括优先级、带宽、时延、抖动、丢包、时间段、链路/节点偏好等, 满足业务差异化保障需求。SRv6 TE Policy 多候选路径、多 Segment list 机制, 可实现灵活的进行路径编排, 多条路径时可提供等价负载分担、权重负载分担服务, 同时通过隧道热备份提供路径保护机制。在极端情况下 SRv6 TE Policy 全部故障, 流量可自动逃生至 SRv6 BE, 业务转发不受影响。

SRv6 TE Policy 由三部分标识:

BSID: 入节点的 SID。

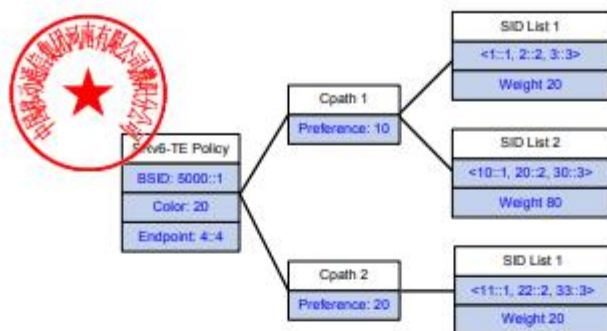
Color: 转发路径的 Color 属性, 用于在相同的源和目的节点之间区分多个 SRv6 TE Policy。

End-point: SRv6 TE Policy 目的节点的 IPv6 地址。

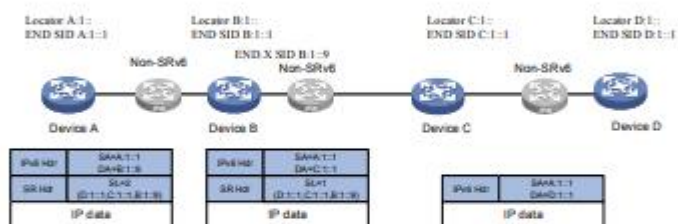
如下图所示, 一个 SRv6 TE Policy 由多条具有不同优先级的 Candidate Paths (候选路径) 组成, 每个候选路径包括由 Segment List (SID 列表) 标识的一条或多条转发路径。

候选路径: 一个 SRv6 TE Policy 包含一条或多条候选路径。通过 SRv6 TE Policy 转发流量时, 设备根据候选路径的优先级从多条候选路径中选择最优路径。不同 SRv6 TE Policy 不能共享同一条候选路径。

SID 列表: SID 列表包含报文转发路径信息, 由转发路径上各个节点的 SID (IPv6 地址) 组成。候选路由由一个 SID 列表或者多个带权重的 SID 列表组成。SRv6 TE Policy 选择某条候选路径后, 会根据 SID 列表的权重, 在候选路径的多个 SID 列表间进行负载分担。



SRv6 TE Policy 转发流程如下：



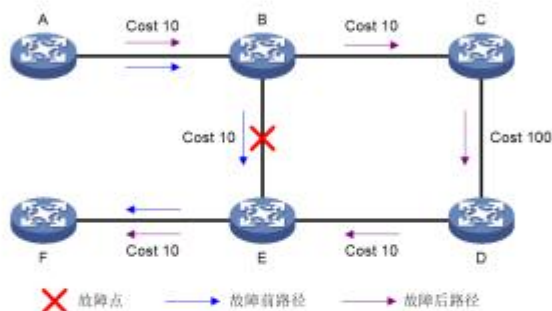
综述，SRv6 BE 提供 VPN 承载和可靠性服务；SRv6 TE Policy 除 SRv6 BE 能力外，还提供路径控制和调优、差异化 SLA 保障服务。

项目	SRv6 BE	SRv6 TE Policy
概念	基础数据承载，尽力而为	流量工程策略，路径灵活调度
路径计算	路由计算，路径无法编程	路径灵活调度，基于延时、带宽、丢包等约束的路径规划
配置	简单，可不需控制器	复杂，需控制器
场景	SLA 要求低，无调度需求	对 SLA 要求严格，有调度需求
设备要求	低、中间设备支持 IPv6 即可	中、调度节点需要支持 SRv6
业务开通	快	中

5) SRv6 TI-LFA 高可靠技术

SRv6 TI-LFA FRR (Topology-Independent Loop-free Alternate Fast Reroute, 拓扑无关无环备份快速重路由) 能为 SRv6 提供链路及节点的保护, 通过预先计算出显式路径表示的备份路径, 当某处链路或节点发生故障时, 流量会快速切换到备份路径继续转发, 从而最大程度避免流量的丢失。

如下图, 当节点 B 和节点 E 之间发生故障后, 节点 B 启用 TI-LFA 计算的备份路径, 为报文指定必须经过 C->D 之间的链路的显式路径表示的备份路径, 保证报文可以沿着备份路径转发。



SRv6 TI-LFA FRR 同时适用于 SRv6 BE 和 SRv6 TE Policy 场景。正常情况下, SRv6 BE 报文封装本身不需要携带 SRH 信息, 但是在 TI-LFA FRR 场景, 为了封装 Repair List 信息, SRv6 BE 报文封装也需要携带 SRH 信息。

3、SRv6 未来发展

当前 SRv6 虽然具备诸多优点, 但是缺点同样明显。主要的缺点在于当 SID 数目增多时, 报文头开销过大。SRv6 报文头过长带来的挑战主要分为以下三个方面:

报文头开销大导致网络链路带宽利用率低, 256byte 负荷包长在 8 层 SID 的情况下带宽利用率只有 60%左右:

新增报文头长度可能导致报文大小超过 MTU, 导致分片或丢包, 导致传输性能急剧下降;

SRv6 报文处理对芯片要求高, 老旧现网设备难以支持深度的报文头的复制操作。

基于以上这些问题, 业界推出基于 SRv6 头压缩技术: G-SRv6。该方案兼容标准 SRv6, 使用固定的 SID 压缩长度, 兼容原有地址规划, 支持现网平滑升级是目前业界领先的 SRv6 及 SRv6 头压缩方案。

1) G-SRv6 技术价值:

在 32bit 压缩中, SRv6 理论上可以将原有 SID 的封装效率提高到 75%左右, 显著减少了报头开销, 扩展了 SRv6 的应用部署范围。同时, G-SRv6 兼容 SRv6, 支持压缩 SRv6 与原生 SRv6 混合编程, 天然支持与原生 SRv6 互联互通, 可支持从普通 SRv6 存量演进, 平滑升级到 G-SRv6。

2) G-SRv6 技术原理:



一个 SRv6 网络中很多 SID 都具有共同前缀 (Common Prefix), 一个 SID List 中 SID 的共同前缀部分都是重复冗余的。所以, SID list 中去掉 SRv6 SID 中的 Common Prefix 部分和其他冗余部分, 保留 Node ID 和 Function ID 作为压缩 SID, 可以很好的减少报文头开销。这也是 SRv6 头压缩方案中的 G-SID (Generalized SID, 通用段标识符) 的基本压缩原理。

G-SID 是可压缩 SRv6 SID 的一部分, 和 Common Prefix 以及 Argument/Padding 一起组合成完整的 SRv6 SID。G-SID 支持 32bit 或者 16bit 两种长度。从硬件处理效率、利旧和可扩展性的角度出发, 一般推荐 32 bit 的 G-SID 长度。由于 G-SID 需要连续的 32 个 bit 位, 填充 Node ID 和 Function ID, 因此在规划 SRv6 locator 地址规划时, 需要规划或预留。

12.1.5.5.2 随流检测

电子政务外网作为委办局接入的公共基础设施, 承载着各种各样不同需求的业务, 如数据, 语音和视频等业务, 其中, 视频会议对网络的质量要求非常高, 视频会议对网络丢包、时延和时延抖动非常敏感, 轻则语音卡顿、视频马赛克, 严重时会导致会议中断。因此在会前准备阶段, 会务组希望能够通过测试会议, 提前测试视频会议终端和网络运行情况。当会议质量不佳时, 需要能够快速定位, 尽快排除网络故障: 是网络设备的问题, 还是视频会议应用系统有问题; 是广域网的问题, 还是委办局的局域网有问题? 在测试会议时, 视频会议业务在网络上的运行质量情况也希望能够可看可查。

当前, 常规都是通过手工 ping、traceroute 等方式模拟报文发包的情况, 通过计算模拟报文的丢包率、时延, 间接得到业务报文的丢包率和时延。这种方式中模拟报文和实际业务流, 在流量路径, 优先级等方面存在差异, 因此无法反映出业务真实的质量; 同时手工方式诊断, 存在定位效率低, 易出错等问题, 严重影响定位效率。

因此，业界提出一种新型的随流检测技术（iFIT（in-situ Flow Information Telemetry）），通过直接测量业务报文得到业务的真实丢包率和时延等信息，通过 Telemetry 技术，将统计信息秒级上报给分析器呈现，通过智能化，自动化方式提升故障定界定位水平。iFIT 技术遵循 RFC 8321。

随流检测技术价值

相较于传统丢包测量技术，iFIT 具有以下优势：

检测精度高：直接对业务报文进行测量，测量数据可以真实反映网络质量状况。

部署简单：中下游设备可以根据 iFIT 报文生成测量信息。

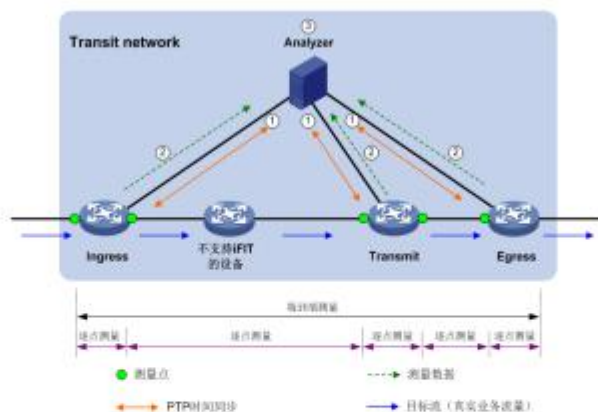
快速定位故障功能：iFIT 提供了随流检测功能，可以真正实时地检测用户流的时延，丢包情况。

可视化功能：iFIT 通过可视化界面展示性能数据，具备快速发现故障点的能力。

支持路径自发现功能：iFIT 在网络中的入节点对于用户关心的业务流程增加报文头，下游设备可以根据 iFIT 报文头自动识别该业务流并生成统计测量信息；分析器可以通过该功能感知业务流量在网络中的实时路径。

基于硬件实现，对于网络影响较小，可扩展性强。

随流检测技术介绍



iFIT 的工作流程如下：

1、分析器和所有 iFIT 设备之间通过 PTP 协议完成时间的同步。

2、iFIT 设备对目标流报文进行 iFIT 处理。

A) 入流量对网络出口的报文流进行解析，识别出目标流，并给目标流报文添加 iFIT 报文头，记录收到每个统计周期第一个报文的时间，同时统计每个周期内收到的目标流报文的个数。然后，按周期将报文计数和时间戳等信息通过 gRPC 连接上报给分析器。

B) 在目标穿越网络的传输接口（在目标穿越网络中支持 iFIT 的设备上，目标流的流入接口和流出接口），对于包含 iFIT 报文头的报文，记录收到每个统计周期第一个报文的时间，同时统计每个周期内收到的目标流报文的个数。然后，按周期将报文计数和时间戳等信息通过 gRPC 连接上报给分析器。

C) 在目标穿越网络的出接口（目标流离开目标穿越网络的接口），对于包含 iFIT 报文头的报文，记录收到每个统计周期第一个报文的时间，同时统计每个周期内收到的目标流报文的个数。然后，按周期将报文计数和时间戳等信息通过 gRPC 连接上报给分析器。最后，去掉目标流报文中的 iFIT 报文头，继续转发。

3、分析器对相同周期、相同目标流进行丢包分析，计算时延。

随流检测技术部署：

1) iFIT 适用于 MPLS、SR-MPLS、SRv6 网络。

2) 如果需要统计流量的时延和抖动信息，那么需要全网部署 1588v2，保障网络设备间的时间同步。

3) iFIT 支持端到端测试和逐点测试两种测量类型。当用户希望测量整个网络的丢包和时延性能时，可以选择端到端测量模式；当用户希望准确定位每个网络节点的丢包和时延性能时，可以选择逐跳测量模式。网络安全服务方案

12.1.5.5.3 网络安全设计

在核心路由侧部署边界安全防护服务，提供向上连接省广域网核心路由服务，向下连接区县级城域网，提供边界隔离防护能力。

在路由器上，根据用户的源 IP 地址，使用策略路由，将相应的业务引入到不同 VPN 的虚拟防火墙中，通过虚拟防火墙对纵向 VPN 和共享 VPN 提供安全防护，数据通过 MPLS VPN 的策略进行标签转发。

本次方案设计采用了融合一体化安全网关设备，提供 NAT、包过滤、安全区域划分、基础安全防护等功能，基于全新的软硬件提供了许多基于应用的安全防护手段及扩展的运维手段

功能；可通过在安全网关上配置抗 DDOS、智能负载均衡、防火墙、IPS 及防病毒等多种安全业务模块实现多种安全防护功能。

通过多种安全业务模块安全功能的相互配合，在网络结构安全、网络访问控制、网络安全审计、网络入侵防范、恶意代码防范、网络设备防护等方面对政务外网出口进行全面的安全防范，充分满足国家法规要求。

本次方案采用基于全新多核处理器架构的专用防火墙安全模块，对网络层、应用层安全进行融合，并采用独有的“并行流过滤引擎”技术，实现一次解包，并行检测，全部安全策略可以一次匹配完成，即使在应用层功能不断扩展的情况下，也不会造成性能的下降和网络时延的增加。

能够对一定时间内的策略日志数据进行分析统计，自动学习和发现会话日志中的访问流量，从而智能生成符合当前网络状态的安全策略。此外，防火墙模块还能统计一定时间内安全策略的命中数量，帮助运维人员发现无用的安全策略，迅速完成策略梳理。

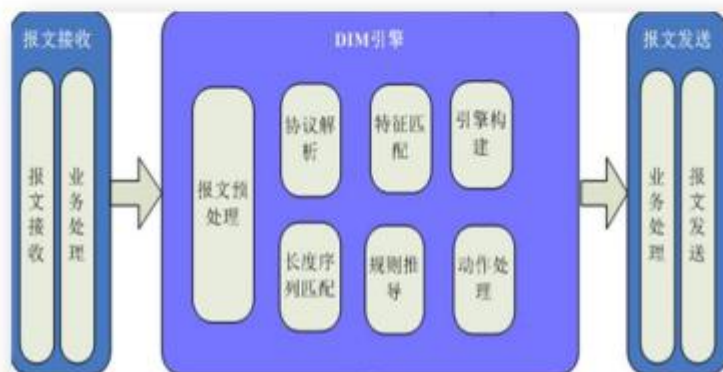
同时，一旦出现网络故障，出口大流量形势下不再适用传统的端口镜像、抓包分析等技术手段，本次使用的防火墙模块内置了数据流分析工具，能够模拟一个数据包从设备入接口到出接口所经过的所有功能模块，通过设备反馈的处理情况，管理人员能够详细了解数据包的处理过程，准确定位数据包状态，迅速排查网络故障，无需从海量的抓包文件中分析，提取问题报文，提升运维体验；

随着网络的飞速发展，以蠕虫、病毒、木马、间谍软件为代表的攻击层出不穷。传统的防护只能针对报文头进行检查和规则匹配，而大量应用层攻击都隐藏在正常报文中，甚至是跨越几个报文，因此仅仅分析单个报文头意义不大。传统 IPS 通常采用识别攻击特征的方式来实现攻击检测，但攻击变种层出不穷、业务应用种类繁多，简单的特征识别方式容易造成较高的误报率及漏报率。

本方案建设中在安全网关上配置全新的入侵防御及防病毒安全模块，全新 IPS 模块采用专用的四大检测引擎：防逃逸检测引擎确保变种攻击无法生效、协议智能推导引擎和协议语义解析引擎对流量进行深度检查与解析、虚拟环境检测引擎通过分析异常行为防护未知威胁，多重安全检测引擎确保入侵防御系统具有极低的误报率和漏报率，安全模块内置了主流杀毒软件厂家的病毒引擎，与主流防病毒厂商合作，能够第一时间对最新的病毒提供可靠的检测、识别、阻断。

DPI 是 Deep Packet Inspect 的简称，是传统 IPS 或者 ACG 设备中的核心技术，旨在借助

字符串特征的逐包匹配来完成入侵检测和流量控制的目的。DPI 技术与搜索引擎的技术恰恰相反，后者的一次搜索是从海量的数据对象中找出特定的片段的所有出现，而 DPI 的一次搜索是从一个特定的片段(一个数据包)中找出海量的数据对象是否有出现。DPI 需要搜索的数据对象称之为检测规则，传统意义的检测规则都是用“字符串特征”来定义的。例如：访问新浪的网站，在第一个 HTTP 请求包的 HOST 域中都携带有 sina.com 的字样，这个字符串就可以作为访问新浪网站的“特征”。



从控制(管理)层面上看，DPI 的各个业务模块的需求都可以抽象化成“规则”，规则之上有“分类”对象，规则同时具有“使能状态、报文动作”等属性，规则内部还有“特征”“选项”等部件。因此，设计上有统一的检测管理框架（DIM），将业务模块的公共业务需求抽象和统一处理，这些需求包括：

- 统一开放格式的规则管理。
- 统一开放格式的特征库加载和文件解析。
- 配置变更和下发流程管理，包括引擎的编译和下发、规则的下发，以及它们的板间同步。

从数据转发层面上看，DPI 的各个业务需求都需要对应用层协议进行解析、解码和搜索。为了保证高效转发和单次报文处理，有别于传统防火墙的设计思路下一代防火墙中必须有并行的检测引擎，保证报文的处理尽可能只有一次。数据转发层面的需求主要由如下几个部件完成：

- 协议解析器。

➤ 搜索算法引擎。

➤ 检测引擎结果处理模块，或者说报文动作处理模块。

规则引擎以协议类型、会话方向、协议域、编码格式、模式串等维度抽象出来用于描述特征的语句。DPI引擎除了可以接纳开放式 TLV 架构的规则，还支持状态事件类、流量模型类等多种规则定义方式。

业务模块	业务模块基本功能介绍	规则的抽象	规则外层的分类
应用可视化控制	可基于应用、应用组、用户、用户组等进行精细化的管理和控制	一个规则对应一个 Application	Application Group: 例如聊天软件、流媒体、游戏等
数据过滤	对应用的内容进行过滤，尤其是对关键字或者文件类型进行过滤	一个规则对应一条 Match Rule 的配置	Content Inspect Class: 例如政治敏感词、公司敏感词等
入侵防御系统	对应用层攻击进行检测并防御的安全防御技术。通过分析流经设备的网络流量，实时检测入侵行为，并做出相应动作，来阻断入侵行为，实现保护企业信息系统和网络免遭攻击的目的	一个规则就是一条描述入侵的攻击规则。	Attacking Category: 例如漏洞、蠕虫等；或者 Attacking Target (有些地方也叫做保护对象): 例如操作系统、Web 服务器等
URL 过滤	对用户访问的 URL 进行控制，即允许或禁止用户访问的 Web 资源，达到规范用户上网行为的目的	一个规则就是一条 URL。	URL Category: 例如新闻、学术、社交、购物、色情等。一个 URL 可以同时属于多个分类

12.1.5.5.4 互联网出口边界防御

安全出口防护：采用部署下一代防火墙的方式实现出口安全，通过在下一代防火墙上通过软件授权方式开启入侵防御、负载均衡、流量控制等一系列集成功能，只有通过将各种安全业务进行深度融合，并借助虚拟化技术实现安全业务层的无缝融合，才能达到简化网络架构、提高网络效率、在融合过程中保护用户既有资源的目的。融合安全网关作为整个互联网的出口，因此必须提供高性能的数据转发和丰富的安全特性。并且融合安全网关不仅仅是一个高速的数据转发中心，还要是一个综合安全防护平台，以保证后期各种新业务和应用在基础网络平台上平滑部署和升级，满足相关业务的增长需求。因此各种应用安全模块可以无缝的部署在安全网关平台上，提供安全融合网络的解决方案。

在安全防护网关上启用 MPLS VPN 隔离各部门及各业务，MPLS VPN 终结在 PE 上。在互联网通过 IPSec VPN 隧道隔离，各部门业务通过独立的 IPSec VPN 隧道连接到政务外网。应在 IPSec VPN 网关和 PE 之间设置相关的策略或启用相关的功能，达到各部门的访问流量端到端隔离的效果。不同政务部门业务流量在通过 IPSec VPN 网关及 PE 设备之后，只能进入本部门所在政务外网骨干网上的 MPLS VPN 通道之中，或者根据需要进入相应的信息共享 MPLS VPN 通道，而不会流向其它部门的私有 MPLS VPN 通道中，以保证不同部门不同业务的安全隔离。

支持 IPSEC VPN、SSL VPN、GRE VPN、L2TP VPN 等多种 VPN 接入方式，与城域网核心通过配置多个子接口或配置多个 VLAN 实现不同业务对接。用户访问 VPN 所对应的 IP 地址或域名时，安全网关通过 NAT 将 VPN 流量转发至 VPN 网关，VPN 网关在完成接入用户 VPN 认证对接后，将 VPN 数据进行解密，后通过配置子接口与城域网核心对接，解密后的数据通过安全网关防火墙模块、入侵防御模块进行安全防护。

在 VPN 网关上针对不同的源 IP 地址和目的 IP 地址配置相应的策略路由。外部加密数据到达网关后根据 VPN 策略匹配相应的隧道，数据解密完成后，再根据源、目的地址，匹配对应的策略路由然后通过配置的不同 VLAN 对接核心 VRF，将数据发送至不同的 VRF。

PE 设备会根据接收的子接口将数据再封装到对应的 MPLS VPN 隧道中。同时在 VPN 内建立状态表。从 PE 设备发送到 VPN，首先会查询中已建立的状态表，根据目的 IP，送入相应的隧道做加密操作，然后发往隧道的对端设备，实现 VPN 访问。

在移动用户侧通过安装 VPN 客户端软件或者通过 IE 浏览器，直接发起 VPN 连接请求，在电子政务外网核心入口处的集中式 VPN 网关上对这些移动用户发起的 VPN 连接请求做统一的处

理，移动用户的接入比较简单。移动用户无论身处何处，只要能登陆 INTERNET（无论任何接入方式，无论任何带宽），即可实现 VPN 接入。这样实现了一个逻辑点到多点的星型结构，对每个移动用户而言，实现了与集中 VPN 网关的单独逻辑连接。

上网行为管理：本方案建设中在出口部署全新的高性能流量控制及与流量分析专用硬件模块。透明模式接入网络中，对经过的数据流量进行分析，实现对用户行为的审计和控制。

具备丰富身份认证方式，可有效的区分用户。是部署差异化授权和审计策略、有效防御身份冒充、权限扩散与滥用等的管理基础。身份认证方式有：

本地认证：Web 认证、用户名/密码认证、IP/MAC/IP-MAC 绑定；

第三方认证：RADIUS、LDAP 等；

短信认证：传统的认证方式，方便快捷；

免认证：认证用户无需进行身份认证，即可快速上网；

APP 认证：不需要借助数据中心软件，无需 APP 修改，避免协调沟通成本；

微信公众号认证：强制关注，自动弹出“一键微信连 WIFI”并关注微信公众号；

混合认证：界面配置选择多种认证方式，用户可根据需要更换认证方式；

单点登录：AD 域一次认证，减免频繁认证。

二维码认证：访客网络安全，管理授权网络访问。

具有业界数量最大、本地化支持最完善、更新最及时的特征库，可识别超过 9000+种网络和应用层协议。借助于应用识别功能，可以准确识别网络上正在运行的应用，应用流量的准确识别不但可洞悉整个网络的运行情况，而且可针对具体需求做用户行为的准确管控，这在一定程度上既可保证业务流的高效运行也可预防由于内网机器受到攻击而生产的威胁，同时识别应用类型也是应用审计与应用流量控制的基础。

随着 P2P 应用的广泛流行和基于 Web 的应用的兴起，令传统的利用固定端口来区分应用类型的设备无能为力。应用识别功能把对报文的协议解析、深度内容检测以及关联分析结合起来，通过对大量实际环境中的流量的分析，总结出每种应用的流量模型，把对数据包的协议解析、深度内容检测和关系分析的结果综合起来，由决策引擎通过与流量模拟的匹配程度，智能的判定应用类型，相比传统的应用识别技术，还具有以下特点：

自定义应用：办公自动化的趋势下，内网均已搭建了应用系统，例如 OA 系统等。面对这种情况，上网行为管理产品通过自带的特性库无法对企业应用系统机型识别、审计和管理具备自定义应用功能，管理员可根据协议、目标端口、IP、域名等维度创建应用特征，进而针

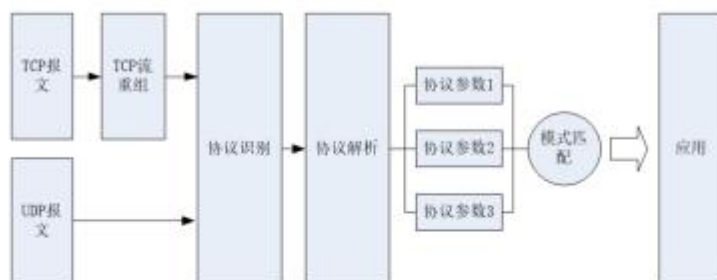
对应用进行审计、流量统计和控制。



基于协议状态分析：对已知协议和 RFC 规范的深入理解，可准确、高效的对各种协议进行解析。例如，对于一次 HTTP 访问，先由协议解析出访问的 URL、Host、User-Agent 等信息，再将解析出来的信息进行特征匹配，这样可以带来以下优点：

提高性能，不需要对整个报文进行模板匹配，可以提高应用识别的性能。

降低误识别率，因为进行模式匹配的字段由整个报文缩小为特定的协议参数，可使特征写的更加精确，减少误识别率。

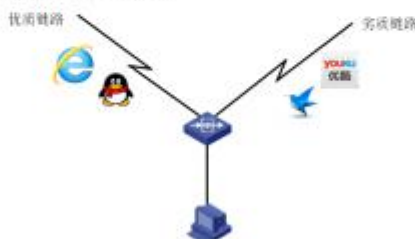


行为检测：不同的应用类型体现在会话连接或数据流上的状态各有不同：基于这一系列流量的行为特征，通过分析会话连接流的包长、连接速率、发送/接收的流量比例、包与包之间的间隔等信息来识别应用类型。

只有在准确识别应用协议的基础上，才能对应用做到深入、全面和准确地控制。不但可以准确、高效的识别出网络流量的应用类型，而且可以精准地识别出应用的行为。随着特征库的

不断更新，支持的应用和行为在不断增加。网络中的应用日新月异，拥有强大的安全服务团队的支持，可以随时对网络中的新应用进行跟踪分析，持续的更新应用特征库。

应用策略：通过配置策略路由，可以实现基于应用的路由选择。在用户有多条链路的情况下，不同的应用分别使用不同的线路，使办公、游戏等重要应用的流量使用链路状态较好的线路，使 P2P、视频等流量走链路状态较差的线路，帮助用户合理的分配链路资源，即保证重要业务的使用，也不影响 P2P、视频等的使用。



基于应用的流量管理基于应用的带宽分配，帮助用户更好的限制 P2P、视频等占用带宽比较高的业务，保障重要业务的运行。

精准的应用控制策略，随着网络应用的日新月异，应用精准控制的需求愈发强烈，提供精准的应用控制功能，应用控制粒度集中体现了应用的识别能力。系统内置的应用对象精细化到应用具体的动作，管理员可以根据网络需要针对应用实现网路允许和网络阻断。相关行为可以触发对应的日志记录。针对邮件发送支持针对发件人和收件人支持黑白名单控制；针对邮件标题和邮件内容支持关键字过滤；针对邮件整体大小支持管理员自定义大小，范围支持 0-100M；针对附件个数同样可以控制，范围支持 0-100 个。相关邮件行为可以触发对应的日志记录。关于 Web 关键字控制主要覆盖三种常见场景：搜索引擎；HTTP 上传；网页内容。以上场景全部支持。功能实现所见即所得。配置更加清晰。

ACG1000 系列行为管理设备基于应用识别的基础可以实现应用中相关内容的审计，记录。常见的审计内容包括电子邮件类、即时通讯类、网络论坛类、博客类、网购类、微博类等应用。ACG1000 行为管理设备通过用户上网的流量解析，将上述应用的交付内容和关键信息全部采集下来，例如 QQ 号、上下线时间、论坛发帖内容、网购搜索内容等。

协议类识别：当始识别流量时，会首先对流量进行高层协议分析，除了基本的 TCP/UDP 协议，还支持 HTTP、FTP、SMTP、POP3、IMAP 等 20 多种协议解析，对于不同的协议可以分析

出不同的信息。例如获取报文的 IP 地址、端口号，对于 HTTP 协议，可以获取请求的 URL，请求头部的 Cookie 字段信息等。此时，对于 SSL 加密流量，在识别前需要进行 SSL 解密工作。

进行流量的识别分析，对于流量会进行进一步的分析，主要手段有 DPI（深度报文检测）和 DFI（深度流检测）两种。其中 DPI 方面主要是进行 Payload 的扫描识别，通过 AC 算法、正则匹配等多种方法对静态报文进行内容解析，提取报文中的关键字或其他需要的信息；而 DFI 方面，提供跨报文识别的解决方案（例如依据包长序列识别迅雷）和流量关联识别（例如通过 FTP 控制通道关联数据通道）。

当完成应用识别工作以后，基于不同的应用类型去匹配应用特征库，使用各类技术手段对获取的信息进行解码和还原，从而能够获取到关键信息的明文，并将审计结果存储到数据库中。

关键信息审计，近年来，一方面随着国家为了净化互联网环境，逐步建立对互联网行业发证的规范，监管力度不断增强，另一方面，组织出于自身信息安全保护的需求如防止信息资产泄密，预防舆论风险，保留安全事件的相关证据，以及管理上的要求，如考核员工的网络工作效率、分析网络应用情况、提供管理依据等，对于行为记录方案的需求日益明确。

内网用户的所有上网行为能够记录以满足公安部 82 号令的要求。针对不同用户（组）进行差异化的行为记录和审计，包括网页访问行为、网络发帖、邮件 Email、IM 聊天内容、文件传输、游戏行为、炒股行为、在线影音、P2P 下载等行为，并且包含该行为的详细信息等。

近年来信息防泄密方案备受组织管理员关注，内网员工无意或有意将组织机密信息泄露到互联网甚至竞争对手，或向论坛 BBS 发布不负责的言论、网络造谣等，将给组织带来泄密和法律风险。不仅能基于关键字过滤、记录员工通过 Mail（包括 Webmail）、BBS、Blog、QQ 空间等发布的网络言论，还有日志记录功能。

对于使用 HTTP、FTP、mail 等方式传送文件所引发的风险，首先可以禁止用户使用 HTTP、FTP 上传下载指定类型的文件，对于上传的文件，也可以全面记录文件内容，做到有据可查。而外发 Email 潜在的泄密风险通过邮件延迟审计（Postponed Sending after Audit，PSA）技术，根据管理员预设条件，将潜在的泄密邮件先拦截，经人工审核后再发送，保障组织信息资产安全。但存心的泄密者通常会更改文件后缀名、删除后缀名、压缩、加密等，再通过 Email 外发、或通过 HTTP、FTP 上传，对以上行为同样可以识别并实时记录审计日志。

在移动互联网的兴起下，移动 APP 的使用已经越来越普遍，因此，公共社交类移动应用将成为发布不实言论、造谣诽谤等的重灾区。针对移动端的新闻评论类（腾讯新闻、网易新闻、新浪新闻等）、微博（新浪微博等）、论坛类（百度贴吧、天涯社区、新浪论坛、搜狐社区

等) APP 进行内容审计, 保护移动互联网时代的网络内容安全。



终端识别: 供以终端识别引擎为核心的安全策略、行为审计、来宾访问、日志分析四大功能。核心思想是帮助 IT 管理员使整个网络易用、安全。IT 管理员可以从用户、设备、应用、行为等多个视角来管理网络。端识别引擎是主要提供用户身份验证、和终端、系统类型识别的功能。当员工携带自己的设备连接到公司的网络之后, 不需要安装任何客户端, 只需要打开浏览器, 就可以轻松的完成用户身份认证, 并获得相应的授权, 这样不仅可以减少 IT 管理员的负担, 最重要的是, 简化了操作, 提高了员工使用自带设备的积极性。在不安装任何客户端软件的情况下, 通过身份识别引擎的设备分析模块, IT 管理员可以看到员工加入的网络中的设备的操作系统、硬件类型和生产厂商。

识别用户系统、终端的方式有两种: 通过 Web 访问的 User Agent 域来识别终端类型。

```
GET / HTTP/1.1
Host: www.baidu.com
User-Agent: Mozilla/5.0 (iPhone; U; CPU iPhone OS 4_3_3 like Mac OS X; zh-cn)
AppletVersion/3.1.2 (KHTML, like Gecko) Version/5.0.2 Mobile/8J2 Safari/
6533.82
Accept: application/xml,application/xhtml+xml,text/html;q=0.9,text/
plain;q=0.8,image/png,*/*;q=0.5
Accept-Language: zh-cn
Accept-Encoding: gzip, deflate
Cookie: Hm_lvt_e8499b7329e8d5d44f3f4c8902bb043a=1372659521;
```

通过移动应用来识别。比如在应用的流量中发现了来自淘宝网(iOS)客户端的流量，那么会通过这些流量判断用户的设备类型为 iOS。

来宾访问当有访客携带自己的智能手机/平板电脑尝试加入到公司网络中，这些访客可以使用来宾访问的功能。不需要通过复杂的验证，不用安装客户端，就可以正常的连接到网络中。

受限的访问控制，确保公司内部资料不会被泄露。

支持上网行为审计，如有需要，可以对来宾开启网络行为控制。

日志分析，所有的系统日志中都会记录有系统、终端类型。这些信息可以有效的帮助 IT 管理员评估网络状况。

随着 WEB2.0 技术的蓬勃发展和动态端口的新应用层出不穷，使得传统网关产品采用五元组的访问控制方式早已变得力不从心，基于 7 元组以及时间和终端维度的访问控制策略，能有效的控制自然人、应用的访问控制。管理员只需要通过一条策略便可完成对源接口、源地址、用户、目的接口、目的地址、应用、服务、时间、终端类型等维度的匹配，并针对入侵防御、病毒防护、应用过滤、URL 过滤、终端公告提醒等进行统一管控，使用方便，维护简单。



内置千万级 URL 库和丰富的应用识别库，涵盖即时通讯、P2P 软件、网络游戏、电子商务、办公软件等 29 类主流应用类型。

最新应用分类：

即时通讯

P2P 软件

P2P 流媒体

其他流媒体

金融登录

金融行情

金融交易

网络游戏

文件传输

云端存储

搜索引擎

网络社区

微博

门户网站

数据库

电子商务

网上银行

网络协议

电子邮件

远程控制

木马控制

生活服务

招聘咨询

文学咨询

网络代理

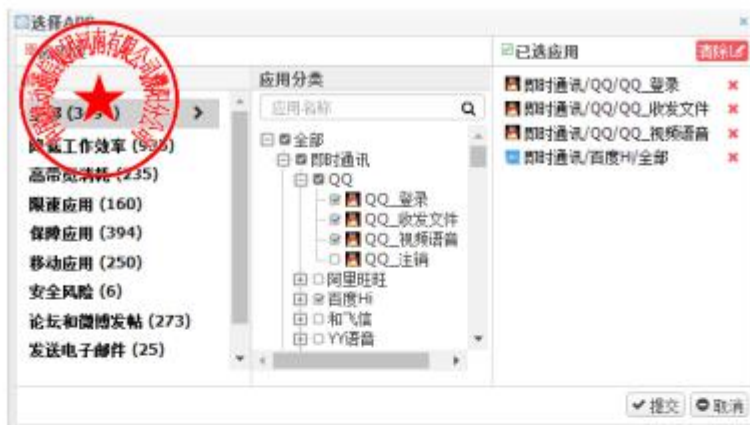
办公软件

软件更新

P2P 信贷

其他类

通过对数据包的深入解析，精细化获取应用及应用的相关行为，完成网络实时应用和系统应用的应用指纹匹配。此外针对应用指纹模糊的应用，系统通过管理分析应用的行为轨迹，通过应用行为完成指纹模糊应用的精准识别。依附引擎对应用的精准识别实现应用的精细化控制。并完成相关应用的日志记录。精细化应用分类和应用行为通过层次结构分明的树形结构完成展示，供管理员用户策略引用。



传统的应用控制之外，针对邮件控制、Web 关键字控制、虚拟账号控制同样完成精细化、标准化的梳理。

针对邮件的精细化控制从如下角度完成标准化：

发件人

收件人

邮件标题和内容

邮件大小

邮件附件个数

全维度覆盖邮件的所有模块，针对发件人和收件支持黑名单或者白名单的便捷控制，满足各种控制需求。



Web 关键控制主要解决市场常见的信息泄露、行为审计、舆论评论等相关问题。ACG1000 采用深度分析引擎和 SSL 解密引擎完成对加密和非加密数据的深度分析。



虚拟账号控制虽然是行为管理的小众场景，但是随着网络时代的发展及国家针对行业的规范化。虚拟账号作为用户身份的标识需求也越发重要，虚拟账号作为用户的标识同样需要精细化控制。



URL 策略管控，是通过 URL 分类库，对网站访问进行过滤。让用户通过网站分类的选择，轻松控制网站访问。同样，URL 过滤也依附于安全策略。可以减少了对数据包的过滤范围，并记录访问网站及 URL。



流量管理：随着网络应用越发复杂，网络带宽管理需要更精细的管理。4 级流控概念，可将物理线路划分为若干虚拟线路和流控通道，支持基于用户/组、应用/组、服务、源地址等七元组的方式实现带宽管理细化，满足用户各种带宽管理的需求。

弹性带宽管理，可以使空闲通道不占用大量带宽，减少带宽的浪费，减少因空闲通道占用带宽，流量达到极限出现丢包现象。弹性带宽就是为了解决带宽浪费的问题，空闲通道会自动让出部分带宽给繁忙的通道。一旦空闲通道带宽不足时，将自动抢占回借用出去的带宽。此特

性避免了带宽浪费，实现价值最大化。

每 IP 用户限速：为了自动均分带宽，当在某个通道中只有一个用户使用时，该用户可以使用全部带宽。如果有更多用户使用该通道时，管理员可设置将带宽按 IP 数量或用户数量均分，提升用户上网体验。

防私接路由，上网用户私接 WiFi 或路由器行为会造成无法校验用户身份、安全性能难以保障、占用额外带宽资源等问题。能够快速识别“一拖 N”的网络私接行为，精准定位“N”即私接用户数量，并进行有效的管控；及时发现非法热点预防个人用户私接路由，拒绝未知网络终端节点，保护运营商利益；同时支持同步和展示认证用户信息，支持同步 PPPoE 账号等认证服务器账号信息。让整个网络拓扑清晰可控，有效预防数据泄露的安全风险；极大的降低了管理员网络维护的工作量。



安全管理，可对当前设备的会话进行监控，管理员可查看会话的发起用户、源目地址、端口、协议、策略、存在时间和超时时间等，具有完备的状态检测表追踪连接会话状态；ACG1000 支持对当前所有会话进行峰值统计，方便管理员快速筛选内网异常用户和 IP，可帮助管理快速定位网络故障；管理员支持针对全局基于 IP 进行并发会话和新建会话的限制，保障内网所有访问行为均在正常数值范围内，确保内网安全。

攻击防护，当受到攻击时，伴随而来的会出现网络异常情形发生，网络异常大概可分为以下三种：

通信协议异常

例如由外界网络流入大量过长的 IP 数据包、大量的 IP 碎片数据包、异常的 TCP 通信协议连机状态、被截断的 IP 数据包、无法重组的 IP 数据包等。

IP/Port 的扫描异常

通过 IP 扫描，黑客可以窥知目的端内网络结构和情形；通过 Port 扫描，黑客可以得知目标主机已启用的端口。

网络流量异常

例如突然产生大量的 TCP SYN、TCP、UDP、ICMP、IGMP 等数据包，占据正常网络使用带宽。

当上述攻击数据包发起时，经过改造的恶意数据包可能会造成企业内部网络系统死机无法对外提供正常的服务；IP/Port 扫描的行为将让企业内部的网络架构轻易被黑客得知；大量的异常流量数据包也可能造成企业路由器、交换机等因承载过重而死机。

内置异常包攻击防御模块，可以检测各项偏离预期的网络行为。依据 RFC 标准规范制作通信协议异常检测模块，可以阻止不符合标准通信协议规范的数据包。支持网络流量异常检测，不单只使用计数的方式，还使用专门的统计算法，可以准确地检测网络流量的异常情形。

支持 ARP 防欺骗、支持 IP、MAC 地址绑定。

支持 ARP Flood 攻击防护、支持基于接口的 ARP 学习控制。

支持 Ping of Death、Land-Base、Tear Drop、TCP flag、Winnuke、Smurf、IP 选项、IP Spoof、Jolt2 等异常包攻击的防御。

支持基于 IPv6 的 Winnuke、Land-Base、TCP flag、Fraggle、IP Spoof 等异常包攻击的防御。

支持基于接口的端口扫描防护和 IP 扫描防护。

支持 SYN flood、UDP flood、ICMP flood、DNS flood 攻击防护，支持自定义阈值。

统计报表，支持实时的数据统计功能，对用户网络行为进行记录与分析。对于日志的留存与分析，即是对国家法律法规的遵从，也是有效利用网络资源的需要。针对用户上网行为以及相关内容的查询统计，能够对用户的网络活动进行较长时间的回溯与反查，全面了解网络的使用情况，为改进网络管理提供详实准确的依据。

内置多套用户行为管理统计汇总模板。管理员可以根据时间维度，全方位查询统计用户、应用等相关上网行为数据。其内容涵盖用户上网行为次数统计、邮件审计统计、IM 审计统计、关键字排名统计、恶意 URL 统计等相关数据统计。为管理员用户提供不同角度的统计报告。提供报表订阅功能，系统内置多套不同的报表模板，且管理员可以根据需求自定义报表内容，为不同行业用户提供最大程度的满足。系统内置的报表订阅功能支持以天、周、月以及自定义时间范围等多种时间维度的报表统计。统计生成之后的报表支持通过邮箱，ftp 等多种方式发送

和上传到第三方。设备针对历史报表也预留一定的存储空间。从而保证报表数据不会因为外置设备异常导致数据丢失。

12.1.5.5 备份机制

现有电子政务外网通过交换机对接，在交换机对应端口进行链路聚合配置，路由器和 IP 路由器采用动态路由协议实现路由选路。采用交换机端口聚合、链路自动保护倒换等技术手段完成故障保护倒换和业务切割。链路聚合、倒换时不影响业务的正常使用。

12.1.5.7 技术功能场景

12.1.5.7.1 IPv6

随着 5G、物联网、智慧城市等创新业务的逐步应用，海量电子政务固定、移动接入端和物联网终端对 IP 地址需求量巨大，原 IPv4 有限的地址段将无法满足实际需求，急需升级为地址数更多的 IPv6 网络。建设基于 IPv6 的电子政务外网，成为必然，需要为 5G、数据中心等新型基础设施建设奠定基础，更为未来发展大规模的物联网、工业互联网开拓网络空间，搭建基础环境。

根据《推进互联网协议第六版（IPv6）规模部署行动计划》要求，政府网站、骨干网、城域网、接入网逐渐实现 IPv6 的规模部署，网络、应用、终端全面支持 IPv6，全面完成向下一代互联网的平滑演进升级，形成全球领先的下一代互联网技术产业体系，同样意味着新一代的电子政务外网必然通过 IPv6 协议承载业务。

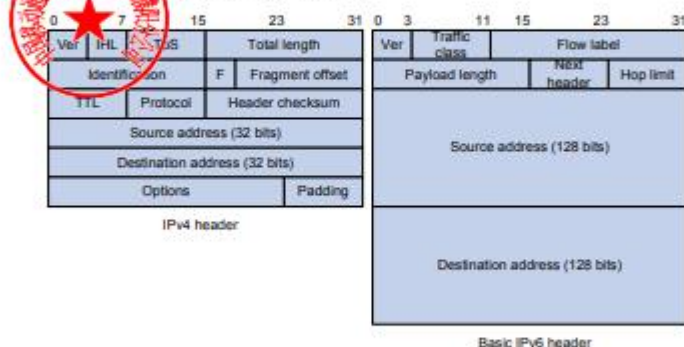
IPv6 技术价值

IPv6（Internet Protocol Version 6，互联网协议版本 6）是网络层协议的第二代标准协议，也被称为 IPng（IP Next Generation，下一代互联网协议），它是 IETF（Internet Engineering Task Force，互联网工程任务组）设计的一套规范，是 IPv4 的升级版本。IPv6 和 IPv4 之间最显著的区别为：IP 地址的长度从 32 比特增加到 128 比特。

（1）简化的报文头格式

通过将 IPv4 报文头中的某些字段裁减或移入到扩展报文头，减小了 IPv6 基本报文头的长度。IPv6 使用固定长度的基本报文头，从而简化了转发设备对 IPv6 报文的处理，提高了转发

效率。尽管 IPv6 地址长度是 IPv4 地址长度的四倍，但 IPv6 基本报文头的长度只有 40 字节，为 IPv4 报文头长度（包括选项字段）的两倍。



图：IPv4 报文头和 IPv6 基本报文头格式比较

（2）充足的地址空间

IPv6 的源地址与目的地址长度都是 128 比特（16 字节）。它可以提供超过 3.4×10^{38} 种可能的地址空间，完全可以满足多层次的地址划分需要，以及公有网络和机构内部私有网络的地址分配。

（3）层次化的地址结构

IPv6 的地址空间采用了层次化的地址结构，有利于路由快速查找，同时可以借助路由聚合，有效减少 IPv6 路由表占用的系统资源。

（4）地址自动配置

为了简化主机配置，IPv6 支持有状态地址配置和无状态地址配置：

有状态地址配置是指从服务器（如 DHCPv6 服务器）获取 IPv6 地址及相关信息；无状态地址配置是指主机根据自己的链路层地址及路由器发布的前缀信息自动配置 IPv6 地址及相关信息。

同时，主机也可根据自己的链路层地址及默认前缀（FE80::/10）形成链路本地地址，实现与本链路上其他主机的通信。

（5）内置安全性

IPv6 将 IPsec 作为它的标准扩展头，可以提供端到端的安全特性。这一特性也为解决网络安全问题提供了标准，并提高了不同 IPv6 应用之间的互操作性。

(6) 支持 QoS

IPv6 报头中的流标签 (Flow Label) 字段实现流量的标识, 允许设备对某一流中的报文进行识别并区别对待。

(7) 邻居发现机制

IPv6 的邻居发现协议是通过一组 ICMPv6 (Internet Control Message Protocol for IPv6, IPv6 互联网控制消息协议) 消息实现的, 管理着邻居节点间 (即同一链路上的节点) 信息的交互。它代替了 ARP (Address Resolution Protocol, 地址解析协议)、ICMPv4 路由器发现和 ICMPv4 重定向消息, 并提供了一系列其他功能。

(8) 灵活的扩展报文头

IPv6 取消了 IPv4 报文头中的选项字段, 并引入了多种扩展报文头, 在提高处理效率的同时还大大增强了 IPv6 的灵活性, 为 IP 协议提供了良好的扩展能力。IPv4 报文头中的选项字段最多只有 40 字节, 而 IPv6 扩展报文头的大小只受到 IPv6 报文大小的限制。

IPv6 技术介绍

1、IPv6 地址类型

IPv6 主要有三种类型的地址: 单播地址、组播地址和任播地址。

单播地址: 用来唯一标识一个接口, 类似于 IPv4 的单播地址。发送到单播地址的数据报文将被传送给此地址所标识的接口。

组播地址: 用来标识一组接口 (通常这组接口属于不同的节点), 类似于 IPv4 的组播地址。发送到组播地址的数据报文被传送给此地址所标识的所有接口。

任播地址: 用来标识一组接口 (通常这组接口属于不同的节点)。发送到任播地址的数据报文被传送给此地址所标识的一组接口中距离源节点最近 (根据使用的路由协议进行度量) 的一个接口。

IPv6 中没有广播地址, 广播地址的功能通过组播地址来实现。

IPv6 地址类型是由地址前面几位 (称为格式前缀) 来指定的, 主要地址类型与格式前缀的对应关系如下表所示。

地址类型		格式前缀 (二进制)		IPv6 前缀标识
单播地址	未指定地址	00...0	(128 bits)	::/128
	环回地址	00...1	(128 bits)	::1/128

地址类型	格式前缀（二进制）	IPv6 前缀标识
链路本地地址	1111111010	FE80::/10
全球单播地址	其他形式	-
组播地址	11111111	FF00::/8

2、IPv6 地址分配方法

IPv6 全球单播地址可以通过下面几种方式配置：

手工配置：用户手工配置 IPv6 全球单播地址。

采用 EUI-64 格式形成：当配置采用 EUI-64 格式形成 IPv6 地址接口的 IPv6 地址的前缀需要手工配置，而接口 ID 则由接口自动生成。

引用前缀生成 IPv6 地址：引用前缀生成 IPv6 地址时，接口的 IPv6 地址的前缀可以通过手工配置或 DHCPv6 动态获取，同时该前缀还会分配给终端设备。

无状态自动配置：根据接收到的 RA 报文中携带的地址前缀信息，自动生成 IPv6 全球单播地址。

	手工静态配置	有状态 DHCPv6	SLAAC EUI-64	SLAAC Privacy	无状态 DHCPv6
适用场景	网络地址（链路互联地址、设备 loopback）、服务器地址	对终端访问行为有强管控需求。例如园区生产/办公终端。	针对物联终端、无强管控需求或较分散的终端。例如视频监控、小规模站点网络等	针对客户端应用（例如浏览器）的临时地址	结合 SLAAC 和 DHCPv6，通过 SLAAC 分配地址前缀，通过 DHCPv6 分配 DNS 和其他 option

P refi 要求	无要 求、自定义	/64	/64	/64
-----------------	-------------	-----	-----	-----

12.1.5.7.2 SDN

数字化应用的落地，需要网络满足业务高效灵活部署的需求。SDN（Software Defined Network），软件定义网络，通过 SDN 控制器对网络设备的统一纳管，实现业务快速部署、重要业务的管控保障、资源深度可视功能，提升网络运维效率。通过 AI 及大数据分析，使网络具备故障快速识别，问题快速定位的能力，并能结合分析结果提供网络趋势预测，给出专家级优化建议，全面提升网络的智能化水平。

SDN 技术价值

SDN 技术主要的优势体现在：

（1）统一管理，提升网络运维效率及资源利用率

通过 SDN 控制器对全域网络设备的统一纳管，实现网络自动化，提升业务部署效率；对业务需求进行统一编排，使网络资源可以基于全局视角统筹分配，提高利用率；为运维人员提供多维可视能力，使网络运行状态一览无余，提升网络智能运维的能力。

（2）智能随行，提升网络主动运维能力

通过 SDN 控制器对业务质量信息（网络流量、状态、关联事件及告警信息等）进行周期性采样、深度分析，实现网络质量可视和故障快速定位的能力。结合数字孪生技术，将物理网络在虚拟空间中模拟，实现业务仿真及风险预测，做到提前规划提前预防，全面提升网络主动运维的能力。

类别	传统广域网	SDN 广域网
网络质量监控	模拟检测（PING、Tracert、TWAMP 等）	随流检测（iFit）
突发拥塞	报障后人工调整	自动发现、自动调整

类别	传统广域网	SDN 广域网
高价值业务	保证优先转发	保证业务 SLA（如带宽、时延），选择最优路径
链路利用率	无法保证	通过流量调整保证链路负载均衡
转发控制	基于路由控制	逐跳可控

SDN 技术介绍

流量调优架构由控制器和电子政务外网基础网络两部分组成。其中控制器设计包括：

1、拓扑收集：AD-WAN 控制器与路由器设备之间建立 BGP-LS 连接，通过 BGP-LS 协议，自动收集网络的拓扑信息。

2、信息采集：AD-WAN 控制器通过 snmp 或 netconf 采集设备信息，通过 netconf 或 telemetry 周期性采集接口流量、业务流量以及隧道流量，通过 NQA 或 TWAMP 技术探测链路质量（时延、抖动、丢包率）等信息，并周期性进行质量信息上报，以便控制器即时感知网络流量和质量信息。

3、调优策略：AD-WAN 控制器配置业务 SLA 策略，对业务进行基于带宽、质量等信息调优，保证网络带宽得到合理利用。

4、隧道下发：AD-WAN 控制器基于业务定义和业务应用网络范围通过 netconf 或 BGP SRv6 Policy 将隧道下发给首节点设备生成 SRv6 TE Policy 隧道。

5、调优算路：SDN 控制器根据业务 SLA 策略进行算路，当链路带宽或质量不能满足业务 SLA 要求时，通过控制器进行重新算路调整。

6、路径下发：控制器通过 netconf 或 BGP SRv6 Policy 向设备下发隧道新路径。

SDN 控制器与设备之间需要设计多种协议通信，具体通信协议设计如下表所示。

部件角色	接口类型	功能说明	部署说明
------	------	------	------

部件角色	接口类型	功能说明	部署说明
SDN 控制器 <—> 路由器	BGP-LS	通过 BGP-LS 从设备收集拓扑信息。	控制器与 ABR 设备建立 BGP-LS 邻居，收集域内拓扑。
	NETCONF	向设备下发与业务相关的配置信息。	控制器与每台网络设备建立 NETCONF 连接。设备先配置 NETCONF 的基础配置，控制器上指定连接设备的 IP 和 NETCONF 用户名、密码等配置，NETCONF 连接在设备上线时自动建立。
	BGP SRv6 Policy	用于 SRv6 隧道建立和 segment list 路径下发。	与业务所在源节点设备建立 BGP SRv6 Policy 连接，存在全网 RR 设备时也可直接与 RR 建立 BGP SRv6 policy 连接。
	SNMP	采集设备信息、接收设备告警和 trap 信息。	和每台设备建立 SNMP 连接。
	Telemetry	采集设备、端口、链路、隧道的流量性能数据等	和每台设备建立 Telemetry 连接。

12.1.5.7.3 EVPN

EVPN (Ethernet Virtual Private Network) 是下一代全业务承载的 VPN 解决方案。EVPN 统一了各种 VPN 业务的控制面，利用 BGP 扩展协议来传递二层或三层的可达性信息，实现转发面和控制面的分离。

EVPN 技术价值

EVPN 有如下技术优势：

- (1) 减少组网压力，提升网络规模

对于大型 VPLS 网络，MAC 地址变化或故障切换，都需要重新泛洪学习，收敛性能差。EVPN 将 MAC 的传递和路由传递一样处理受控学习，减轻整网泛洪的学习压力，提升学习性能。同时 EVPN 支持路由反射器，所有 PE 和反射器建立邻居关系，通过路由反射器来反射 EVPN 路由，大大降低网络复杂度，从而提升 L2VPN 规模部署压力。

(2) 双活负载分担，提升链路利用率

传统 VPLS，为了避免 CE 侧到 PE 侧产生环路，CE 到 PE 侧只支持单活模式，不支持冗余，导致链路利用率低。EVPN 支持负载分担，可以合理提供网络资源，减少网络拥塞。

(3) 简化控制，现网兼容

EVPN 可以支持 L2VPN 和 L3VPN 业务控制，可以做到控制平面简化归一。同时 EVPN 配合 SRv6 的转发面简化，实现网络极简。后续业务如有 L2VPN 需要，只需简单配置 EVPN 配置，即可简易开通。

同时 EVPN 使用和 MP-BGP 不同的 address family，路由天然隔离，简化网络路由规划，有利于网络平滑过渡。

EVPN 技术介绍

为了支持 EVPN，MP-BGP 在 L2VPN 地址族下定义了新的子地址族——EVPN 地址族，并新增了如下 EVPN NLRI (Network Layer Reachability Information，网络层可达性信息)，即 EVPN 路由：

Ethernet Auto-discovery Route：以太网自动发现路由，能够用来在站点多归属组网中通告 ES 信息和 service ID 信息，也能够用来在 EVPN VPWS 组网中通告 service ID 信息。

MAC/IP Advertisement Route：MAC/IP 发布路由，用来通告 MAC 地址和主机路由信息（即 ARP 信息和 ND 信息）。

Inclusive Multicast Ethernet Tag Route：包含性组播以太网标签路由，又称为 IMET 路由。在 EVPN VXLAN 组网中用来通告 VTEP 及其所属 VXLAN 信息，以实现自动发现 VTEP、自动建立 VXLAN 隧道和自动关联 VXLAN 与 VXLAN 隧道；在 EVPN VPLS 组网中用来通告 PE 信息，实现 PE 的自动发现、自动建立 PW。

Ethernet Segment Route：以太网段路由，用来通告 ES 及其连接的 VTEP 或 PE 信息。

IP Prefix advertisement route：IP 前缀路由，用来以 IP 前缀的形式通告 BGP IPv4 单播路由或 BGP IPv6 单播路由。

EVPN 路由中包含 RD (Route Distinguisher，路由标识符) 字段，用来区分 VSI 或交叉连

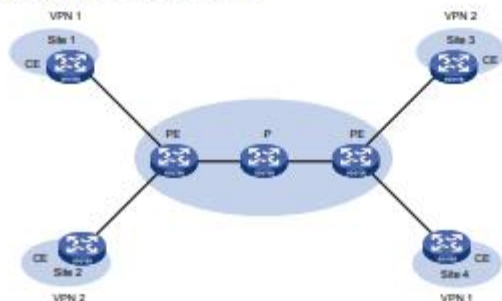
接组的 EVPN 路由, 以免 EVPN 路由冲突。

VTEP 在发布 VPN 路由时, 会携带 VPN Target 扩展团体属性(也称为 Route Target)。VPN target 属性定义了本地发送的 EVPN 路由可以为哪些 VTEP 或 PE 所接收, VTEP 或 PE 可以接收哪些远端 VTEP 或 PE 发送来的 EVPN 路由。MP-BGP 通过 VPN Target 属性来控制 EVPN 路由信息的发布与接收。

VPN target 属性分为以下两种, 每一种都可以包括多个属性值:

Export target 属性: 本地 VTEP 或 PE 在通过 BGP 的 Update 消息将 EVPN 路由发送给远端 VTEP 或 PE 时, 将 Update 消息中携带的 VPN target 属性设置为 Export target。

Import target 属性: VTEP 或 PE 收到其它 VTEP 或 PE 发布的 Update 消息时, 将消息中携带的 VPN target 属性与本地配置的 Import target 属性进行比较, 只有二者中存在相同的属性值时, 才会接收该消息中的 EVPN 路由。



下面以在 EVPN L3VPN 组网为例, 描述 VPN 路由的传递过程。VPN 路由信息的发布涉及 CE 和 PE。P 路由器只维护骨干网的路由, 不需要了解任何 VPN 路由信息。PE 路由器只维护与它直接相连的 VPN 的路由信息, 不维护所有 VPN 路由。

(1) 本地 CE 到入口 PE 的路由信息交换

CE 使用静态路由、RIP、OSPF、IS-IS、EBGP 或 IBGP, 将本站点的 VPN 路由发布给 PE。CE 发布给 PE 的是标准的 IPv4 或 IPv6 路由。

(2) 入口 PE 到出口 PE 的路由信息交换

PE 从 CE 学到 VPN 路由信息后, 将其存放到相应的 VPN 实例的路由表中。PE 为这些标准 IPv4 或 IPv6 路由增加 RD 和 Export Target 属性, 并为这些路由分配 MPLS 私网标签, 形成 EVPN 的 IP 前缀路由(包括 RD、Export Target 属性和 MPLS 私网标签)发布给出口 PE。出口 PE 将

IP 前缀路由的 Export Target 属性与自己维护的 VPN 实例的 Import Target 属性进行匹配。如果出口 IP 前缀路由的 Import Target 属性与路由的 Export Target 属性中存在相同的属性值，则将该 IP 前缀路由并将其添加到 VPN 路由表中。

(3) 出口 PE 到远端 CE 的路由信息交换

与本地 CE 到入口 PE 的路由信息交换相同，远端 CE 可以通过多种方式从出口 PE 学习 VPN 路由，包括静态路由、RIP、OSPF、IS-IS、EBGP 和 IBGP。

12.1.5.7.4 网络切片

近年来，随着云计算、大数据、物联网等新业务的兴起，人们对 IP 网络的诉求从关注带宽逐渐转移到业务体验、服务质量和组网效率层面，网络切片技术的产生有效解决了上述诉求。

网络切片技术实现数据转发面的隔离，使各个业务独立转发，以此满足不同业务对带宽、时延等的需求。

网络切片技术价值

(1) 业务资源隔离，互不相互抢占

网络切片能够为不同业务切分出不同的逻辑网络切片，不同的网络切片间带宽相互隔离，互不相互抢占。例如通过硬件切片技术为共享数据交换业务和视频业务在同一物理线路上分配不同的业务通道，即使在共享数据交换业务出现流量拥塞时，也不会影响视频业务的体验。

(2) 层次化网络规划，资源有效利用

传统的带宽保障通过 QoS 方式预留，如果要绝对保障高优业务时，会出现低优业务“饿死”无资源可用的情况，导致低优业务无法正常运行。

网络切片技术支持 1M-5G 不同粒度的切片粒度，为不同类业务，不同优先级创建不同颗粒度切片，规划不同带宽，满足各类业务并行共存，安全稳定运行，有效提升资源利用率。

(3) 简化带宽保障配置，切片独立运维

通过和控制器配合，网络切片可以通过控制器可视化管理，包括网络切片的创建，删除，带宽调整，路径编排等。同时，通过物理硬切片，可以实现切片间的运维独立，提升运维效率。

网络切片技术介绍

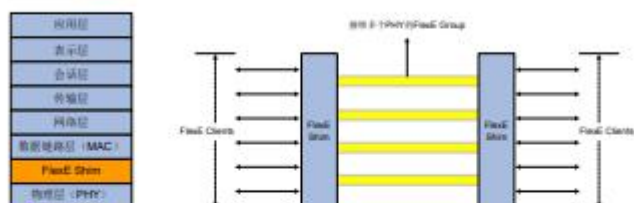
网络切片技术分为两个层面，一个是设备上的资源保障隔离技术，

1、资源隔离技术原理

当前网络切片的资源隔离技术包括物理层的 FlexE 切片和资源层的子接口切片。

灵活以太网 (FlexE)

灵活以太网 (Flexible Ethernet, 简称 FlexE) 技术是在现有 802.3 高速以太接口架构的基础上, 将 MAC 和 PHY 层解耦, 以获取灵活速率的以太接口, 实现的低成本、高可靠、可动态灵活配置的网络接口技术。



根据 FlexE 的 MAC/PHY 解耦的技术特点, FlexE 可提供三种主要功能:

1) 子速率。基于 IEEE 802.3 标准物理接口的子速率是指一个低速率的数据流共享一个 PHY 或多个 PHY。例如, 在 2 个 100G 速率的物理接口上仅仅承载 50G 的 MAC 层速率。

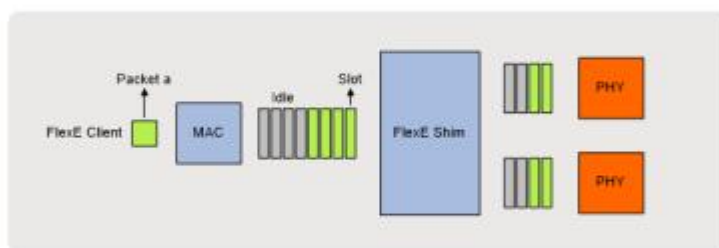


图 子速率功能示意图

2) 通道化。对基于 IEEE 802.3 标准的物理接口的通道化是指多个低速率数据流共享一个 PHY 或多个 PHY。例如, 在 1 个 100G 速率的物理接口上承载 25G 和 75G 两个 MAC 层速率的数据流。

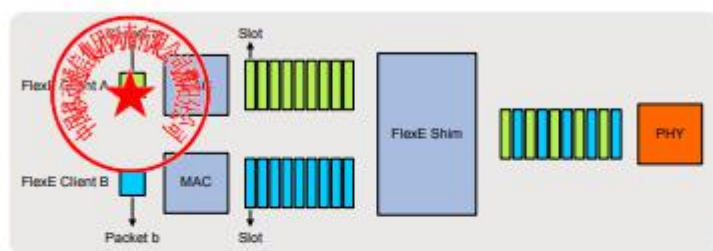


图 通道化功能示意图

3) 捆绑：FlexE支持捆绑多个IEEE 802.3标准的物理接口，使多个PHY一起工作，以支持更高速率。例如，将2个100G物理接口捆绑，实现200G的MAC层速率

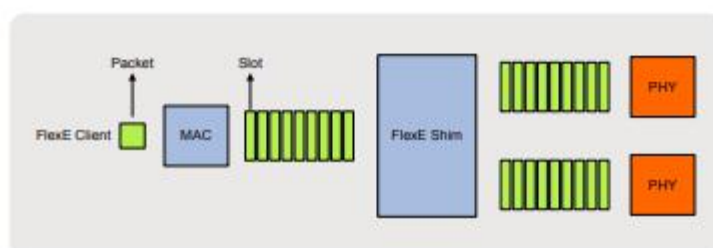


图 捆绑功能示意图

FlexE技术可以通过子速率特性实现带宽的硬管道隔离，针对重要业务按需分配专享带宽，达到保障业务的低时延，高质量，稳定运行；FlexE接口可以通过大带宽接口特性，实现更高速端口，满足未来业务扩展需要。

但是：当前FlexE存在一些待解决的问题，对网络部署存在较高要求，具体如下：

最小颗粒度为5G，和接入网络带宽需求不匹配。

最低适配接口带宽50G，端口和传输部署成本高。

任意速率的切片暂无标准，存在对接问题。

子接口切片

子接口切片是一种小粒度的切片技术，通过在高速率端口上创建子接口，并为某些子接口配置子接口切片带宽，就可以实现子接口切片功能。这些配置了子接口切片带宽的子接口称为切片子接口。切片子接口独享为其分配的带宽，并使用独立的队列进行调度。

子接口切片可以具备如下价值：

带宽独享，不被抢占。由于同一物理接口上不同切片子接口之间的带宽严格隔离，可以有效解决业务带宽被抢占问题，保障重要业务 SLA。

小颗粒度切片，部署要求低。子接口切片使用芯片队列和带宽预留技术，支持最小 M 级颗粒度，满足委办局的 M 级精细粒度带宽接入诉求。

资源隔离技术对比

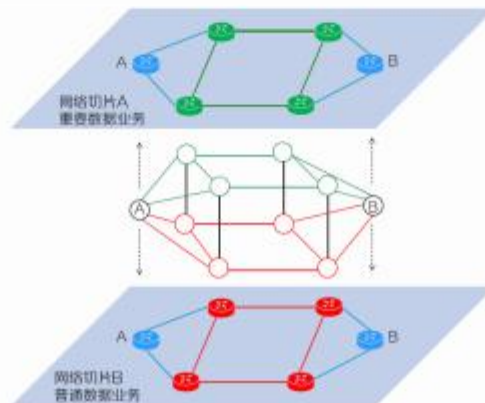
技术特点	子接口切片	FlexE
端口类型	GE、10GE、25GE、40GE、50GE、100GE	50GE、100GE
配置复杂程度	简单	中等
最小切片粒度	1Mbps	5Gbps：已商用 1Gbps：未标准化
的切片数量	千级	百级

2、平面隔离技术原理

网络切片是在一张物理网络上切分出多张包含特定网络功能，由定制网络拓扑和网络资源组成的虚拟网络，用于满足不同网络切片的业务功能需求和服务质量（SLA）保障。

基于亲和属性的网络切片

亲和属性，链路的一种属性，也称为链路颜色。用户根据自己业务需要，为接口或子接口配置亲和属性，相同亲和属性的接口或子接口组成一个逻辑拓扑，在同一拓扑内使用 Flex- Algo 灵活算法（如，链路开销，链路时延等），由此达到在一个物理网络上规划出不同逻辑拓扑的网络切片。同时可以将亲和属性资源隔离接口关联，那么这样就实现从拓扑层和资



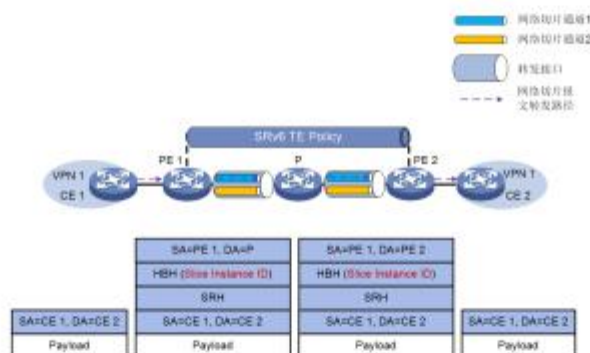
源层的拓扑统一，满足不同网络切片的业务功能需求和服务质量（SLA）保障。

如上所示，绿色路径时延低，资费较高；红色路径时延高，但资费更低。通过 Flex-Algo 算法的规划进行网络切片后，可以将从 A 到 B 的重要业务流量限制在绿色路径内，普通数据业务流量限制在红色路径内，实现了普通数据业务和重要业务的隔离，在保障业务质量的同时，节约了成本。

基于 Slice ID 的网络切片

在 SRv6 源节点，为报文头增加 IPv6 逐跳扩展头（Hop-by-Hop Extension Header），且在 IPv6 逐跳扩展头中添加网络切片实例 ID（Slice Instance ID）信息，中间设备根据网络切片实例 ID 查找资源出口。

转发流程如下所述：



在 SRv6 网络中存在网络切片实例 1 和网络切片实例 2。PE 1、P 和 PE 2 的转发接口上均存在分别与网络切片实例 1 和网络切片实例 2 关联的网络切片通道 1 和网络切片通道 2。VPN 1 中两个站点 CE 1 和 CE 2 之间的流量使用 SRv6 TE Policy 承载，SRv6 TE Policy 关联了网络切片实例 1。CE 1 访问 CE 2 的报文转发过程为：

(1) CE 1 向 PE 1 发送 IPv4 单播报文。PE 1 接收到 CE 1 发送的报文之后，查找 VPN 实例路由表，该路由的出接口为 SRv6 TE Policy。PE 1 为报文封装如下信息：

封装 SRH 头，在 SRH 头中携带 SRv6 TE Policy 的 SID List。

封装 HBH 扩展头，在 HBH 扩展头中携带 SRv6 TE Policy 关联的网络切片实例的 ID（Slice

Instance ID 字段置值为 1)。

封装 P 的基本报文。

(2) 中间 P 将报文转发给 P，转发时根据 Slice Instance ID 信息在出接口上查找与其对应的网络切片通道，并通过该通道转发报文。

(3) 中间 P 备根据 SRH 信息转发报文，转发时根据 Slice Instance ID 在出接口上查找与其对应的网络切片通道，并通过该通道转发报文。

平面隔离技术对比

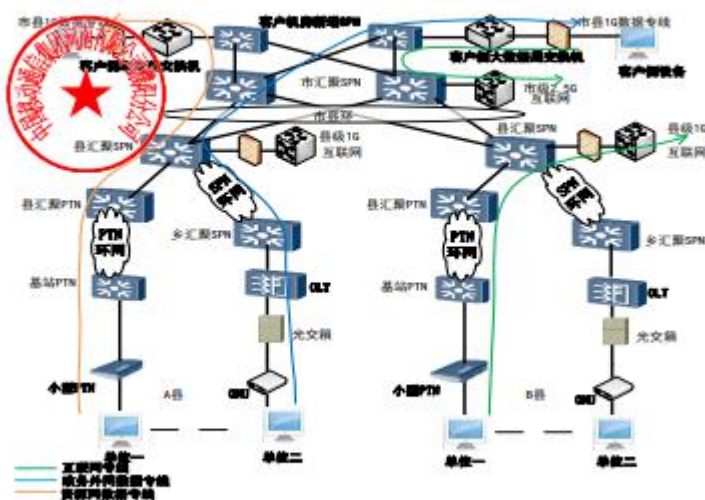
类型	亲和属性方案	Slice ID 方案
算法	支持按网络质量算路（如丢包时延抖动）	否
切片数量	少，128 个；控制面压力大	多，K 级；控制面压力小
节省 IP	否	是。基础接口配 IP，其他切片共用基础接口 IP
适用场景	组网型切片	专线型切片

12.1.5.8 网络接入方案

12.1.5.8.1 网络接入方案概述

本次濮阳市电子政务外网升级融合项目方案，濮阳移动采用汇聚层 SPN 组网方式、接入层根据需求采用 PTN 或 PON 网络进行建设，依托濮阳市移动公司丰富的网络资源，满足市政府“互联网+政务”发展需求，实现濮阳市电子政务外网融合立体全覆盖。

包含市直重点单位电子政务外网专线接入服务。



➤互联网接入线路

- 1) 采用光纤方式接入到移动核心城域网，且必须有完善可靠的冗余保护措施。
- 2) 互联网业务节点必须接入移动的 CMNET 骨干网。
- 3) 提供 GE、10GE 业务接口，具备提供 100~1000Mbps 和 N*1Gbps 带宽能力，且线路带宽能够平滑升级。

➤PON 专网线路

提供符合信息产业部颁布的《电信服务标准（试行）》的电信业务质量要求的线路质量，长期运行基本无瞬时中断现象，误码率在 $10E-8$ 以内的电信级线路：

线路性能要求：光纤用波长为 1310nm 进行测试时，损耗应小于 0.40dB/公里（包括接头损耗）；用波长为 1550nm 进行测试时，损耗应小于 0.25dB/公里。障碍历时不大于 6 小时。

➤提供与接入设备及线路相匹配的光模块，并明确光模块的品牌和型号。

➤安装线路时不能对现有业务网络造成影响，必须平滑过渡。

12.1.5.8.2市直重点单位网络建设方案

➤市直重点单位广域网设计

市直重点单位广域网路由节点通过 1000Mbps 数据专线向上连接到省核心区接入服务，

市级广域网路由节点提供接入本市内城域网核心路由节点，横向连接市级城域网。

广域网路由节点配置 8 个万兆接口（可兼容千兆），支持端口聚合和链路捆绑，提高可靠性。与市级城域网节点处于统一自治域内，目前县级政务外网主要采用三层平面路由技术或 MPLS VPN 技术建设。

对于采用三层平面路由技术构建的区级政务外网，采用三层路由模式与市级政务外网节点对接。市级政务外网的 PE 设备可通过 VPN 区分市级政务外网内不同业务系统的业务流量，从而实现县级用户对市级政务外网的访问。

对于采用 MPLS VPN 技术构建的市级政务外网，建议采用 OPTION A 的跨域对接方式，实现 VPN 业务的贯通，县级政务外网 PE 设备与市级政务外网 PE 设备之间的链路，可以采用基于 802.1Q 的不同 VLAN（Virtual Local Area Network，虚拟局域网）子接口方式，实现一条物理链路承载多个 VPN 业务。

政务外网广域网节点具备完善的 MPLS VPN 功能支持 LDP、RSVP-TE 等 MPLS 标签分发协议，支持 P/PE 功能，符合 RFC2547bis 协议，支持三种跨域 MPLS VPN 方式，支持分层 PE（HoPE），支持多角色主机，支持二层、三层 VPN，跨域 L2、L3 VPN 实现，支持 MPLS TE FRR 和 LDP FRR，切换时间小于 50ms，支持 6PE、6vPE，支持分布式组播 VPN，支持 ACL 识别流量功能，将流量导入到不同的 VPN，支持 MPLS VPN 网络故障定位功能，支持 MPLS PING/TRACEROUTE，支持 L2 VPN 接入 L3 VPN，支持 QinQ 方式 VPLS 接入。

支持 IPv4 和 IPv6 双协议栈，支持静态路由、RIP、RIPng、OSPF、OSPFv3、IS-IS、IS-ISv6、BGP、BGP4+，支持 VRRP、VRRPv3，支持 IPv6 邻居发现，PMTU 发现，TCP6，ping IPv6，traceroute IPv6，socket IPv6，静态 IPv6 DNS，指定 IPv6 DNS 服务器，TFTP IPv6 client，支持 IPv4 向 IPv6 的过渡技术，支持 ICMPv6 MIB、UDP6 MIB、TCP6 MIB、IPv6 MIB 等，支持等价路由 ECMP，非等价路由 UCMP，支持策略路由，支持路由策略，支持 GRE 等隧道功能，支持静态路由 FRR、OSPF FRR、ISIS FRR、BGP FRR。

支持 VXLAN、EVPN，支持 PECP 协议，支持 BGP-LS 等网络信息收集协议，支持 Netconf、YANG 协议，支持 Segment routing，支持 CBTS，支持 OpenFlow v1.3 协议，支持 BGP FlowSpec 功能等主流的 SDN 技术。

支持流量统计分析功能，支持 Netstream，符合 V5/V8/V9 输出格式，支持采样功能和流统计功能，支持多日志主机功能，支持硬件的网络流量应用分析技术，支持 IPv4/IPv6/MPLS 的流量采集分析，支持端口进出方向的流量采集分析，支持异常流量检测及监控功能

(host-monitor)，协助运维人员实时了解核心网络流量情况。

支持多套的拥塞避免机制(H-QoS)，支持PQ/WFQ/CBWFQ等队列调度机制，支持流量整形Shaping，支持RED/WRED等拥塞避免技术，支持优先级标记Mark/Remark，支持802.1p、ToS、DSCP、EXP优先级映射，支持拥塞避免、流量监管和整形功能(Car、traffic Shaping等)，支持数据包标记功能(基于IP地址、端口号、802.1P、DSCP值等)，支持数据包多级队列机制(包括CQ、PQ、LLQ、WFQ等)，支持组播的QoS功能，支持200ms缓存。

支持PIM-DM、PIM-SM、PIM-SSM、MSDP、MBGP、Anycast-RP等路由协议，支持IGMP V1/V2/V3、IGMP Snooping V1/2/3，支持PIM6-DM、PIM6-SM、PIM6-SSM，支持MLD(Multicast Listener Discovery) V1/V2、MLD Snooping V1，支持组播策略和组播QoS等组播相关协议。

支持不间断转发NSF、不间断路由NSR和GR，支持IP TRUNK、MP、ETH端口聚合，支持PW redundancy、Ethernet OAM、Y.1731等保护机制，支持BFD，实现各协议的快速故障检测机制，故障切换时间小于50ms，支持FRR，业务切换时间小于50ms网络可用度为99.999%，支持RFC2544，支持自动发包检测吞吐量、时延抖动和丢包检测链路等，平均无故障时间(MTBF)大于20年。

支持多重安全保障机制，如支持用户分级管理和口令保护，支持AAA安全认证协议(如Radius等)，支持控制平面防攻击，支持安全认证功能，支持SSHv2，为用户登录提供安全加密通道，支持标准和扩展ACL，可以对报文进行过滤，防止网络攻击，支持防止ARP、未知单播报文、广播报文、未知单播报文、本机网段路由扫描报文、TCP SYN报文、TTL=1报文、PADI、DHCP、TCP Sync、Portal、协议报文等攻击功能，支持PADI、DHCP、PORTAL防攻击，支持单播逆向路由检查URPF技术，防止基于源地址欺骗的网络攻击行为，支持RIPv2、OSPF、ISIS、BGP、OSPFv3、ISISv6及BGP4+的明文及MD5密文认证，支持Keychain功能，可以基于时间段生效不同密钥，支持安全网管SNMPv3等。

➤市直重点单位城域网核心设计

市直重点单位城域网采用核心、汇聚、接入三级架构设计，核心层设备只需要做高速的数据交换，汇聚层设备用于接入部门的汇接，接入层设备部署于各政务部门机房，用于各政务部门局域网的接入。

实现区各政务部门联网后，与市级广域网核心节点高速互联，实现部门网络(含VPN)与国家、省级电子政务外网、市县政务外网的互联互通。

城域网路由：城域网路由节点配置8个万兆接口(可兼容千兆)，支持端口聚合和链路拥

绑,提高可靠性,向上连接域核心路由组网,向下接入区域域汇聚交换服务。

支持丰富的 MPLS 功能,如支持 LDP、RSVP-TE 等 MPLS 标签分发协议,支持 P/PE 功能,符合 RFC2545 协议,支持三种跨域 MPLS VPN 方式,支持分层 PE (HoPE),支持多角色主机,支持二层、三层 VPN,跨域 L2、L3 VPN 实现,支持 MPLS TE FRR 和 LDP FRR,切换时间小于 50ms,支持 6PE、6vPE,支持分布式组播 VPN,支持 ACL 识别流量功能,将流量导入到不同的 VPN,支持 MPLS VPN 网络故障定位功能,支持 MPLS PING/TRACEROUTE,支持 L2 VPN 接入 L3 VPN,支持 QinQ 方式 VPLS 接入。

支持 IPv4 和 IPv6 双协议栈,支持静态路由、RIP、RIPng、OSPF、OSPFv3、IS-IS、IS-ISv6、BGP、BGP4+,支持 VRRP、VRRPv3,支持 IPv6 邻居发现、PMTU 发现、TCP6、ping IPv6、traceroute IPv6、socket IPv6、静态 IPv6 DNS、指定 IPv6 DNS 服务器、TFTP IPv6 client,支持 IPv4 向 IPv6 的过渡技术,支持 ICMPv6 MIB、UDP6 MIB、TCP6 MIB、IPv6 MIB 等,支持等价路由 ECMP,非等价路由 UCMP,支持策略路由,支持路由策略,支持 GRE 等隧道功能,支持静态路由 FRR、OSPF FRR、ISIS FRR、BGP FRR。

支持 VXLAN、EVPN,支持 PECP 协议,支持 BGP-LS 等网络信息收集协议,支持 Netconf、YANG 协议,支持 Segment routing,支持 CBTS,支持 OpenFlow v1.3 协议,支持 BGP FlowSpec 功能等主流的 SDN 技术。

支持流量统计分析功能,支持 Netstream,符合 V5/V8/V9 输出格式,支持采样功能和流统计功能,支持多日志主机功能,支持硬件的网络流量应用分析技术,支持 IPv4/IPv6/MPLS 的流量采集分析,支持端口进出方向的流量采集分析,支持异常流量检测及监控功能 (host-monitor),协助运维人员实时了解核心网络流量情况。

支持多层嵌套的 QoS 机制 (H-QoS),支持 PQ/WFQ/CBWFQ 等队列调度机制,支持流量整形 Shaping,支持尾丢弃 TD /WRED 等拥塞避免技术,支持优先级标记 Mark/Remark,支持 802.1p、TOS、DSCP、EXP 优先级映射,支持拥塞避免、流量监管和整形功能 (Car、traffic Shaping 等),支持数据标记功能 (基于 IP 地址、端口号、802.1p、DSCP 值等),支持数据包多级队列机制 (包括 CQ、PQ、LLQ、WFQ 等),支持组播的 QoS 功能,支持 200ms 缓存。

支持 PIM-DM、PIM-SM、PIM-SSM、MSDP、MBGP、Anycast-RP 等路由协议,支持 IGMP V1/V2/V3、IGMP Snooping V1/2/3,支持 PIM6-DM、PIM6-SM、PIM6-SSM,支持 MLD (Multicast Listener Discovery) V1/V2、MLD Snooping V1,支持组播策略和组播 QoS 等组播相关协议。

支持不间断转发 NSF、不间断路由 NSR 和 GR,支持 IP TRUNK、MP、ETH 端口聚合,支持

PW redundancy、Ethernet OAM、Y.1731 等保护机制，支持 BFD，实现各协议的快速故障检测机制，故障恢复时间小于 50ms，支持 FRR，业务切换时间小于 50ms 网络可用度为 99.999%，支持 RFC2544，支持自动丢包检测吞吐量、时延抖动和丢包检测链路等，平均无故障时间 (MTBF) 大于 20 年。

支持多重安全保障机制，如支持用户分级管理和口令保护，支持 AAA 安全认证协议（如 Radius 等），支持控制平面防攻击，支持安全认证功能，支持 SSHv2，为用户登录提供安全加密通道，支持标准和扩展 ACL，可以对报文进行过滤，防止网络攻击，支持防止 ARP、未知组播报文、广播报文、未知单播报文、本机网段路由扫描报文、TCP SYN 报文、TTL=1 报文、PAD1、DHCP、TCP Sync、Portat、协议报文等攻击功能，支持 PAD1、DHCP、PORTAL 防攻击，支持单播逆向路由检查 URPF 技术，防止基于源地址欺骗的网络攻击行为，支持 RIPv2、OSPF、ISIS、BGP、OSPFv3、ISISv6 及 BGP4+ 的明文及 MD5 密文认证，支持 Keychain 功能，可以基于时间段生效不同密钥，支持安全网管 SNMPv3 等。

►市直重点单位级城域网汇聚设计

市直重点单位城域网汇聚：汇聚节点配置千兆接口和万兆接口。支持端口聚合和链路捆绑，提高可靠性。向上与城域核心路由互联，向下通过数据专线与全区县各单位机构互联。

市直重点单位城域网汇聚节点支持 IPv4/IPv6 双协议栈，支持多种隧道技术，支持 IPv4/IPv6 的组播技术，具备完善的 IPv4/IPv6 解决方案。提供完善的安全防护机制，可从控制、管理、转发三平面全面保障网络的安全：在控制平面，内置协议报文攻击识别模块，防止 TCN、ARP 等协议报文攻击，OSPF/BGP/IS-IS 路由协议采用 MD5 验证，防止非法路由更新报文导致的网络瘫痪；在管理平面，SNMPv3 网管协议，SSH V2，基于 802.1x、AAA/Radius 的用户身份认证以及分级的用户权限管理保证了设备管理的安全性；在转发平面，支持 IP、VLAN、MAC 和端口等多种组合精细绑定；支持 uRPF 单播反向路径转发，防止非法流量访问网络，采用最长匹配逐包转发机制，有效抵御病毒的攻击。支持强大的 ACL 能力：支持标准和扩展 ACL；支持基于 VLAN 的 ACL，方便用户配置，节省 ACL 资源；支持出方向和入方向的 ACL，满足访问权限严格控制的需求。支持不间断转发和优雅重启，提供毫秒级的切换时间；支持等价路由，可帮助用户建立多条等值路径，实现流量的负载均衡及冗余备份；支持 RRRP 快速环网保护协议；支持 Smart-Link 协议，保证双上行网络拓扑的业务毫秒级快速切换。通过上述技术，可以在承载多业务的情况下不间断运行，实现业务的水续。

二层特性	支持 IEEE 802.1p (CoS 优先级) 支持 IEEE 802.1Q (VLAN) 支持 IEEE 802.1d (STP) / 802.1w (RSTP) / 802.1s (MSTP) / BPDU 保护 支持 IEEE 802.1ad (QinQ), 灵活 QinQ 和 Vlan mapping 支持 IEEE 802.3x (全双工流控) 和背压式流控 (半双工) 支持 IEEE 802.3ad (链路聚合) 和跨板链路聚合 支持 RRPP (快速环网保护协议) 支持跨板端口/流镜像 支持端口广播/多播/未知单播风暴抑制 支持静态 MAC、动态 MAC、黑洞 MAC 支持 Jumbo Frame 支持基于端口、协议、子网和 MAC 的 VLAN 划分 支持 SuperVLAN 支持 PVLAN 支持 Multicast VLAN+ 支持点到点单 VLAN 交叉连接、双 VLAN 交叉连接 支持最大 VLAN MAPPING/灵活 QinQ 表项 支持 GVRP 支持 LLDP
IPv4 路由特性	支持 ARP Proxy 支持 DHCP Relay 支持 DHCP Server 支持静态路由 支持 RIPv1/v2 支持 OSPFv2 支持 IS-IS 支持 BGPv4 支持 OSPF/IS-IS/BGP GR (Graceful Restart 优雅重启) 支持等价路由

	支持策略路由 支持策略
IPv6 特性	支持 IPv6 支持 ICMPv6 重定向 支持 DHCPv6 支持 ACLv6 支持 OSPFv3 支持 RIPng 支持 BGP4+ 支持 IS-ISv6 支持手工隧道 支持 ISATAP 支持 6to4 隧道 支持 IPv6 和 IPv4 双栈 支持 SAVI 功能
组播	支持 IGMPv1/v2/v3 支持 IGMPv1/v2/v3 Snooping 支持 IGMP Filter 支持 IGMP Fast leave 支持 PIM-SM/PIM-DM/PIM-SSM 支持 MSDP 支持 AnyCast-RP 支持 MLDv2/MLDv2 Snooping 支持 PIM-SMv6、PIM-DMv6、PIM-SSMv6 支持用户快速离开机制 支持组播查询器
ACL/QoS	支持标准和扩展 ACL 支持基于 VLAN 的 ACL 支持 Ingress/Egress ACL

	支持 Ingress/Egress CAR，粒度可达 8Kbps 支持 聚合 CAR，MAC 聚合 CAR 功能 支持 流量整形 (Traffic Shaping) 支持 Schedule 支持 802.1P/DSCP 优先级 Mark/Remark 支持层次化 QoS (H-QoS)，支持三级队列调度 支持队列调度机制，包括 SP、WRR、SP+WRR、WFQ 支持拥塞避免机制，包括 Tail-Drop、WRED 支持 Mirroring 支持基于 Layer2 协议头、Layer3 协议、Layer4 协议、802.1p 优先级等的组合流分类
SDN/ OpenFlow	支持 OpenFlow 1.3 标准 支持多控制器 (EQUAL 模式、主备模式) 支持多表流水线 支持 Group table 支持两级 Meter 能力
VXLAN	支持 VXLAN 二层交换 支持 VXLAN 三层交换 支持 VXLAN 路由交换 支持 VXLAN 网关 支持 BGP EVPN 特性 支持 IS-IS+ENDP 的 VXLAN 分布式控制平面 支持 OpenFlow+Netconf 的 VXLAN 集中式控制平面 支持分布式 Anycast 网关，支持 VxLAN Fabric 的自动化部署
MPLS/VPLS	支持 L3 MPLS VPN 支持 L2 VPN: VLL (Martini, Kompella) 支持 MCE 支持 MPLS OAM 支持 VPLS, VLL

	 支持分层 VPLS 支持 VRRP 功能 支持 L2TP 协议
安全机制	支持 EoE 安全解决方案 支持 Portal 认证 支持 MAC 认证 支持 IEEE 802.1x 和 IEEE 802.1x SERVER 支持 AAA/Radius 支持 HWTACACS, 支持命令行认证 支持 SSHv1.x/SSHv2 支持 ACL 流过滤机制 支持 OSPF、RIPv2 及 BGPv4 报文的明文及 MD5 密文认证 支持命令行采用分级保护方式, 防止未授权用户的非法侵入, 为不同级别的用户有不同的配置权限 支持受限的 IP 地址的 Telnet 的登录和口令机制 支持 IP 地址、VLAN ID、MAC 地址和端口等多种组合绑定 支持 uRPF 支持 Macsec, 实现 MAC 层安全加密, 支持对用户数据加密、数据恢复完整性检查及数据源真实性校验 支持主备数据备份机制 支持故障后报警和自恢复 支持数据日志 支持微分段 支持 IP Source Guard, 支持防范 DoS 攻击、ARP 攻击、TCP 的 SYN Flood 攻击、UDP Flood 攻击、广播风暴攻击、大流量攻击 支持 IPv6 RA Guard 支持 CPU 硬件队列实现控制面协议报文分级调度和保护 支持 RMON 支持安全启动

系统管理	 - 支持 FTP、TFTP、Xmodem - 支持 SNMP v1/v2c/v3 - 支持 sFlow 流量统计 - 支持 RMON - 支持 NTP 时钟、PTP (1588V2) 时钟 - 支持电源智能管理，支持 802.3az 高效节能以太网 - 支持设备在线状态监测机制，实现对包括主控引擎、背板、芯片和存储等关键元器件进行检测 - 支持 Telemetry 流量可视化功能 - 支持 INQA 功能，通过对业务报文进行标记，实现对网络级和设备级的丢包统计 - 支持内置智能管理功能，支持通过图形化界面设备配置及命令一键下发和版本智能升级 - 支持 eMDI 技术 - 支持 BootROM 升级和远程在线升级 - 支持热补丁功能，可在线进行补丁升级 - 支持 OPS 开放可编程系统 - 支持 NetStream 流量分析协议
可编程性	- 支持 Ansible 自动化配置，实现网络配置批量发放 - 支持通过 Python/NETCONF/TCL 等对网络自动化编排，实现 DevOps 自动化运维

➤市直重点单位级城域网接入设计

市直重点单位接入单位节点：采取就近接入的原则，采用裸光纤、MSTP、OTN 等灵活的接入方式单链路上联至汇聚层汇聚节点。本项目方案提供一级接入单位 100M 数据专线接入服务。

部门接入路由对政务部门业务开展至关重要，接入路由器需选择高稳定性、高安全性的企业级路由器。一级单位接入专网提供千兆端口接入服务，支持 MPLS VPN、QoS 等功能，满足本部门用于整合共享的公共业务、部门专用业务和互联网业务的高安全接入电子政务外网。接入路由满足电子政务外网接入要求，其特性如下：

业务安全：报文过滤功能，支持状态过滤、MAC 地址过滤、IP 和端口号过滤、时间段过滤等；支持业务流量实时分析等。

网络安全：多样化 VPN 技术，包括 IPsec、L2TP、GRE、ADVPN、MPLSVPN，以及多种 VPN 技术的叠加使用；支持路由器的安全防护，支持 OSPF/RIP/IS-IS/BGP 动态路由协议认证、支持 OSPFv3/RIPng/IS-ISv6/BGP 的 IPsec 加密、支持丰富的路由策略控制功能。

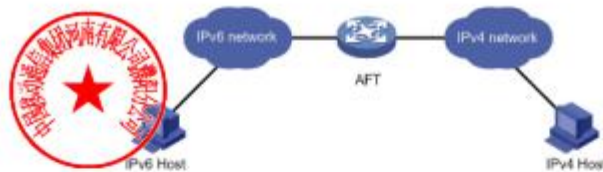
终端接入安全：一体化的终端接入绑定认证，包括 EAD 安全检查认证、802.1x 认证、终端 MAC 地址认证、基于 WEB 的 Portal 认证、终端接入静态绑定、MAC 自动学习绑定；ARP 攻击防范，支持源 MAC 地址固定、ARP 报文攻击防范、地址冲突检测和防护、ARP 端口限速、ARPDetection、ARP 源 MAC 地址一致性检查、ARP 源抑制、ARP 主动确认机制等。

设备管理安全：支持基于角色权限管理，能够基于角色进行资源分配、用户与角色的对应、权限二维分配方式；支持控制平面流量限制，支持基于协议类型、不同队列、已知协议报文、指定协议报文等进行流量控制和过滤；远程安全管理，支持 SNMPv3、支持 SSH、TR069 远程管理等；管理行为控制审计，支持 AAA 服务器集中验证、执行命令行授权、操作记录实时上报等；国密办加密算法；支持国家密码管理局提出的 SM1、SM2、SM3、SM4 加密算法。

➤市直重点单位互联网出口设计

市直重点单位集中统一互联网出口，在互联网出口区分别部署安全出口防护服务和控制管理网关，提供互联网安全隔离防护，提供 IPSEC/SSLVPN、L2TP、GRE、L2TP over IPSEC、GRE over IPSEC 等 VPN 功能。通过安全出口防护服务实现 NAT 转换，NAT (Network Address Translation, 网络地址转换) 是将 IP 数据报文头中的 IP 地址转换为另一个 IP 地址的过程。用于实现允许内部网络用户访问外部公共网络以及允许外部公共网络访问部分内部网络资源 (例如内部服务器) 的目的。提供了 IPv4 和 IPv6 地址之间的相互转换功能。在 IPv4 网络完全过渡到 IPv6 网络之前，两个网络之间直接的通信可以通过 NAT64 来实现。例如，使用 NAT64 可以使 IPv4 网络中的主机直接访问 IPv6 网络中的 FTP 服务器。

如图所示，NAT64 作用于 IPv4 和 IPv6 网络边缘设备上，所有的地址转换过程都在该设备上实现，对 IPv4 和 IPv6 网络内的用户来说是透明的，即用户不必改变目前网络中主机的配置就可实现 IPv6 网络与 IPv4 网络的通信。



12.1.5.8.3 带宽及链路类型设计

电子政务外网链路带宽及网络特性如下表所示。

链路带宽建议及网络特性表

通信链路类型	参数要求	通信延时	单位	数量
电子政务外网骨干线路	1、单条带宽 $\geq 100\text{M}$; 2、速率要求上行、下行对称; 3、所提供的物理链接光纤信号衰减不超过 20db; 4、采用专线直连的方式。	默认 PING 传输时延上限值 10ms; PING 带 2000 字节包, 上限值为 20ms; (省市设备间延时上限值为 100ms; 市县设备间延时上限值为 50ms)	条	135

电子政务外网需采用支持 OTN/MSTP/PTN 或基于 VPLS/MPLS 技术的二层链路, 在链路质量、链路性能等方面应与现有电子政务外网保持一致。链路关键设备应具有冗余、主备等保护措施, 满足各类业务对稳定性、可靠性和安全性的要求。

12.1.5.9 实施关键节点

我公司承诺严格响应招标文件要求, 在合同签订后 15 天内完成。

12.1.5.9.1 第一阶段：项目准备阶段

(1) 主要活动

编号	工作项	描述	交付
----	-----	----	----

1	启动	明确项目组织架构和角色分工。	《会议纪要》
2	制定项目管理计划（经双方确认）	制定质量保证计划。	《质量保证计划》
		制定项目评测计划。	《评测计划》
		制定问题解决计划。	《问题解决计划》
		制定风险管理计划。	《风险管理计划》
		制定整体解决方案。	《项目集成计划》《实施方案设计》
		制定工程实施手册。	《施工实施手册》
		制定测试报告。	《测试报告》
		制定设备配置文档及详细物理连接图。	《设备配置文档及详细物理连接图》
		制定技术报告。	《技术报告》
3	评审项目管理计划	用户方审核乙方的方案文档	《方案评审纪录》

(2) 客户方及其他配合内容

编号	工作项	客户方及其他配合内容
1	制定项目管理计划	确定用户网络基础设施构建项目组成员及其职责。
		负责协调确定接口单位的配合项目建设的人员。

		并确定项目组成员及其职责。
	评审	参与评审并确认承建方制定的《项目管理计划》和《实施手册》等文档。
3	培训	参与制定并确认《系统培训计划》。
		组织人员按培训计划参加培训和测试。
		填写《培训反馈表》，提出培训中出现的问题。
		签署《系统培训服务确认书》。

(3) 具体实施计划

根据要求，我方将在用户所规定的时间内安排设备安装勘察设计，采购本项目所需软、硬件产品，提供本项目详细设计图纸，并在采购人认可的相应的施工图纸及相关技术资料下开展施工准备工作。

根据濮阳市电子政务外网及各基层机构维护人员的具体实际情况，结合本项目的工程特点，对维护人员进行现场实施前的基础知识培训。

所有设备的配置都保证系统的完整性。

12.1.5.9.2 第二阶段：设备到货

(1) 主要活动

编号	工作项	描述	交付
1	濮阳市电子政务外网所需提供的主设备货物。	采购相关材料。 组织供货。 组织各方进行验货。 对机房及安装环境调研	《货物交接单》 《设备到货验收合格单》
2	设备到货后的相关准备工作。	对相关细节进行检查及核对。	

(2) 客户方及其他配合内容

编号	工作项	客户方及其他配合内容
1	货品采购、到货	配合施工方进行现场勘察。 接受实施方的现场培训。
2	到货验收	进行到货验收，签署《货物签收单》。

(3) 具体实施计划

我公司承诺在到货前提供所有实施设备的工作环境说明，包括机房环境要求、供电要求、空间要求、承重要求、散热等。

订货采购期间对施工现场进行实地勘察，到货后组织进行货物验收。在货物包装及运输过程中，我公司将遵循以下要求：

➤提供原厂包装，以防货物在运输中损坏，并提供原厂包装证明。

➤每个箱子侧面清楚标明交货地点的全称；装箱单清楚注明每个站点总箱数（如果分站点交货）；对包装箱内每件辅件进行标签，标明“备件”或“工具”及具体名称，并注明合同号、箱号及安装站。

➤有关的技术资料如样本、图纸、操作手册、维修指南及服务手册、产品产地证明书、质量保证书和系统操作说明书等应清晰、正确、完整，并应随同货物一起发运。

➤我公司负责办理货物的运输及运输保险事宜、支付交货前发生的包装费、运费、保险费、商检费、搬运费等费用。

➤将货物及合同规定的相关文件送达指定的现场。

12.1.5.9.3 第三阶段：工程施工

(1) 主要活动

编号	工作项	描述	交付
1	按照招标文件技术要求和实施计划要求进行线路施工	相关设备的上架和光缆线路铺设。 按照施工工艺手册调试设备。 按照测试方案对平台进行测试。 完成与配套设备的联合调试，构成整体的系统平台。 在现场对用户进行必要的现场培训工 作。	《工作日志》 《调试文档》

编号	工作项	描述	交付
2	按照施工工艺手册调试设备	实施工艺手册调试设备。 安装完毕后进行测试及状态确认。 在现场对用户进行必要的现场培训工作。	《工作日志》
3	按照测试方案进行测试	按照测试方案进行测试。 在现场对用户进行必要的现场培训工作。	《工作日志》 《安装测试报告》

(2) 客户方及其他配合内容

编号	活动	客户方及其他配合内容
1	设备施工	审核并确认承建方制定的《设备施工计划》。 积极配合承建方的安装调试工作，协助进行系统平台测试，编写《系统平台测试报告》。 接受实施方的现场培训。
2	按照施工工艺手册调试设备	审核并确认承建方制定的《线路施工计划》。 积极配合承建方的安装调试工作，协助进行测试及状态确认。 接受实施方的现场培训。
3	按照测试方案进行测试	协助进行测试及状态确认。 接受实施方的现场培训。

(3) 具体实施计划

➤ 设备安装在我方机房，我方将遵守以下施工要求：

- 选择符合电信级要求的机房安装用户设备。

- 项目组专职人员负责设备安装的总协调，确保我方设备安装机房和其它安装场地配备符合货物安装的要求设施。我方派遣有经验的技术人员组成工作小组到现场实施技术服务，包括设备安装、软硬件的调试和调优服务等。并且提供工作小组成员名单及联系方式

(包括电话、手机、传真及电子邮件等)。设备安装调试的主要目标是使采购设备能够正常运行,我方确保与之相联的全部设备正常、正常运行。

●项目所有设备全部由我方完成安装调试,在安装、调试过程中造成的设备损坏,一切责任由我方承担。安装、调试及验收期间的工作进度、每天的主要工作、发现的问题及解决方法均须记录在工作日志上。

●按标书要求对其货物的性能和配置进行安装、调测检查,并做出安装、调测报告。所供设备在合同中所规定的地点和环境下,实现正常运行并达到合同要求的性能和产品技术规格中的性能。完成与配套设备(包括本项目采购的其它设备、其它项目近期采购的设备和原有设备)的联合调试,构成整体的系统平台,进行相关的配置和系统优化调试。当所供设备或软件在安装、调测中出现性能指标或功能上不符合技术要求时,由我方负责免费解决。

●项目实施过程中,我方将按照涉密信息系统集成的相关要求开展工作,遵守国家保密工作部门的相关规定。

➤设备安装和用户机房,我方将遵守以下施工要求

●用户确保在我方的工程师到来之前,机房和其它安装场地配备符合货物安装的要求设施。我方派遣有经验的技术人员组成工作小组到现场实施技术服务,包括设备安装、软硬件的调试和调优服务、现场培训等。并且提供工作小组成员名单及联系方式(包括电话、手机、传真及电子邮件等)。设备安装调试的主要目标是使采购设备能够正常运行,我方确保与之相联的全部设备正常、正常运行。我方在安装设备之前,先对用户的相关人员进行现场培训,并在用户相关技术人员的监督下进行安装、检测和排除故障。

●我方未经用户批准,不在现场安装任何设备。提供的所有设备全部由我方完成安装调试,用户派遣技术人员参与整套设备的安装和调试,在安装调试过程中我方的技术人员负责说明设备的安装步骤和应该注意的事项,安装的每一件设备应作安装详细记录。在安装、调试过程中造成的设备损坏,一切责任由我方承担。安装、调试及验收期间的工作进度、每天的主要工作、发现的问题及解决方法均须记录在工作日志上,工作日志每天的记录双方签字确认,双方各保留一份。

●按标书要求对其货物的性能和配置进行安装、调测检查,并做出安装、调测报告。所供设备在合同中所规定的地点和环境下,实现正常运行并达到合同要求的性能和产品技术规格中的性能。完成与配套设备(包括本项目采购的其它设备、其它项目近期采购的设

备和原有设备）的联合调试，构成整体的系统平台，进行相关的配置和系统优化调试。当所供设备软件安装、调测中出现性能指标或功能上不符合技术要求时，由我方负责免费解决。

●项目实施过程中，我方将按照涉密信息系统集成的相关要求开展工作，遵守国家保密工作部门的相关规定。

12.1.5.9.4 第四阶段：调试开通

(1) 主要活动

编号	工作项	描述	交付
1	设备调试开通	安装的设备以及传输电路开通调试。 和用户共同对性能指标进行测试验收。	《阶段工作成果报告》 《实施报告》 《验收测试报告》
2	系统试运行	制定验收计划。 制定测试计划。 组织测试。 组织项目验收。 为设备移交编写相关手册	《项目验收计划》 《整体测试报告》 《验收报告》 《安装手册》

(2) 客户方及其他配合内容

编号	活动	客户方及其他配合内容
1	系统调试开通	配合乙方对性能指标进行测试验收。 参议对项目的整体测试工作。 听取乙方的项目汇报。 对阶段工作提出建议。
2	系统试运行	参与制定制定验收计划。 组织相关部门参与项目初验。 签署《系统试运行报告》

(3)具体实施计划

➤所有设备安装完成并通过初步验收后，进入1个月的连续试运行。在试运行期间，我方负责任何故障或问题都能在收到故障通知后2-4小时内（节、假日也不例外）被修复和解决，并给出详细修复细节报告。系统最终验收合格的条件至少满足以下三个要求：

- ① 已提供了合同的全部产品和资料；
- ② 试运行时间满足合同要求；
- ③ 性能测试和试运行时出现的问题已被解决。

12.1.5.9.5关键节点保障措施

我方已经针对本项目制定了详尽的设计和缜密的实施方案。我方除安排安装工程师进行设备安装外，还有1组备份人员。同时，针对各类突发事件，我们设计了相应的预防与解决措施，提供了完整的应急处理流程。

我们要求项目实施过程中，实施人员直接将突发情况报告项目经理，项目经理对突发事件做出判断，安排相关小组处理。如属软件问题，安排系统设计小组以最快的方式向实施人员提供没问题的软件；如属硬件和货物问题，安排商务小组以最快的方式向实施人员提供备用的设备或部件。

同时，由项目经理将故障情况通报各项目实施小组，保证所有实施人员可以尽快获得相关信息，避免同一情况的再次发生。

12.1.5.10实施项目进度控制

12.1.5.10.1实施进度安排

根据项目实施计划安排，具体实施进度安排如下，整网并行实施，分两组组实施人员，整个工期为15天，安装调试计划如下：

序号	实施环节	具体实施内容	工期（天）	备注
1	工前准备	工程实施方案	0.5	实施团队、技术专家与甲方单位项目经理一同分析讨论
2		开工会，工期协调会	0.5	实施团队、技术专家、甲方单位一同参加

3		施工人员技术培训	工前	实施团队、技术专家
4	验收	设备开箱验收, 确保设备数量齐全, 签署设备签收单	0.5	实施团队项目经理、甲方单位项目经理
5		设备加电验收, 确保设备工作正常, 签署设备验收单	0.5	实施团队项目经理、甲方单位项目经理
6	设备安装调试	工勘实施环境, 形成工勘报告	工前	实施团队成员、甲方单位项目成员
7		协调设备安装, 设备出库和进场	1	实施团队成员、甲方单位项目成员
8		设备安装, 严格安装厂商的设备安装规范安装及加电, 注意实施环境卫生及规范	5	实施团队成员
9		设备加电、升级软件版本, 设备预配置	2	实施团队成员
10	试运行	按照甲方业务试运行条例要求, 确保业务正常运行	1	实施团队成员, 甲方单位项目成员
11	项目验收	通过试运行期后, 整个系统能够稳定可靠的运行; 全部设计功能运行无误。	1	评审专家、实施团队项目经理、技术专家、甲方单位等参加
12	实施培训	确保运维团队详细、准确了解项目情况	1	实施团队项目经理、甲方单位项目经理、甲方单位运维团队
13	技术培训	确保运维团队详细、准确了解项目技术情况	1	实施团队项目经理、甲方单位项目经理、甲方单位运维团队
14	文档提交	项目文档提交, 确保文档	1	实施团队项目经理、甲方单位

	详细、准确，便于查阅	项目经理、甲方单位运维团队
--	------------	---------------

12.1.5.10.2 施工进度里程碑

为了进一步确保施工进度和质量，便于提前发现问题、解决问题，我们将对项目进行分解，定义相应的阶段里程碑，配有相关的考核标准，以细化控制粒度，确保工程实施能够满足客户要求。详细的里程碑及考核标准设计如下表所示：

序号	里程碑事件	考核标准
1	工前准备	1. 项目组织架构明确清晰 2. 项目组成员分工明确 3. 施工人员技术培训完备 4. 实施方案细致准确
2	到货验收	1. 到货数量盘点 2. 设备上电测试
3	设备安装调试	1. 所有设备上架完备 2. 所有设备版本升级 3. 所有设备配置调试
4	试运行保障	试运行保障，按照招标要求实行保障
5	系统终验	通过试运行期后，整个系统能够稳定可靠的运行；全部设计功能运行无误。
6	技术文档提交及培训	技术文档提交及培训

12.1.5.10.3 施工进度控制计划

编制详细的施工进度计划表，并执行施工进度计划：严格按照制订好的进度计划，全方位开展施工。在施工过程如发现施工进度与形象进度有出入时，马上找原因，并及时进行调整，确保每道工序、每个分项工程都在计划工期之内。整个工程要加强计划工期控制，每周制订工程周进度计划，并严格执行进度计划。

➤采取有效措施，控制影响工期的因素

为保证该工程项目能按计划顺利、有序地进行，并达到预定的目标，必须对有可能影响工

工程按计划进行的因素进行分析,事先采取措施,尽量缩小实际进度与计划进度的偏差,实现对项目工期的控制。影响项目进度的主要因素有计划因素、人员因素、技术因素、材料和设备因素、机具因素、气候因素等,对于上述影响工期的诸多因素,我们将按事前、事中、事后控制的原则,分别对这些因素加以分析、研究,制定对策,以确保工程按期完成。

➤利用计算机进行计划管理

根据本项目的工程、特点及难点,安排合理的施工流程和施工顺序,尽可能提供施工作业面,使各分项工程可交叉进行。在各工序持续时间的安排上将根据以往同类工序的经验,结合本工程的特点,留有一定的余地,并充分征求有关方面意见加以确定,同时要据各个工序的逻辑关系,应用目前国内较先进的梦龙网络软件,编制总体网络控制计划,明确关键线路,确定若干工期控制点,同时将总计划分解成月、旬、周、日作业计划,以做到以日保周、以周保月、以月保总体计划的工期保证体系。

根据确定的进度检查日期,及时对实际进度进行检查,并据此做出各期进度控制点,及时利用微机对实际进度与计划进度加以分析、比较、及时对计划加以调整,在具体实施时牢牢抓住关键工序及设定的各控制点两个关键点,一旦发生关键工序进度滞后,则及时采取增加投入或适当延长日作业时间等行之有效的方法加以调整。

➤确保材料、构件、设备保质保量按计划到位

施工中根据施工进度计划和施工预算中的工料分析,编制材料、构件及相关设备需用量计划,作为定货、备料、供料和确定仓库、堆场面积及组织运输的依据。按计划分批进场,并做好进场验收、发放和保管工作。

➤严格安全管理,杜绝重大事故发生

制定严格的安全管理制度,结合具体情况,制定周密的安全技术方案和安全操作规程,并在实施中狠抓落实,杜绝安全事故发生。

12.1.5.11 实施部署问题预判与解决方法

12.1.5.11.1 问题预判与解决方法

(1) 本项目实施中可能面临的问题分析

本项目工期短,按期完成建设是实施的最大难点;

本项目是一个综合性的网络系统集成项目,涉及多个实施环节,与多个部门的交互,容易造成项目管理上的混乱,无法精准把控项目进度;

本项目建设单位数量众多且分布分散，难以协调时间和容易遗漏安装部署点位；

同时，项目实施中可在保证进度的前提下，保证设备的安全和人身的安全，这个也是项目管理中要解决的问题。

(2) 项目实施中的问题解决方法

集中力量保质量、保工期

在人力、物资上给工程施工以充分保证。各项管理工作应着眼于促进该项目施工工作，搞好与各有关单位及部门的全面协调配合。

分阶段施工

由于项目施工设备较多，我们把整体项目拆分成多阶段实施，力争做到忙而不乱，疏而不漏。整体项目实施分4个阶段，包括调研规划阶段、县级单位建设阶段、系统联调测试阶段、项目验收阶段等。

配合施工，穿插作业，重点单位抢工

该工程施工配合量大、面广，在不影响各专业的情况下，必须配合各有关单位及部门的工作时间进行施工，确保工程按期投入使用。

实施全过程进行人身安全防护

操作设备前，应佩戴防静电手套和腕带，并去除首饰和手表等易导电物体，以免被电击或灼伤。

如果发生火灾，应撤离建筑物或设备区域并按下火警警铃，或者拨打火警电话。任何情况下，严禁再次进入燃烧的建筑物。

实施全过程进行设备安全防护

操作前，应先将设备可靠地固定在地板或其他稳固的物体上，如墙体或安装架。

系统运行时，请勿堵塞通风口。

安装面板时，如果螺钉需要拧紧，必须使用工具操作。

安装完设备，请清除设备区域的空包装材料。

12.1.5.11.2 SRv6 基础网络部署

SRv6 路由协议部署

Segment Routing 是对 MPLS 协议的简化和优化，尤其是控制平面，只需要支持 IGP 协议，不再需要部署 LDP 或 RSVP-TE 协议，通过 IGP 协议的 SR 扩展来同步，或者由控制器统一进行

分配和下发，大大简化了设备运行的协议数量。

Segment Routing 只需要 IGP 协议就可以完成标签转发表的建立，并且非常容易扩展，规模也很小。目前 SRv6 节点标签数量，一般为全网节点数量 + A（邻接标签数据，一般为设备接口数量）。

现使用 OSPFv3 协议作为 SRv6 IGP 协议。OSPFv3 为支持 SRv6 也做了扩展：

SRv6 Locator LSA 和 Prefix LSA：发布 Locator 路由信息，其中普通 IPv6 节点通过 Prefix LSA 学习 Locator 路由，SRv6 Locator LSA 除了携带路由信息外，还会携带 End SID 等 SRv6 SID 信息，SID Sub-TLV 发布 SRv6 SID 和 SID 对应的 SRv6 Endpoint 节点行为信息。

OSPFv3 能够传递 Locator 路由信息，能够把节点以及链路信息发布至全网（电子政务外网骨干网内部），帮助我们构建隧道。

还需要一种协议用来传递 PE 间业务路由，此协议选择 BGP，由于网络采用 IPv6 协议作为基础地址配置，所以采用 BGP4+ 作为电子政务外网骨干网业务路由传递协议。

BGP 4+ 协议部署

区县电子政务外网的核心层路由器和市核心路由都被划分到同一个 AS 中，IGP 选择 OSPFv3 协议，BGP 地址族选择 EVPN 协议。采用 EVPN L3VPN over SRv6 技术体系进行组网发布 VPN 路由。

BGP 路由器标识部署

BGP4+ 的 router id 只能使用 X.X.X.X 的 IPv4 地址形式表示，因此本项目中 BGP4+ 的 router id 与 Loopback0 的 IPv4 地址值相同。

BGP 邻居关系的类型

电子政务外网骨干网内使用 EVPN L3VPN over SRv6 技术建立 IBGP 邻居关系，骨干网与省网间建立 EBGP 邻居关系。

OSPFv3 协议部署

OSPFv3 协议作 IGP 协议，用于传递设备间建立 EVPN 邻居的 Loopback 地址和 SRv6 Locator 信息。

协议设计说明：

骨干网内所有路由器均需要启用 OSPFv3 协议，与 CE 互联接口不启用 OSPFv3；

为了保障 OSPFv3 协议自身安全性，接口下开启相关认证，认证采用 MD5 认证；

正常情况下 OSPFv3 DB 表内没有任何域外路由；

所有链路类型均为 point-to-point 模式:

通过配置 OSPF Grace 和 OSPF NSR 实现设备主备主控板切换时 OSPF 会话不中断:

OSPF 进程规划

电子政务外网骨干网所有设备上 OSPFv3 进程号统一。

OSPFv3 router id 规划

由于 OSPFv3 的 router id 只能使用 X.X.X.X 形式表示, 本次项目中 OSPFv3 的 router id 使用与设备 Loopback0 地址相同的值作为 router id。

OSPFv3 区域号规划

由核心层和接入层组成的骨干网内的设备都部署在单一 OSPFv3 骨干区域内。

OSPF Cost 值规划

OSPF 协议通过收集链路的 Cost 值, 对比大小来评价路由的优劣, 决定数据流传递的路径。Cost 值的配置可以分为静态配置和依据带宽动态计算配置两种方法。静态配置方法的路由可控性比较好, 但不足之处是一旦设定, Cost 值不能随链路物理带宽的变化而发生改变, 而动态自动计算的方法, Cost 值可以随链路物理带宽变化自动计算。目前调度数据网采用的是动态计算 OSPF Cost 值的方法。

OSPF Cost 值动态自动计算的公式如下:

链路 Cost = [参考带宽/物理接口带宽]

电子政务外网骨干网带宽范围是 10G-100G, 因此带宽参考值配置为 100G。

OSPFv2 协议部署

双栈场景中, OSPFv2 与 OSPFv3 采用相同的部署方式, 具体规划部署参考本文档中 OSPFv3 协议部署章节。

12.1.5.11.3 SRv6 Overlay 网络部署

流量转发模型

概述

本章节介绍电子政务外网骨干网流量转发模式原理设计, 基于基础网络环境已经构建完成的基础上 (OSPFv3 以及 BGP4+)。重点介绍数据流量在广域网是如何流转的, 主要说明流量转发基础环境以及转发过程涉及主要技术以及原理。具体设计细节由后续章节进行补充。

流量转发原理

假设链路中断或对应某种业务带宽、延迟和抖动等链路需求不再满足需求，ADWAN 控制器流量进行重调度。

背景：控制器已纳管相关网络设备，并在控制器上已定义完成应用组配置，控制器已下发相关配置至路由器设备。

流量从 CE1 流出，进入 PE1 入口处。

业务流量在 PE1 被定义成 ACL，使用 MQC 配置重新标记业务流量的 Service-class 值与 SRv6 封装后的 IPv6 头部 DSCP 值。

Service-class 值是业务流量与隧道的纽带，业务流量通过此值进入相应隧道，然后路由器会根据 SR 功能给流量封装 SRH 头部与 IPv6 头部。封装完成后流量根据 SRH 头部中 SID 进行转发。

通过查看 PE1 的 FIB 表，即可观察流量转发情况。

数据包在封装 SRv6 的 IPv6 头部时，会根据 MQC 重标记的 DSCP 值重置 IPv6 头部中的 DSCP 值，使此值与预先配置好的 CBQ 队列保障中值对应，使流量按照队列保障规则进行转发。

实现方式



实现方式分为以下步骤：

SRv6 SID 同步，路由学习。

流量分类与染色：此处用于定义业务流量，分配 Service-class 值，同时分配 DSCP 值。Service-class 值用于匹配隧道，DSCP 值用于匹配流量出接口队列保障 DSCP 值。

隧道建立：此处控制器为应用下发隧道，其中隧道中包含 Service-class 值，此值与应用定义时的 Service-class 值相对应，是应用与隧道之间的纽带，用于区分不同流量进入不同隧道。

数据流引流：应用定义完成后与隧道绑定，流量即可进入隧道转发。

SID 同步、路由学习

标识网络的 SID 由 OSPFv3 同步,使每个设备知晓网络中每个节点(路由器)的 SID 信息。
同时控制器通过 BGP-LS 收集到全网链路及设备信息,用于路径编排。

流量转发的前提是在网络中每台 PE 设备都通过 BGP4+ 协议学习到对端的业务路由。所以需要配置好相关路由配置,使业务路由能够整网传递。这样流量在始发 PE 设备上查找对端业务路由时才能根据 SRv6 协议能力引流至隧道中。

业务分类与定义

根据业务类型进行区分重要程度,然后在控制器上根据五元组进行定义。

假设:

某业务源地址为 A,目标地址为 B。

始发设备为 PE1,目标为 PE1。

那么策略作用域源为 PE1,目标为 PE1。

如下图所示:

然后控制器会在 PE1 上下发 ACL 定义流量,配置如下(因为业务流量为双向流量,所以实际配置中需要定义双向流量):

(控制器下发,非手动配置)

```
acl advanced name ACL-c4013a0a-5840-4089-9fad-e9e85a47220b
```

```
rule 0 permit ip source A destination B
```

```
traffic classifier ADWAN-trafficClassifier1 operator or
```

```
if-match acl name ACL-c4013a0a-5840-4089-9fad-e9e85a47220b
```

(控制器下发,非手动配置)

```
traffic behavior ADWAN-trafficBehavior1
```

```
remark tunnel-dscp 56 //对应配置好的 CBQ 模板。进入相应的队列。
```

```
remark local-precedence 7
```

```
remark Service-class 1 //此值与隧道中的值对应,即可根据此值引入响应隧道。
```

```
#
```

```
QoS policy ADWAN-QPInXGExxx //在 PE 路由器流量入口处下发
```

```
classifier ADWAN-trafficClassifier1 behavior ADWAN-trafficBehavior1
```

#

SRv6 Policy 建立

控制器根据 Policy SID 级别中要求的链路质量信息为应用选出符合的链路 SID 集合，生成隧道下发至配置策略作用域的设备中，流量根据隧道中 SID 进行转发。

(控制器下发，非手动配置)

segment-list ADWAN-SRV6-PATH-1 //隧道路径

index 10 IPv6 SID1

index 20 IPv6 SID2

index 30 IPv6 SID3

policy ADWAN-SRV6Policy-715faeb0-0dc9-4cb9-88bf-e45b694e3ff0 //隧道名称

binding-sid IPv6 xxx

color 2 end-point IPv6 xxx

backup hot-standby enable

sbfd enable remote 1000036 template SRV6-BFD-Template0 oam-sid xxxx

Service-class 1 //隧道通

过此值与流量绑定

candidate-paths

preference 300

explicit segment-list ADWAN-SRV6-PATH-1 weight 100

数据流引流

引流流程：控制器上定义应用后下发 ACL 至设备，然后通过 MQC 中类匹配该 ACL，在流行为中为该流打上 Service-class 值，控制器根据该应用 SLA 要求的链路质量下发隧道，隧道中匹配该 Service-class 值，至此流量引入至该隧道。当数据流引入至 SRv6 隧道后，数据流根据 SID 值进行转发。

SRv6 SID 部署

标识 SRv6 Segment 的 ID 称为 SRv6 SID，是一个 128bit 的值，通常由三部分组成：



Locator: 是一个网络节点的标识, 具有路由能力, 指导流量在指定的节点转发。Locator 在 SR 域内唯一。

Function: 标识该指令要执行的转发动作, 不同的转发行为由不同的 Function 来表达, 例如转发报文到指定链路、在指定的表中进行查表转发等。SR 域内指定节点收到流量后, 根据 SRv6 SID 的 Function 字段执行相关操作。

Arguments (Args) 是一个可选字段, 是指令在执行时对应的参数, 例如流、服务或其他相关的信息。

SRv6 的 SID 主要体现在 Locator 中, 由管理员手工部署, 通过 OSPFv3 路由同步全网。本方案中使用到的 SRv6 SID 如下:

标识网络的 Function End SID: 把下一个 SID 复制到 IPv6 目的地址, 进行查表转发, 每个设备分配一个, 由控制器自动下发通过 OSPFv3 路由由全网同步形成转发表项, 使用静态分配 Function 标签范围:

标识网络的 Function End.X: 根据指定出接口转发报文。设备每一个下一跳分配一个, 由控制器自动下发, 并通过配置形成转发表项, 使用静态分配 Function 标签范围:

标识服务的 Function BSID: 在 SRv6 Policy 的引流中起着重要作用。控制器下发的每个 SRv6 Policy 都分配一个 BSID。当应用转发路径太长需要进行 Policy 链接, 则在源节点将中间节点需要链接的 SRv6 Policy 对应的 BSID 标签封装到 Segment list 最后一个 SID。可以节省 Segment 列表空间。

标识服务的 Function, END.DT4 SID / END.DT6 SID 等 VPN SID, 设备自动生成、同步, 并封装在 SRv6 路径中。使用动态分配 Function 标签范围。

[PE1]display segment-routing IPv6 local-sid end-dt4 (示意图, 例子)

Local SID forwarding table (End.DT4)

Total SIDs: 2

SID : 10::31:8000:0:0/80
Function type : End.DT4 Flavor : PSP
VPN instance : Public instance Allocation type: Dynamic //公网分配一个 End.DT4 SID

Network type : MPLS L3VPN
Locator name : pe1
Owner : BGP State : Active
Create Time : Apr 19 11:42:19.576 2021
SID : 10::31:8000:3:0/80
Function type : End.DT4 Flavor : PSP
VPN instance : ADWAN-VPN1 Allocation type: Dynamic
Network type : EVPN L3VPN
Locator name : pe1
Owner : BGP State : Active
Create Time : May 08 11:11:37.317 2021

电子政务外网骨干网 Locator 设计原则如下:

广域网中每台设备的 Locator 使用一个 96 掩码的网段的 IPv6 地址:

在剩余的 32bits 中, 前 16bits 为 Function, 后 16bits 为 args:

在 16bits 的 Function 中, 将前 4 个 bits 全为 0 设置为静态分配的 Function 范围, 共 12 个 bits 可配置, 4096 个静态 SID 可用:

在 16bits 的 Function 中, 前 1 个 bits 不全为 0 设置为动态分配的 SID 范围, 共可以支持 65536 个 SID 作为动态 SID:

策略作用域规划

该功能定义了应用的起始设备, 控制器会根据策略作用域在相应设备上下发隧道等配置。

默认情况下是全网自动识别。现根据自己的需求, 来定义其中的子网网络范围。

使用自定义策略作用域, 可分为以下几类:

1. 一对一: 源设备为一台设备, 目标设备为一台设备。
2. 一对多: 源设备为一台设备, 目标设备为多台设备。
3. 多对多: 源设备为多台设备, 目标设备为多台设备。

调研方式：根据业务始发路由器和目标路由器配置，PE 设备一般为主备方式，配置时两台 PE 设备同时选择，当 PE 失效，流量从备 PE 始发时仍有效。

应用需求（SLA 需求）

ADWAN 控制器为用户提供 8 级 SLA（SLA7、SLA6、SLA5、SLA4、SLA3、SLA2、SLA1 和 SLA0），不同 SLA 承诺不同链路质量。ADWAN 控制器预定义 8 个 SLA 服务等级链路质量参数，可根据实际需求自定义 SLA 服务等级的链路质量参数。设备加入到 ADWAN 管理域中，ADWAN 初始化网络拓扑后，下发 NQA（UDP-jitter）配置探测链路质量，探测报文承载在 SRv6 网络中，并按照 SLA 对应的 DSCP 优先级进行转发。控制器根据设备返回的链路质量信息为用户选择满足应用 SLA 需求的路径转发流量。

SLA 策略可包括优先级、带宽、时延、抖动、丢包、时间段、链路/节点偏好等，满足业务差异化保障需求。

SLA 分级规划

控制器设计 SLA 共分为 8 级，6 级与 7 级为协议使用不承载业务，优先级越高对应业务级别越高，高 SLA 等级的应用组可优先抢占到网络资源，所以能够对不同业务对应优先级进行区分保障。

SLA 级别分类如下：

SLA 级别	名称	带宽	时延	抖动	丢包	DSCP
SLA7	SLA7	100	≤10	≤1	≤1	48
SLA6	SLA6	100	≤10	≤1	≤1	46
SLA5	SLA5	100	≤10	≤1	≤1	44
SLA4	SLA4	100	≤10	≤1	≤1	42
SLA3	SLA3	100	≤10	≤1	≤1	40
SLA2	SLA2	100	≤10	≤1	≤1	38
SLA1	SLA1	100	≤10	≤1	≤1	36
SLA0	SLA0	100	≤10	≤1	≤1	34

SLA 调优规划

由于不同 SLA 定义了不同的链路质量参数，控制器现有默认参数可能不适用现网，所以需要调对 SLA 参数进行优化。

现网默认参数设计如下：

SLA 优先级	延迟 (ms)	丢包率 (%)	抖动 (ms)	DSCP
5	≤50	≤0.05	≤3	48
4	≤100	≤0.05	≤5	46
3	≤150	≤0.10	≤5	32

2	≤300	≤0.15	≤5	18
	≤500	≤0.25	≤10	10
	≤1000	≤0.5	≤50	0

调优方案如下：

使网络运行一段时间后在控制器上导出链路质量报表，根据报表参数计算出平均值后重新定义各参数。

观察控制器中日志，若某应用在一段时间内进行频繁调度，则需要对该 SLA 参数进行调大。

观察控制器中日志以及相关应用组人员反馈，若某应用（如视频应用）出现延迟卡顿情况，但是未进行优质链路调度，则进行相关 SLA 参数调小。

数据流引流

电子政务外网骨干网 ADWAN 使用 SRv6 TE Policy(调度隧道)承载业务，采用 SRv6 TE Policy CBTS (Class-based Tunnel Selection, 基于服务类型的隧道选择) 隧道选择技术。利用 CBTS 技术，可通过 IP 五元组、DSCP、VNI 等任意组合方式来进行精细化流分类，如某目的端口、某源网段都可以用来标识业务，从而为不同的业务提供不同的转发服务。

其中 CBTS 关键参数为 Service-class 值，CBTS 利用 Service-class 值关联应用组与隧道，指导不同应用组流量进入不同隧道。其中 Service-class 值范围为 0-127 (0 为默认隧道使用，禁止手动分配)。Service-class 值按照表格从前至后使用，每个设备最多支持 127 个。

使用中需合并部分相同优先级应用共用一个应用组，防止 Service-class 值资源不足。

现规划 Service-class 值如下：

SLA 级别	Service-class 值范围
5	101-127
4	81-100
3	61-80
2	41-60
1	21-40
0	1-20

QoS 部署

概述

QoS 即服务质量，主要是为了避免以下问题：

高速链路汇聚的并发数据流，转到低速链路上传输，在低速接口转发时形成瞬时转发瓶颈，形成端口阻塞，引发传输时延、抖动甚至队列丢包等问题，对实时业务、语音、视频等丢包、时延、抖动敏感的多媒体业务造成影响。

多个接口流量并发到单个相同速率的接口造成的拥塞。

因此，QoS 的设计应该根据各种业务的特点来对网络资源进行合理的规划和分配，从而使网络资源得到高效利用。

对于部分已存在 QoS 配置控制器不支持（GTS），保留原有配置即可。

应用保障部署

CBQ 为用户提供了定义类的支持，为每个用户定义类分配一个单独的 FIFO 预留队列，用来缓冲同一类的数据。在网络拥塞时，CBQ 对报文根据用户定义类规则进行匹配，并使其进入相应的队列，在入队列之前必须进行拥塞避免机制和带宽限制的检查。在报文出队列时，加权公平调度每个类对应的队列中的报文。

CBQ 包括以下队列：

- LLQ 队列：即 EF 队列，为实时业务报文提供严格优先发送服务。在使用 LLQ 时将会为每个优先类指定可用最大带宽，该带宽值用于拥塞发生时监管流量。如果拥塞未发生，优先类允许使用超过分配的带宽。如果拥塞发生，优先类超过分配带宽的数据包将被丢弃。

- BQ 队列：即 AF 队列。为 AF 业务提供严格、精确的带宽保证，并且保证各类 AF 业务之间按一定的比例关系进行队列调度

为了使隧道流量能够进行 CBQ 保障，需要对应用策略 SLA 中 DSCP 值进行修改，匹配现网 DSCP 值，即可对不同应用进行不同保障。

链路限速部署（LR）

为了防止业务流量被运营商链路丢弃需要配置链路限速，限速值根据运营商链路带宽值配置即可，配置完成后控制器会在设备接口下发 LR 配置。由于链路在控制器上查看是双向，所以链路限速双向配置限速，限速值与运营商分配带宽值保持一致。此处现网已配置相应限速，保留原有配置即可。

备注：控制器无法配置 CBS 值，建议手动配置 LR。

链路参数部署（Bandwidth）

应用保障的占比是基于接口带宽，在运营商链路上实际可用带宽比接口带宽小（WAN 口限速的情况下），则需要配置带宽为实际可用带宽（Bandwidth），此外应用保障队列默认只使用

80%的带宽，现网中队列使用全部带宽，解除 80%使用限制，配置为 100%。此处现网已配置，保留原有配置即可。

在控制面上，将链路带宽值为运营商分配带宽值。控制器根据此带宽值算出链路剩余真实可用带宽，可对应用进行调度保障。

具体算法如下：

剩余可用带宽=Bandwith-应用已用带宽。

NQA 获取链路质量信息

应用调度时参考物理链路质量，方案中链路质量由延时，抖动和丢包率作为参考，通过 NQA 技术探测物理链路的链路质量。



因接口 QoS 队列存在，不同优先级的应用在链路上实际传输的质量不同。NQA 探测为了和应用流量优先级一致，所以在构建 NQA 探测报文时，会有以下三种探测模式：

8 级 SLA 探测：

高优先级 (SLA 4~7) 进行高频探测，10 秒内在监控拓扑呈现质量信息；低优先级 (SLA 0~3) 进行低频探测，30 秒内在监控拓扑呈现质量信息。

5 级 SLA 探测：

高优先级（SLA 4~5）进行高频探测，10 秒内在监控拓扑呈现质量信息；低优先级（SLA 0~3）进行低频探测，30 秒内在监控拓扑呈现质量信息。

默认情况下，设备每 1 分钟进行一次探测，10 秒内呈现质量信息。

12.1.5.11.1 设备安全设置

协议安全

OSPFv2 和 OSPFv3 启用基于区域认证，BGP 邻居基于 MD5 认证。

MACsec 链路安全

MACsec（Media Access Control Security，MAC 安全）定义了基于 IEEE 802 局域网络的数据安全通信的方法。MACsec 可为用户提供安全的 MAC 层数据发送和接收服务，包括用户数据加密、数据帧完整性检查及数据源真实性校验。MACsec 通常与 802.1X 认证框架配合使用，通过使用 MKA（MACsec Key Agreement，MACsec 密钥协商）协议协商生成的密钥对已认证的用户数据进行加密和完整性检查，避免端口处理未认证设备的报文或者经过篡改的报文。

安全基线项目名称	面向设备模式 MACsec 配置组网
安全基线级别	可选
安全基线项说明	设备间的 MACsec 协议交互过程无身份认证阶段，直接从会话协商阶段开始。设备之间使用配置的预共享密钥开始协商会话，会话协商结束后开始安全通信。该模式下，会话协商、安全通信和会话终止的具体机制与面向客户端模式的 MACsec 协议交互过程类似。但密钥服务器的选举方式不同，面向设备模式中优先级较高的端口将被选举为密钥服务器，负责生成和分发 SAK。
检测操作步骤	<pre><DeviceA> system-view # 在接口 GigabitEthernet1/0/1 上配置期望进行 MACsec 保护。 [DeviceA] interface gigabitethernet 1/0/1 [DeviceA-GigabitEthernet1/0/1] macsec desire</pre>

	# 配置 MKA 密钥服务器的优先级为 5。（本例中，Device A 作为密钥服务器，所以配置的 Device A 的优先级要比 Device B 的优先级高 <pre>[DeviceA-GigabitEthernet1/0/1] mka priority 5</pre> # 配置预共享密钥的名称为 E9AC，预共享密钥为明文 09DB3EF1。 <pre>[DeviceA-GigabitEthernet1/0/1] mka psk ckn E9AC cak simple 09DB3EF1</pre> # 配置 MACsec 加密偏移量为 30。 <pre>[DeviceA-GigabitEthernet1/0/1] macsec confidentiality-offset 30</pre> # 开启 MACsec 重播保护功能。 <pre>[DeviceA-GigabitEthernet1/0/1] macsec replay-protection enable</pre> # 配置 MACsec 重播保护窗口大小为 100。 <pre>[DeviceA-GigabitEthernet1/0/1] macsec replay-protection window-size 100</pre> # 配置严格的 MACsec 校验模式。 <pre>[DeviceA-GigabitEthernet1/0/1] macsec validation mode strict</pre> # 开启 MKA 协议。 <pre>[DeviceA-GigabitEthernet1/0/1] mka enable</pre> <pre>[DeviceA-GigabitEthernet1/0/1] quit</pre> 配置 Device B <pre><DeviceB> system-view</pre> # 进入 GigabitEthernet1/0/1 接口视图。 <pre>[DeviceB] interface gigabitethernet 1/0/1</pre> # 配置期望进行 MACsec 保护。 <pre>[DeviceB-GigabitEthernet1/0/1] macsec desire</pre> # 配置 MKA 密钥服务器的优先级为 10。
---	---

	<pre>[DeviceB-GigabitEthernet1/0/1] mka priority 10 # 配置预共享密钥的名称为 E9AC，预共享密钥为明文 09DB3EF1。 [DeviceB-GigabitEthernet1/0/1] mka psk ckn E9AC cak simple 09DB3EF1 # 配置 MACsec 加密偏移量为 30。 [DeviceB-GigabitEthernet1/0/1] macsec confidentiality-offset 30 # 开启 MACsec 重播保护功能。 [DeviceB-GigabitEthernet1/0/1] macsec replay-protection enable # 配置 MACsec 重播保护窗口大小为 100。 [DeviceB-GigabitEthernet1/0/1] macsec replay-protection window-size 100 # 配置严格的 MACsec 校验模式。 [DeviceB-GigabitEthernet1/0/1] macsec validation mode strict # 开启 MKA 协议。 [DeviceB-GigabitEthernet1/0/1] mka enable [DeviceB-GigabitEthernet1/0/1] quit</pre>
备注	无

帐号管理、认证授权安全要求

账户安全

配置默认安全级别

安全基线 项目名称	配置默认级别安全基线要求项
安全基线 级别	必选项

安全基线 项目名称	命令级别其分为访问、监控、系统、管理 4 个级别，分别对应标识 0、1、2、3。配置登录默认级别为访问级（0-VISIT）
检测操作 步骤	1、参考配置操作 <pre> user-interface aux 1/0 authentication-mode password user privilege level 0 set authentication password cipher xxx user-interface vty 0 15 authentication-mode password\或 authentication-mode scheme user privilege level 0 set authentication password cipher xxx </pre> 2、补充说明 无。
备注	无

口令安全

密码认证登录

安全基线 项目名称	密码认证登录安全基线要求项
安全基线 级别	必选项
安全基线 项说明	通过控制台和远程终端，需要密码才能登录。口令长度至少 8 位，并包括数字、小写字母、大写字母和特殊符号四类中至少两类。且 5 次以内不得设置相同的口令。密码应至少每 90 天进行更换。
检测操作 步骤	1、参考配置操作 <pre> user-interface aux 1/0 authentication-mode password user privilege level 0 set authentication password cipher xxx </pre>

	<pre> user-interface vty 0 15 authentication-mode password // // authentication-mode scheme user privilege level 0 set authentication password cipher xxx 2、补充说明 无。 </pre>
备注	

设置访问级别切换密码

安全基线 项目名称	设置访问级别切换密码安全基线要求项
安全基线 级别	必选项
安全基线 项说明	用户可以无条件切换到比当前低的用户级别，但是当使用 AUX 或 VTY 用户界面登录，并且从低级别往高级别切换时，需要输入级别切换密码（级别切换密码可以通过 <code>super password</code> 命令设置）。如果输入的密码错误或者没有配置级别切换密码，切换操作失败。因此，在进行切换操作前，请先配置级别切换密码。
检测操作 步骤	1、参考配置操作 <pre> <Sysname> system-view [Sysname] super password level 1 cipher password1 [Sysname] super password level 2 cipher password2 [Sysname] super password level 3 cipher password3 </pre> 2、补充说明 无。
备注	无

加密口令

安全基线 项目名称	加密口令安全基线要求项
安全基线 级别	必选项
安全基线 项说明	静态口令必须使用不可逆加密算法加密后保存于配置文件中。
检测操作 步骤	1、参考配置操作 <pre> user-interface aux 1/0 user privilege level 0 set authentication password cipher xxx user-interface vty 0 15 user privilege level 0 set authentication password cipher xxx super password level 1 cipher password1 super password level 2 cipher password2 super password level 3 cipher password3 </pre>
备注	无

日志安全要求

配置远程日志服务器

安全基线 项目名称	配置远程日志服务器安全基线要求项
安全基线 级别	可选项
安全基线 项说明	设备应配置远程日志功能。所有设备日志均能通过远程日志功能传输到日志服务器。设备应配置至少一种通用的远程标准日志接口，如 SYSLOG 等。

检测操作 步骤	参考配置操作 [Sysname] info-center enable [Sysname] info-center loghost xxxxx channel loghost
备注	无

设备远程访问安全要求

使用 SSH 加密管理

安全基线 项目名称	使用 SSH 加密管理安全基线要求项
安全基线 级别	必选项
安全基线 项说明	对于使用 IP 协议进行远程维护的设备，设备应配置使用 SSH 等加密协议，关闭 TELNET 协议。
检测操作 步骤	参考配置操作 # 设置用户界面 VTY 0 到 VTY 15 支持 SSH 协议。 <pre> <Sysname> system-view [Sysname] user-interface vty 0 15 [Sysname-ui-vty0-4] authentication-mode scheme [Sysname-ui-vty0-4] protocol inbound ssh </pre> 2、补充说明 无。
备注	无

系统远程管理服务只允许特定地址访问

安全基线 项目名称	系统远程管理服务只允许特定地址访问安全基线要求项
安全基线 级别	必选项

安全基线 项目名称	系统远程管理服务 SSH 默认可以接受任何地址的连接，出于安全考虑，应该只允许特定地址访问。
检测操作 步骤	1、参考配置操作 <pre> AcF number 2000 rule 1 permit source 192.168.0.0 0.0.255.255 User-interface vty 0 4 acl 2000 inbound </pre> 2、补充说明 无。
备注	无

SNMP 安全要求

修改 SNMP 默认通行字

安全基线 项目名称	修改 SNMP 默认通行字安全基线要求项
安全基线 级别	必选项
安全基线 项说明	系统应修改 SNMP 的 Community 默认通行字，通行字应符合口令强度要求。
检测操作 步骤	1、参考配置操作 <pre> snmp-agent community read xxx snmp-agent community write xxxx </pre> 2、补充说明 无。
备注	无

使用 SNMPV2 或以上版本

安全基线 项目名称	SNMP 版本安全基线要求项
安全基线	必选项

级别	
安全基线项目说明	配置为 SNMPV2 或以上版本。
检测操作步骤	1、参考配置操作 snmp-agent sys-info version v3 2、补充说明 无。
备注	无

SNMP 访问控制

安全基线项目名称	SNMP 访问控制安全基线要求项
安全基线级别	必选项
安全基线项说明	设置 SNMP 访问安全限制, 只允许特定主机通过 SNMP 访问网络设备。
检测操作步骤	1、参考配置操作 snmp-agent community read XXXX01 acl 2000 2、补充说明 无。
备注	无

其他安全要求

关闭未使用的端口

安全基线项目名称	关闭未使用的端口安全基线要求项
安全基线级别	可选项
安全基线项说明	关闭未使用的端口。

检测操作 步骤	1、参考配置操作 [Sysname-Ethernet3/0/0]shutdown 补充说明 无。
基线符合性判定依据	判定条件 未使用端口状态为 admin down。 参考检测操作 Display interface 补充说明 无。
备注	无

帐号登录超时

安全基线项目名称	帐号登录超时安全基线要求项
安全基线级别	可选项
安全基线项说明	配置定时帐号自动登出，登出后用户需再次登录才能进入系统。设置超时时间为 5 分钟。
检测操作步骤	参考配置操作 设置超时时间为 5 分钟(缺省为 10 分钟) <Sysname> system-view [Sysname] user-interface console 1/0 //Or user-interface aux 1/0 [Sysname-ui-console0] idle-timeout 5 0 2、补充说明 无。
备注	无

关闭不需要的服务

安全基线项	关闭不需要的服务安全基线要求项
安全基线级别	必选
安全基线项说明	关闭网络设备不必要的服务，比如 FTP、TFTP 服务等。
检测操作步骤	1、参考配置操作 undo ftp server 2、补充说明 无。
备注	无

12.1.5.12 施工现场管理

（一）设备安装

（1）设备机架安装

机架安装位置应符合施工图平面设计要求，根据设计图纸尺寸，画线定位。

需加固底座或机帽的，宽和厚的尺寸应与机架尺寸相符，总体高度应与机房整体机架高度一致，漆色同机架色泽。

底脚螺丝安装数量应符合机架底角孔洞数量，机架垂直偏差不大于机架高度的 1‰。

调整机架垂直可在机架底角处置放金属片，最多只能垫机架的三个底角。一列有多个机架，先安装列头首架，然后依次安装其余各机架，整列机架允许偏差为 3mm，机架之间的缝隙上下均匀一致。

安装机门要求位置正确，开启灵活。机架、列架标志正确、清晰、齐全。

（2）子架安装

子架位置符合设计要求，安装应牢固，保证子架接线插接件的电气接触良好。

（二）设备缆线及电源线的布放

（1）线缆布放原则

电源线、信号线与锁线等应分离布放，电源线、地线也应分开布放、绑扎，绑扎时应使用

同色的色扎带。

线缆在走线架上应平直，不得交叉。从走线架下线应垂直于所接机柜。

同一束内不同线缆的垂直部分的扎带在绑扎时应尽量保持在同一水平线上。

使用扎带绑扎时，扎带扣应朝向操作侧背面，扎带扣修剪平齐。

(2) 敷设电源线

电源线、信号线及铜、铝接线端子、螺栓、螺、母的规定、型号必须符合施工图设计的规定。

电源线应外皮完整，必须是整段材料，中间不得有接头和急转弯。直流电源线、交流电源线应分开敷设，避免在同一线束内。

电源线应走线方便、整齐、美观，与设备连线越短越好，同时不应妨碍今后的维护工作。

直流电源线、交流电源线、信号线必须分开布放，避免在同一线束内。其中直流电源线正极外皮颜色应为红色，负极外皮颜色应为蓝色。电源线敷设时，应保持其平直、整齐，转弯应均匀圆滑，铠装电力电缆弯曲半径不得小于外径的 12 倍，塑包线和胶皮电缆转弯半径不得小于外径的 6 倍。绑扎松紧适度，间距均匀。线扣多余部分应齐根剪掉，剪后不扎于，线扣头放在隐蔽处。

机房布线、架间连线及各部件连线应正确无误，接触良好，焊接光滑。不得碰地、短路、断路。

(3) 光纤布放

槽道内光纤应顺直、不扭绞，拐弯处曲率半径不小于光缆直径的 20 倍。

槽道内光纤应加套管或线槽进行保护，无套管保护处用扎带绑扎，但不宜过紧。

光纤两端必须按规范和客户要求粘贴标签

(三) 电源线接线端子制作

电源线接线端子的制作和锁头制作一样的重要，如果制作不规范，不把电源线插到底再压接，不用专用的压线钳压接端子等，都会可能发生接线端子和线缆脱接的事故，一旦脱节轻则会导致基站断电，重则能引起火灾，所以接线端子的制作规范也尤为重要。

(四) 设备的通电检查

(1) 通电前的检查

1. 卸下架内保险和分保险，检查架内电源线连接是否正确、牢固无松动。
2. 机架电源输入端应检查电源电压、极性、相序。

3. 机架和机框内部应清洁, 查看有无焊锡、芯线头、脱落的紧固件或其他异物。

4. 架内断线、短路、开关、旋钮、继电器、印刷电路板齐全, 插接牢固。

5. 开关、旋钮、继电器等应符合说明书要求。

6. 各线器、连接电缆插头连接应正确、牢固、可靠。

7. 接线端子插接应正确无误。

(2) 通电检查

1. 先接通机架总保险, 观察有无异样情况。

2. 开启主电源开关, 逐级接通分保险通过眼看、耳听、鼻闻注意有无异味、冒烟、打火和不正常的声音等现象。

3. 电源开启后预热一小時无任何异常现象后, 开启高压电源, 加上高压应保持不跳闸。

4. 各种信号灯、电表指示应符合要求, 如有异常, 应关机检查。

5. 个别单盘有问题, 应换盘试验, 确认故障原因。

6. 加电检查时, 应戴防静电手套, 手套与机架接地点接触良好。

(五) 设备接地

(1) 直流电源工作地应从接地汇集线上引入。

(2) 所有交直流配电设备的机壳应从接地汇集线上引入保护接地线。交流配电屏中的中性线汇集排应与机架绝缘。严禁采用中性线作交流保护地线。

(3) 通信设备机壳应作保护接地。

(4) 机房内空调等金属设施应按工程设计要求引接保护地线。

(5) 机房内接地线的布置方式, 可采取辐射式或平面型。机房内所有通信设备除从接地汇集线上就近引接地线外, 不得通过安装力 H 固螺栓与建筑钢筋相碰而自然形成的电气连通。

(6) 各类需要接地的设备与接地汇集线间的连线, 其截面应根据通过的最大负荷电流确定一般宜采用 35-95 平的绝缘铜线, 严禁使用裸导线布放。

12.1.6 人员培训

12.1.6.1 培训目标

培训是一个非常重要的环节, 通过培训使得培训后的人员能了解和掌握系统结构和工作原理、设备性能、设备操作, 使得这些操作人员能担负起网络及设备的日常操作使用和保养工作,

保障设备长期可靠稳定的运行。

要使网络及设备管理人员能够熟练、高效的操作设备，发挥网络及设备的最佳使用效果，还必须要对网络及设备使用人员进行操作培训。

12.1.6.2 培训内容

(1) 网络工作原理：包括各种涉及网络的工作原理，技术标准、技术细节及各项注意事项等。

(2) 设备的使用方法：参加培训的人员应了解设备的各种设置、参数及指示灯的含义等。

(3) 参数配置：参加培训人员达到熟练掌握 MSTP、VPDN 及裸光纤网络设备的管理，配置系统参数，学会分析排查设备的一般性故障。

(4) 设备的操作方法：参加培训的人员应熟练掌握设备软硬件的调试方法、各项功能操作应用。

(5) 日常的维护保养知识：介绍系统设备软硬件的日常养护知识确保设备得到正确的养护方法，延长设备寿命。

(6) 安全及其它注意事项。

(7) 电子政务外网使用培训：根据用户的具体情况，对用户提供商直一级单位电子政务外网接入服务的网络系统维护管理、系统操作使用等方面的培训。具体培训课程、时间、对象，根据用户的安排与用户协商确定。

培训课程一：

课程编号	课程名称
1	路由器的产品架构
2	网络管理平台及功能组件产品概述
3	路由器的基础配置指导（CLI 配置、设备登录、FTP 与 TFTP、软件升级等）
4	二层以太网交换技术原理及配置指导（MAC、VLAN、二层转发原理、STP、链路聚合等）
5	三层技术原理及配置指导（ARP、地址配置、IP 转发原理、NAT、DHCP、DNS、静态路由等）

6	网络管理和监控技术原理及配置指导（NTP、SNMP、镜像等）
	网络管理平台的安装指导、设备管理维护及日常维护

培训课程二：

课程编号	课程名称
1	路由器的产品架构
2	网络管理平台及功能组件产品概述
3	二层广域网接入技术原理及配置指导（IPoE、L2TP、PPPoE）
4	三层高级路由技术原理及配置指导（OSPF、BGP）
5	网络管理和监控技术原理及配置指导（NTP、SNMP、镜像等）
6	网络管理平台的安装指导、设备管理维护及日常维护
7	常用认证技术原理及配置指导（802.1x、Portal）；常用组件配置及维护（EAD）

培训课程三：

课程编号	课程名称
1	路由器的产品架构
2	网络管理平台及功能组件产品概述
3	二层广域网接入技术原理及配置指导（IPoE、L2TP、PPPoE）
4	三层高级路由技术原理及配置指导（OSPF、BGP）
5	MPLS VPN 技术原理及配置指导
6	网络管理平台的安装指导、设备管理维护及日常维护
7	常用认证技术原理及配置指导（802.1x、Portal） 常用组件配置及维护（EAD、MPLS VPN 等）
8	组网强化与网络排错指导

12.1.6.2.1 业务操作培训

培训对象：针对市直单位电子政务外网接入服务的网络系统项目建设单位、使用单位、运维单位等在内的相关领导及核心业务人员；这部分用户是整个系统的关键用户，他们直接担负

着项目推动和配合开展实施工作，可以说整个项目的成败，有很大程度将依赖这部分用户的参与程度和成效。因此，这部分用户的培训也将是整个项目进行培训的重点。

这部分培训的主要内容为系统框架介绍及理念介绍，系统业务流程介绍及系统使用配套管理制度探讨等。

培训课程名称	业务操作培训		
培训地点	待定		
培训对象	相关领导及核心业务人员		
培训人数	10—15 人（双方协定）		
人员要求	熟悉业务流程及相关制度，具备一定的计算机、网络相关知识		
培训目的	使核心业务人员和关键用户掌握产品业务功能的使用及熟悉项目实施方案		
课程概述	系统业务流程介绍、实施方案以及相关业务问题及系统使用配套管理制度探讨等		
培训周期	培训内容	培训资料	讲师
2 课时	系统框架介绍及理念介绍，业务流程介绍及系统配套管理制度探讨等	1、《电子政务外网系统框架介绍及理念培训》 2、《电子政务外网系统管理功能应用培训》 3、《常见问题及沟通方法培训》	高级实施顾问

12.1.6.2.2 系统管理及维护培训

培训对象：针对市直一级单位电子政务外网接入服务的网络系统项目建设单位、使用单位、运维单位等在内的系统管理员和技术维护人员，系统管理员是一个信息化系统持续稳定运行的基础，承担着日常运行环境维护，数据备份，技术问题沟通等职责，对该部分用户的培训将主要侧重于技术层面，同时兼顾部分业务流程的讲解。

主要培训内容系统架构、产品功能说明、系统日志及维护操作、系统安装、数据恢复与备份、日常故障维护等。



培训名称	系统管理及维护培训		
培训地点	待定		
培训对象	系统管理员、核心技术人员		
培训人数	3—5 人（双方协定）		
人员要求	对网络、数据库、服务器等有专业的知识		
培训目的	使系统管理员了解系统的运行环境以及熟悉系统日常维护内容。		
课程概述	使系统管理员了解系统的运行环境以及熟悉系统日常维护内容。		
培训周期	培训内容	培训资料	讲师
2 课时	系统安装及调试，数据备份与恢复、系统管理功能应用、常见问题及沟通方法、系统日志及维护操作、日常故障维护等	1、《电子政务外网相关产品安装及调试培训》 2、《电子政务外网系统管理功能应用培训》 3、《常见问题及沟通方法培训》	高级技术顾问

12.1.6.2.3 业务流程及产品操作培训

培训对象：针对市直一级单位电子政务外网接入服务的网络系统项目建设单位、使用单位、运维单位等在内所有系统操作人员。这部分用户是最终使用人员。在系统上线之前，应针对每个岗位的具体业务制定有针对性的培训方案，并结合各岗位的实际业务进行培训。

这部分培训的主要内容为软件平台业务流程及功能使用介绍。

培训名称	业务流程及产品操作培训
培训地点	待定
培训对象	系统最终用户
人员要求	具备一定的计算机及网络相关的知识、技能。
培训目的	使操作用户掌握系统功能的使用

	系统业务流程及功能使用介绍		
	培训内容	培训资料	讲师
	相关系统、产品的业务流程及功能使用介绍	1、《产品手册》 (含产品基本介绍、功能介绍、操作方法等)	实施顾问

12.1.6.3 培训方法

本项目涉及硬件、软件和相应的光电技术、通信技术、计算机技术等，因此采用软件和硬件相结合的培训方法，使得操作人员在熟练使用的同时，能对系统进行简单而有效的维护工作。

12.1.6.3.1 书面讲解

根据我方提供的培训教材，如文档、PPT 等由我方的培训工程师向客户指定的培训人员讲授网络工作原理、设备工作原理和简单的故障排查。培训资料参训人员人手一册。

12.1.6.3.2 实际操作

领会基本原理后，在我方培训工程师的讲解和指导下，带领客户指定的培训人员到设备安装现场进行实际操作，熟悉设备性能、指示灯显示及故障排查等。

12.1.6.3.3 答疑

在上述两阶段的培训过程中及完成后，由我方的培训工程师进行统一解答培训人员的相关问题。

12.1.6.4 培训组织方式

本项目的培训组织方式主要包括现场培训、远程视频会议培训、现场实操。

12.1.6.4.1 现场培训

资深技术工程师在产品的安装调试过程中进行，直接针对采购人工程师进行现场教学，即

时指导，增加用户的学习机会，使之能更形象地了解产品，直接更迅速地掌握各项知识和技能。

12.1.6.2 远程视频会议培训

考虑到用户对各种产品需要全方位的了解，根据用户的需求及项目的实际情况，提供丰富多样的培训方式。通过电视电话会议对技术人员进行远程培训。

远程培训可以提供语音、视频、应用共享、文档共享、文字交流等多种培训手段和辅助工具。在整个培训过程中，我方可以方便的通过各种表现方式来进行讲授，并可随时的与用户之间进行沟通和补充。

我公司将编写详细的使用说明书，提供给客户的应用人员作为学习和培训教材。另外，在必要的时候，公司可以委派技术人员进行现场技术指导和应用技术讲座，以满足客户方人员的需要。

12.1.6.4.3 现场实操

设备操作培训是我公司提供的服务设备，对设备对应的运维人员开展培训。包括设备的调试，设备的参数设置、基本使用和功能维护等内容。

12.1.6.5 培训检验评估

培训结束，可以针对客户的需求对培训的结果进行检验，检验方式可以通过实际操作和理论考试两种形式进行。公司将为客户的考试提供相应的技术支持。

12.1.6.6 具体计划安排

服务期内可组织不少于 3 次培训，计划安排如下，具体根据实际需求我方可进行相应调整，确保满足客户需要。

序号	培训地点	培训课程	培训内容	培训对象	培训时间
1	培训中心	设备的原理和技术性能、操作维护方法、安装调试、	网络结构及工作原理 设备的配置和性	市直重点单位的相关人员	1 天

3		排除故障等，提供 培训教材（中文） 培训课程计划	能描述		
			设备的运行和操作使用		
			设备日常维护、常见故障处理及注意事项		
4	维护 现场	设备日常维护、常见故障处理及注意事项	设备日常维护、常见故障处理及注意事项	市直重点单位的相关人员	1 天
5	培训结果检验		通过	合格	
			重新培训	不合格	

12.1.7政策依据

- (1)《国务院关于加强数字政府建设的指导意见》（国发〔2022〕14号）
- (2)《国家发展改革委关于印发〈“十四五”推进国家政务信息化规划〉的通知》（发改高技〔2021〕1898号）
- (3)中央网络安全和信息化委员会印发的《“十四五”国家信息化规划》
- (4)《国务院办公厅关于印发全国一体化政务大数据体系建设指南的通知》（国办函〔2022〕102号）
- (5)《国务院办公厅关于加快推进政务服务“跨省通办”的指导意见》（国办发〔2020〕35号）
- (6)《中央网信办、国家发展改革委、工信部关于加快推进互联网协议第六版（IPv6）规模部署和应用工作的通知》（中网办发〔2021〕15号）
- (7)《工业和信息化部 中央网络安全和信息化委员会办公室关于印发〈IPv6流量提升三年专项行动计划（2021-2023年）〉的通知》（工信部联通信〔2021〕84号）
- (8)《中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要》
- (9)《河南省人民政府关于印发河南省“十四五”数字经济和信息化发展规划的通知》（豫政〔2021〕51号）

(10)《河南省人民政府关于印发河南省加强数字政府建设实施方案（2023—2025 年）的通知》（豫政〔2023〕45 号）

(11)《河南省人民政府办公厅关于印发河南省建立健全政务数据共享协调机制加快推进数据有序共享实施方案的通知》（豫政办〔2022〕62 号）

(12)《河南省人民政府办公厅关于加快推进新型智慧城市建设的指导意见》（豫政办〔2020〕27 号）

(13)《河南省推进互联网协议第六版（IPv6）规模部署实施计划》

(14)《濮阳市国民经济和社会发展第十四个五年发展规划和 2035 年远景发展目标纲要》

12.1.8 技术标准

(1)《中华人民共和国网络安全法》

(2)《中华人民共和国个人信息保护法》

(3)《中华人民共和国密码法》；

(4)《中华人民共和国数据安全法》；

(5)《关键信息基础设施安全保护条例》（国令第 745 号）；

(6)《电子政务外网安全接入技术规范》（DB34/T 4283-2022）

(7)《国家电子政务外网 IPv6 地址规划》（GW0209—2019）

(8)《信息安全技术 网络安全等级保护测评要求》（GB/T 28448—2019）；

(9)《国家政务服务平台安全接入检测要求》（CO115-2018）；

(10)《政务网络安全监测平台总体技术要求》（TC11A 005-2019）；

(11)《政务网络安全监测平台数据总线结构规范》（T/CI1A 007—2020）；

(12)《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）；

(13)《信息安全技术 网络安全等级保护安全设计技术要求》（GB/T 25070-2019）；

(14)《信息安全技术 网络安全等级保护实施指南》（GB/T 25058-2019）；

(15)《信息安全技术 网络安全监测基本要求与实施指南》（BG/T 36635-2018）；

(16)《信息安全技术 电子政务移动办公系统安全技术规范》（GB/T 35282-2017）；

(17)《国家电子政务外网信息安全标准体系框架》（GW0101-2014）；

(18)《国家电子政务外网信息安全标准化工作规范》（GW0102-2014）；

- (19)《接入政务外网的局域网安全技术规范》（GW0206-2014）；
- (20)《国家电子政务外网安全接入平台技术规范》（GW0202-2014）；
- (21)《国家电子政务外网安全管理系统技术要求与接口规范》（GW0204-2014）；
- (22)《国家电子政务外网安全等级保护实施指南》（GW0104-2014）；
- (23)《国家电子政务外网跨网数据安全交换技术要求与实施指南》（GW0205-2014）；
- (24)《国家电子政务外网安全监测体系技术规范与实施指南》（GW0203-2014）。

12.1.9网络安全要求

我公司对政务外网网络安全负责，所建设政务外网符合三级等保要求，并通过国家三级等保认证。我公司采取必要的技术和管理措施，确保政务外网安全。

12.1.10采购内容及参数

名称	参数要求	单位	数量	
电子政务网	1、单条宽带 100M； 2、速率上行、下行对称； 3、所提供的物理链接光纤信号衰减不超过 20db； 4、采用专线直连的方式。	条	第一标包	135

12.1.11建设工期及进度

合同签订后，在 15 天内完成。

12.1.12租赁期限

濮阳市行政审批和政务信息管理局濮阳市市直电子政务外网线路租赁服务项目第一标包项目租赁期限为 1 年。

12.2 保密要求

我公司提供的线路及工作人员能够遵守保密原则，保证政务信息不因线路问题外泄。

12.2.1 保密原则

12.2.1.1 数据保密性

确保政府机构在网络上传输和存储的信息和数据受到保护，防止未经授权的访问和泄露。

12.2.1.2 数据完整性

确保政府机构在网络上的信息和数据在传输和存储过程中不被篡改或损坏。

12.2.1.3 可用性

确保政府机构的信息系统和网络能够及时可靠地提供服务，以满足公民和企业的需求。

12.2.1.4 身份验证和访问控制

确保只有经过授权的用户能够访问系统和敏感信息，通过身份验证机制和访问控制策略实现权限分级管理。

12.2.1.5 审计和监控

实时监控系统和网络活动，记录用户操作和系统事件，以便及时发现和应对安全威胁。

12.2.1.6 风险管理

识别、评估和管理电子政务外网的安全风险，采取措施降低风险，保护系统和数据的安全。

12.2.2 保护措施

12.2.2.1 访问控制

只有经过严格授权的人员才能访问政务外网线路和相关设备。授权将根据需要进行分级，以确保只有那些有必要接触政务信息的人员才能获得访问权限。

访问权限将通过强大的身份验证措施进行管理，例如双因素认证、密码策略和访问控制列表（ACL）等。

每位员工都将被分配唯一的身份标识，以便追踪其对政务外网线路和相关设备的访问。这些身份标识将根据员工的职责和需要进行分配，并随时进行审查和更新。

访问权限将根据最小权限原则进行授予，确保员工仅能访问其工作职责所需的信息和功能。权限将根据职位层级和工作功能进行分级，并严格控制。

所有访问政务外网的员工都将被要求通过多因素身份验证进行身份验证，例如使用智能卡、生物识别或令牌等，以确保访问者的身份得到充分确认。

12.2.2.2 加密通信

所有政务信息在传输过程中都将使用最先进的加密技术进行保护，例如传输层安全协议（TLS）或虚拟专用网络（VPN）等。

政务信息在传输过程中将使用 256 位 SSL/TLS 加密进行保护，确保数据在传输过程中的机密性和完整性。

VPN 通道将采用最新的加密算法和安全协议，例如 IPsec（Internet Protocol Security）或 SSL VPN，以提供端到端的加密通信。

加密密钥将进行安全管理，确保只有授权人员才能访问和使用。

12.2.2.3 物理安全

政务外网线路和相关设备将部署在受限制的物理环境中，例如数据中心或安全房间等，以确保未经授权的人员无法接触。

政务外网线路和设备将部署在高度安全的数据中心或专用设施中，这些设施将配备有严格

的物理访问控制措施，包括生物识别、密钥卡和安全警报系统等。

所有服务器和线路设备被锁定在防火、防水和防尘的机架或柜中，并定期进行巡检和维护，以确保其可用性。

12.2.2.4 审计和监控

审计和监控系统将实时监视政务外网的活动，包括访问日志、系统日志和网络流量等，以及对任何异常行为进行自动检测和警报。

系统将记录和存储所有审计数据和日志信息，并采用严格的访问控制措施，以确保其保密性和完整性。

12.2.2.5 培训和意识

所有与政务外网工作相关的员工都将接受定期的保密培训和教育，内容包括但不限于保密政策、数据保护法规、信息安全最佳实践和最新的安全威胁等。

培训将强调员工个人责任和行为准则，以确保他们理解和遵守保密规定。培训将通过多种形式进行，包括在线培训课程、面对面培训会议和安全意识活动等，以确保员工对保密责任和要求的全面理解和认知。

12.2.2.6 保密责任

所有与政务外网工作有关的员工都将被要求签署保密协议，明确承诺遵守保密规定，并清楚了解违反保密规定可能带来的后果，包括可能的法律责任、行政处罚和职业失信等。

12.3 网络连续性方案

12.3.1 业务数据备份

在部署新专线网络之前，对客户现有的业务数据进行全面备份。这包括数据库、应用程序代码、配置文件等关键数据和信息的备份。

备份数据存储在安全的位置，并定期进行更新和验证以确保数据完整性和可用性。

12.3.2 平行测试

在正式部署新网络之前，进行平行测试以验证新网络的功能和性能。这意味着新网络将与现有网络同时运行，以确保它可以正确地处理业务流程和数据。

平行测试包括正常操作模式下的测试，以及紧急情况下的灾难恢复测试，以确保在各种情况下都能保持业务的连续性。

12.3.3 逐步部署

将新网络逐步部署到客户环境中，而不是一次性地替换现有网络。这可以减少潜在的风险，并允许及时发现和解决任何问题。

针对每个阶段的部署，制定详细的计划和时间表，并与客户方共同协商和确认。

12.3.4 备份网络连通性

在部署过程中，确保备份网络连接，以防止由于主网络故障而导致的业务中断。备份网络可以是备用的 ISP 连接、4G/5G 网络连接或者其他可靠的备用通信渠道。

备份网络随时准备就绪，并在主网络发生故障时自动切换以保持业务的连续性。

12.3.5 实时监控和警报

配置实时监控系统，以监视网络的性能、可用性和安全性。这包括监测网络流量、服务器负载、存储空间、数据库响应时间等关键指标。

设置警报机制，当网络出现异常或潜在问题时能够及时通知运维团队，以便他们可以迅速采取措施防止业务中断。

12.3.6 灾难恢复计划

制定详细的灾难恢复计划（DRP），包括恢复关键系统和数据的步骤、责任人员、联系方式等信息。

定期进行灾难恢复演练，以验证 DRP 的有效性，并根据演练结果进行调整和改进。

12.3.7 持续支持和维护

提供持续的技术支持和系统维护服务，包括定期的网络升级、安全补丁、性能优化等。及时响应客户的需求和问题，并提供解决方案以确保业务的连续性和稳定性。

12.4 培训

12.4.1 培训内容

(1) 网络工作原理：包括各种涉及网络的工作原理，技术标准、技术细节及各项注意事项等。

(2) 设备的使用方法：参加培训的人员应了解设备的各种设置、参数及指示灯的含义等。

(3) 参数配置：参加培训人员达到熟练掌握 MSTP、VPDN 及裸光纤网络设备的管理，配置系统参数，学会分析排查设备的一般性故障。

(4) 设备的操作方法：参加培训的人员应熟练掌握设备软硬件的调试方法、各项功能操作应用。

(5) 日常的维护保养知识：介绍系统设备软硬件的日常养护知识确保设备得到正确的养护方法，延长设备寿命。

(6) 安全及其它注意事项。

(7) 电子政务外网使用培训：根据用户的具体情况，对用户提市直一级单位电子政务外网接入服务的网络系统维护管理、系统操作使用等方面的培训。具体培训课程、时间、对象，根据用户的安排与用户协商确定。

培训课程一：

课程编号	课程名称
1	路由器的产品架构
2	网络管理平台及功能组件产品概述
3	路由器的基础配置指导（CLI 配置、设备登录、FTP 与 TFTP、软件升级等）
4	二层以太网交换技术原理及配置指导（MAC、VLAN、二层转发原理、STP、链路聚合等）
5	三层技术原理及配置指导（ARP、地址配置、IP 转发原理、NAT、DHCP、DNS、静态路由等）
6	网络管理和监控技术原理及配置指导（NTP、SNMP、镜像等）

7	网络管理平台的安装指导、设备管理 & 日常维护
---	-------------------------

培训课程二：

课程编号	课程名称
1	路由器的产品架构
2	网络管理平台及功能组件产品概述
3	二层广域网接入技术原理及配置指导（IPoE、L2TP、PPPoE）
4	三层高级路由技术原理及配置指导（OSPF、BGP）
5	网络管理和监控技术原理及配置指导（NTP、SNMP、镜像等）
6	网络管理平台的安装指导、设备管理 & 日常维护
7	常用认证技术原理及配置指导（802.1x、Portal）；常用组件配置及维护（EAD）

培训课程三：

课程编号	课程名称
1	路由器的产品架构
2	网络管理平台及功能组件产品概述
3	二层广域网接入技术原理及配置指导（IPoE、L2TP、PPPoE）
4	三层高级路由技术原理及配置指导（OSPF、BGP）
5	MPLS VPN 技术原理及配置指导
6	网络管理平台的安装指导、设备管理 & 日常维护
7	常用认证技术原理及配置指导（802.1x、Portal） 常用组件配置及维护（EAD、MPLS VPN 等）
8	组网强化与网络排错指导

12.4.1.1 业务操作培训

培训对象：针对市直单位电子政务外网接入服务的网络系统项目建设单位、使用单位、运维单位等在内的相关领导及核心业务人员；这部分用户是整个系统的关键用户，他们直接担负着项目推动和配合开展实施工作，可以说整个项目的成败，有很大程度将依赖这部分用户的参

与程度和应用效果。对于这部分用户的培训也将是整个项目进行培训的重点。

这部分培训的主要内容为系统框架介绍及理念介绍，系统业务流程介绍及系统使用配套管理制度探讨等。

培训课程名称	业务操作培训		
培训地点	待定		
培训对象	相关领导及核心业务人员		
培训人数	10—15 人（双方协定）		
人员要求	熟悉业务流程及相关制度，具备一定的计算机、网络相关知识		
培训目的	使核心业务人员和关键用户掌握产品业务功能的使用及熟悉项目实施方案		
课程概述	系统业务流程介绍、实施方案以及相关业务问题及系统使用配套管理制度探讨等		
培训周期	培训内容	培训资料	讲师
2 课时	系统框架介绍及理念介绍，业务流程介绍及系统配套管理制度探讨等	1、《电子政务外网系统框架介绍及理念培训》 2、《电子政务外网系统管理功能应用培训》 3、《常见问题及沟通方法培训》	高级实施顾问

12.4.1.2 系统管理及维护培训

培训对象：针对市直一级单位电子政务外网接入服务的网络系统项目建设单位、使用单位、运维单位等在内的系统管理员和技术维护人员，系统管理员是一个信息化系统持续稳定运行的基础，承担着日常运行环境维护，数据备份，技术问题沟通等职责，对该部分用户的培训将主要侧重于技术层面，同时兼顾部分业务流程的讲解。

主要培训内容系统架构、产品功能说明、系统日志及维护操作、系统安装、数据恢复与备份、日常故障维护等。

培训名称	系统管理及维护培训		
培训地点	待定		
培训对象	系统管理员、核心技术人员		
培训人数	3—5 人（双方协定）		
人员要求	对网络、数据库、服务器等有专业的知识		
培训目的	使系统管理员了解系统的运行环境以及熟悉系统日常维护内容。		
课程概述	使系统管理员了解系统的运行环境以及熟悉系统日常维护内容。		
培训周期	培训内容	培训资料	讲师
2 课时	系统安装及调试，数据备份与恢复、系统管理功能应用、常见问题及沟通方法、系统日志及维护操作、日常故障维护等	1、《电子政务外网相关产品安装及调试培训》 2、《电子政务外网系统管理功能应用培训》 3、《常见问题及沟通方法培训》	高级技术顾问

12.4.1.3 业务流程及产品操作培训

培训对象：针对市直一级单位电子政务外网接入服务的网络系统项目建设单位、使用单位、运维单位等在内所有系统操作人员。这部分用户是最终使用人员。在系统上线之前，应针对每个岗位的具体业务制定有针对性的培训方案，并结合各岗位的实际业务进行培训。

这部分培训的主要内容为软件平台业务流程及功能使用介绍。

培训名称	业务流程及产品操作培训
培训地点	待定
培训对象	系统最终用户

培训对象	具备一定的计算机及网络相关的知识、技能。		
培训目的	使操作用户掌握系统功能的使用		
课程概述	系统业务流程及功能使用介绍		
培训周期	培训内容	培训资料	讲师
5 课时	相关系统、产品的业务流程及功能使用介绍	1、《产品手册》 (含产品基本介绍、功能介绍、操作方法等)	实施顾问

12.4.2 培训目标

培训是一个非常重要的环节,通过培训使得培训后的人员能了解和掌握系统结构和工作原理、设备性能、设备操作,使得这些操作人员能担负起网络及设备的日常操作使用和保养工作,保障设备长期可靠稳定的运行。

要使网络及设备使用人员能够熟练、高效的操作设备,发挥网络及设备的最佳使用效果,还必须要对网络和设备的使用人员进行操作培训。

12.4.3 培训方式

本项目的培训组织方式主要包括现场培训、远程视频会议培训、现场实操。

12.4.3.1 现场培训

资深技术工程师在产品的安装调试过程中进行,直接针对采购人工程师进行现场教学,即时指导,增加用户的学习机会,使之能更形象地了解产品,直接更迅速地掌握各项知识和技能。

12.4.3.2 远程视频会议培训

考虑到用户对各种产品需要全方位的了解,根据用户的需求及项目的实际情况,提供丰富多样的培训方式。通过电视电话会议对技术人员进行远程培训。

远程培训可以提供语音、视频、应用共享、文档共享、文字交流等多种培训手段和辅助工具。在整个培训过程中，我方可以方便的通过各种表现方式来进行讲授，并可随时与用户之间进行沟通与补充。

我公司将编写详细的使用说明书，提供给客户的应用人员作为学习和培训教材。另外，在必要的时候，公司可以委派技术人员进行现场技术指导和应用技术讲座，以满足客户方人员的需要。

12.4.3.3现场实操

设备操作培训是我公司提供的服务设备，对设备对应的运维人员开展培训。包括设备的调试，设备的参数设置、基本使用和功能维护等内容。

12.4.4培训对象

12.4.4.1业务操作培训对象

培训对象：针对市直单位电子政务外网接入服务的网络系统项目建设单位、使用单位、运维单位等在内的相关领导及核心业务人员；这部分用户是整个系统的关键用户，他们直接担负着项目推动和配合开展实施工作，可以说整个项目的成败，有很大程度将依赖这部分用户的参与程度和应用效果。对于这部分用户的培训也将是整个项目进行培训的重点。

12.4.4.2系统管理及维护培训对象

培训对象：针对市直单位电子政务外网接入服务的网络系统项目建设单位、使用单位、运维单位等在内的系统管理员和技术维护人员，系统管理员是一个信息化系统持续稳定运行的基础，承担着日常运行环境维护，数据备份，技术问题沟通等职责，对该部分用户的培训将主要侧重于技术层面，同时兼顾部分业务流程的讲解。

12.4.4.3业务流程及产品操作培训对象

培训对象：针对市直一级单位电子政务外网接入服务的网络系统项目建设单位、使用单

位、运维单位等在内所有系统操作人员。这部分用户是最终使用人员。在系统上线之前，应针对每个岗位的具体业务制定有针对性的培训方案，并结合各岗位的实际业务进行培训。

12.4.3 培训次数

服务期内可组织不少于 3 次培训，计划安排如下，具体根据实际需求我方进行相应调整，确保满足客户需要。

序号	培训地点	培训课程	培训内容	培训对象	培训时间
1	培训中心	设备的原理和技术性能、操作维护方法、安装调试、排除故障等，提供培训教材（中文）和培训课程计划表	网络结构及工作原理	市直重点单位的相关人员	1 天
2			设备的配置和性能描述		
3			设备的运行和操作使用		
4	维护现场	设备日常维护、常见故障处理及注意事项	设备日常维护、常见故障处理及注意事项	市直重点单位的相关人员	1 天
5	培训结果检验		通过	合格	
			重新培训	不合格	

12.4.6 培训方法

本项目涉及设计、施工和相应的光电技术、通信技术、计算机技术等，因此采用软件和硬件相结合的培训方法，使操作人员熟练掌握的同时，能对系统进行简单而有效的维护工作。

12.4.6.1 书面讲解

根据我方提供的培训教材，如文档、PPT 等由我方的培训工程师向客户指定的培训人员讲授网络工作原理、设备工作原理和简单的故障排查。培训资料参训人员人手一册。

12.4.6.2 实际操作

领会基本原理后，在我方培训工程师的讲解和指导下，带领客户指定的培训人员到设备安装现场进行实际操作，熟悉设备性能、指示灯显示及故障排查等。

12.4.6.3 答疑

在上述两阶段的培训过程中及完成后，由我方的培训工程师进行统一解答培训人员的相关问题。

12.4.7 培训检验评估

培训结束，可以针对客户的需求对培训的结果进行检验，检验方式可以通过实际操作和理论考试两种形式进行。公司将为客户的考试提供相应的技术支持。

12.5 售后服务

12.5.1 售后运维要求

我公司制定系统运行维护计划、工作流程、管理制度、服务质量要求，根据不同的联网系统设备和环境制定具体的保养方案。包括但不限于符合以下要求。

(1) 网络租赁维护期内，对于系统故障在 1 小时内响应，在 2 小时内确定故障原因和解决方案，在 12 小时内排除故障，24 小时内不能修复的，保证线路稳定运行。

(2) 我公司承诺配备 6 人的专职运行维护、售后服务队伍。

(3) 我公司制定系统日常维护工作计划，并严格按照工作计划进行系统的日常维护。日常维护不影响系统的正常使用。

(4) 招标方要求的其他内容，具体以后期合同约定。

售后服务队伍人员

序号	姓名	联系电话	角色	备注
1	和鑫	13525606099	项目负责人	无
2	于士奇	19839386556	项目经理	无
3	钟建锋	13839291019	技术负责人	无
4	许光华	13939336527	技术员	无
5	李英杰	13781354080	技术员	无
6	柳亚鑫	19720379721	技术员	无

12.5.2 售后服务措施

12.5.2.1 售后服务目标

我公司将确保电子政务外网网络安全可靠运行服务保障工作，确保服务时效和质量。根据客户服务需求和服务周期安排，我公司配备 6 人的专职运行维护、售后服务队伍，项目经理与

客户深入沟通交流，制定客户专属服务计划，后期将按照服务计划，严格进行服务交付。在项目交付过程中，项目团队按照对本时间段内所有交付的服务进行总结，并给客户售后部门做专项汇报，与客户沟通服务交付。

对本项目中涉及的重点单位接入电子政务外网服务，保证各市直单位用户接入服务等网络系统的正常运行，降低整体管理成本，提高网络系统的整体服务水平。同时根据日常维护的数据和记录，提供用户网络系统的整体建设规划和建议，更好地为用户的信息化发展提供有力的保障。

通过运行维护服务的有效管理来提升各市直接入单位接入服务等网络系统的服务效率，协调各业务系统的内部运作，改善网络系统部门与业务部门的沟通，提高服务质量。结合用户现有的环境、组织结构、IT 资源和管理流程的特点，从流程、人员和技术三方面来规划用户的新风系统的结构。将用户的运行目标、业务需求与 IT 服务的相协调一致。

售后服务的目标是，对各市直接入单位接入服务等网络系统基础资源进行监控和管理，及时掌握网络系统资源现状和配置信息，反映系统资源的可用性情况和健康状况，创建一个可知可控的 IT 环境，从而保证系统的可靠、高效、持续、安全运行。

服务项目范围覆盖系统资源以下方面的关键状态及参数指标：

运行状态、故障情况；

配置信息；

可用性情况及健康状况性能指标；

统计售后数据、提供系统管理和工作报告、归纳总结并提供用户想了解的数据报告。

12.5.2.2 售后服务计划

为保障网络租赁期间系统的正常运行，我公司配备 6 人的专职运行维护、售后服务队伍，为客户提供全流程、全方位的服务。

序号	服务项目	服务内容
1	远程技术支持服务	提供 7×24 小时技术服务热线，提供产品技术咨询、故障申报受理、硬件维修 RMA 受理等服务内容。维保范围内的设备有相关问题时，可以拨打原厂技术支持中心 400 电话进行问题解决。

2	 在线支持服务	在维保服务有效期内，提供原厂官方网站与论坛 VIP 帐号；访问原厂相关技术网站和社区。可以获取维保服务相关的产品和技术资料，如产品版本、产品安装指南、版本说明书、经典维护案例、经验汇总等。还可以在社区里面提问，原厂工程师及时进行问题解答。 在维保服务有效期内，可以登录数字化服务管理系统，进行账号注册，用账号登录数字化服务管理系统，使用数字化服务管理系统的服务功能。服务功能包括但不限于：设备基本信息管理、资源状态检查、配置安全评估、技术公告扫描、版本管理、硬件问题主动服务、项目交维检查服务和远程管理。
3	软件支持服务	在维保服务有效期内，提供相应的软件支持服务。软件支持服务包括设备主机软件的版本，如软件补丁（Bug Fixes）、固件版本（Firmware Version）、软件版本更新（Soft Version Updates）等，以及这些软件的配套文档资料。
4	快速备件先行更换服务	在维保服务有效期内，提供 7×24×ND 发出级别备件更换服务，一旦定位是硬件故障，中标方应在规定时间内将原厂商正品备件先行运抵现场，保证故障部件得到及时更换，以使贵方的业务能在最短时间内恢复正常。
5	巡检服务	每个季度提供一次对所维保的设备的巡检服务，提出技术建议、实施优化。每个季度末提供原厂出具的详细的设备维修、故障报告、巡检报告，以便采购人了解维护状况，及时预见并解决问题。
6	重大网上问题现场支持服务	当出现重大设备故障对生产经营有较大影响时，我方无条件派遣工程师 4 小时内到达现场并开始处理问题。
7	现场值守服务	在设备发生故障、重大事件、关键时点、系统升级、运

	备	维保障等情况下，派遣相应级别且能解决问题的工程师到达现场，为了提供更加快捷的现场响应，提供现场值守服务，直至系统能够满足贵方业务正常运行要求。
8	培训	在服务期内，不定期提供针对贵方维护人员在网络维护、配置、故障排查等方面的培训。

12.5.2.3 远程问题诊断和支持服务

客户提出服务请求后，公司将在合同限定的服务时间内与客户合作，共同解决系统问题。在提供任何必要的现场服务之前，公司将在可行的情况下，首先使用远程支持服务工具对公司提供支持的系统进行远程诊断，或通过其它方式为远程解决问题提供帮助。

隔离软件产品出现的问题。如果问题与硬件有关，则通知客户，并将派遣工程师去现场进行维修。

12.5.2.4 现场硬件更换服务

如果公司确定硬件问题不能通过远程方式解决，则一名公司的工程师将到客户现场进行硬件的维修使其恢复运行。此外，公司还可能进行一些必要的工程改进，以便这些硬件产品能够正常运行，并与更换部件兼容。公司可全权决定安装固件更新，从而使公司所提供支持的产品恢复正常运行。

12.5.2.5 远程访问支持服务

在征得客户同意后，公司将使用选定的远程访问工具，帮助客户迅速解决问题。客户可以选择任何一种选定的工具，以帮助处理服务请求。作为此项服务的一部分，客户只能使用公司提供、认可的工具。公司可能要求客户安装并运行这些工具的软件修订版，而且，向这些修订版提供支持。

12.5.2.6 备件服务

公司拥有多个大型备件库房，与众多专业物流服务商合作，共同建立了一个快速后勤网络来保证备件供应，确保备件供应的有效运作。

针对客户系统的服务需求，公司提供的备件服务是：在服务合同期内，合同范围内需要更换的备品备件均免费提供并免费更换安装，用户不需要付额外费用。在公司的本地支持服务办公室，已经设有备件库为本地客户提供备件服务。

公司承诺采购原厂备件，保证备件的质量。

公司的备件管理部门根据设备故障率和长期备件管理经验，会将各设备的备品备件按相应重要程度区分：

关键备件：内存、CPU、主板、电源，即发生故障可能导致设备性能严重下降甚至不能正常工作的备件；

重要备件：硬盘、存储卡、网卡；

一般备件：如线缆等外部连接件。

然后再根据服务级别做出备品与备件计划：

对具有 7×24 系统支持服务设备的关键和重要备件一般会在本地/附近的备件库中存放。当这些备件被消耗后会从分拨中心或中心备件库及时补库；

在合同维护期内，关键及重要备件均就近保存在公司的备件库内，这样，当硬件故障发生时，公司将启动维护支持流程，公司直接将所需的备品备件送至故障现场，维修硬件故障，以保证快速恢复系统，使之投入正常运行。当备件库中的备件数量因被使用而减少时，将从公司的分拨中心或中心备件库及时补充备件。

12.5.2.7 日常巡检

对于客户业务环境中的各项设备巡检需求，将协调相应的专家按照客户巡检要求，提前与客户进行巡检计划沟通。在确认巡检计划后，由专业的工程师现场上门采集设备日志、诊断信息、设备指示灯状态，结合客户实际环境中的业务应用，输出专业的巡检汇总报告，同时对报告进行解读，告知客户风险隐患，并及时进行设备预防式维修。建立光纤巡查机制，派专人就提供的光纤运行质量状态进行巡查。每季度巡查不少于一次，并做好巡查登记记录和通知维修

记录。

12.5.3 售后服务制度

电子政务外网的售后服务制度是确保政府机构在实施电子政务项目后能够提供及时、有效的技术支持和问题解决方案，以确保系统的稳定运行和用户满意度的重要机制。以下是电子政务外网售后服务制度的详细内容：

12.5.3.1 售后服务组织架构

服务团队组成：

建立专门的售后服务团队，包括技术支持人员、系统维护人员、客户服务人员等，具备相应的技术和沟通能力。

服务流程管理：

制定明确的服务流程和责任分工，确保问题能够及时准确地得到解决。

12.5.3.2 服务内容和范围

技术支持：

提供系统使用过程中的技术支持，包括系统故障排查、功能操作指导、系统配置调整等。

问题解决：

对用户在使用中遇到的问题进行分析和解决，确保问题能够及时得到妥善处理。

系统维护：

定期对系统进行维护和升级，确保系统的安全性和稳定性。

12.5.3.3 服务响应时间

响应时限：

制定明确的服务响应时限，对用户提交的问题或请求要在规定时间内进行回复和处理。

12.5.3.4 服务渠道和方式

服务渠道：

提供多种服务渠道，包括电话、邮件、在线客服等，方便用户随时随地获取帮助。

服务方式：

根据用户需求和问题性质，采取远程支持、现场支持等不同的服务方式。

12.5.3.5 问题处理流程

问题登记：

用户向售后服务团队提交问题或请求，服务团队负责进行问题登记和分类。

问题分析：

技术支持人员对用户提出的问题进行分析和诊断，确定解决方案和处理措施。

问题解决：

根据问题的性质和紧急程度，及时采取相应的解决措施，确保问题能够得到有效处理。

问题反馈：

在问题解决后，向用户及时反馈处理结果，确保用户满意度。

12.5.3.6 服务质量评估

用户满意度调查：

定期对用户进行满意度调查，了解用户对服务质量的评价和建议，持续改进服务水平。

服务绩效考核：

对售后服务团队的工作绩效进行考核，奖惩并存，激励团队提升服务质量。

12.5.3.7 售后服务升级

根据需求调整：

根据用户反馈和系统运行情况，及时调整售后服务制度和流程，不断提升服务水平。

技术支持升级：

跟踪新技术发展，不断提升技术支持团队的技术水平和专业能力。

以上是电子政务外网的售后服务制度的详细内容，通过建立健全的售后服务机制，能够保障政府机构电子政务系统的稳定运行和用户满意度。

12.5.4 故障响应计划

序号	响应方式	响应内容
1	热线响应	我司提供 7×24 小时热线支持，通过 400 服务台为用户提供工单录入、进度查询、商务咨询、用户回访等服务内容，并依据业务需要协调售后工程师或我司相关部门进行处理。 工作时间：在 7*24 小时工作时间内设置由专人值守的热线电话，接听内部的服务请求，并记录服务台事件处理结果。 非工作时间：设置有专人 7*24 小时接听的移动电话热线，用于解决内部的技术问题以及接听 7*24 小时值班人员的突发情况汇报。
2	远程响应	对用户申报的故障，通过电话、邮件、QQ 远程等多种远程支持方式提供售后质量保障服务，避免由于交通等原因造成的服务响应不及时。我司运维服务团队接到服务请求后，将在协议约定的服务等级响应时间内，通过电话或 QQ 等方式及时响应，并根据故障现象划分故障等级，帮助客户进行故障定位，并提出解决方案，指导客户排除设备故障。 对于通过电话支持服务不能解决的技术问题，在征得客户同意后，可通过远程终端登录到客户申告问题的系统中进行调查和收集数据，然后进行故障诊断和相应的处理，指导客户现场维护人员排除设备故障。
3	现场响应	我司提供 7*24 小时现场支持服务，到场时间 ≤ 1 小时，故障恢复时限 ≤ 4 小时，可提供系统巡检、网络优化、版本发布等维护服务。同时，对于通过电话支持服务和远程接入服务都不能解决的设备问题，将安排经验丰富的售后工程师赴现场分析故障原因，制定故障解决方案，并最终排除故障。除不可抗力及市政施工等原因以外，保证一年内发生不超过 5 次线路故障在 48 小时内未能及时修复。

	故障返修服务是指用户设备在运行期间发生硬件故障，我司运维队伍提供响应现场维修或返厂维修服务，对无法修复的硬件设备，提供性能、功能相同的板件或设备予以替换，并上门安装调试。
---	--

12.5.5故障响应速度

我方提供 7×24 小时呼叫服务专线；从用户报障开始计算人员，到场时间 ≤1 小时，故障恢复时限 ≤4 小时。除不可抗力及市政施工等原因以外，一年内发生不超过 5 次线路故障在 48 小时内未能及时修复。

网络租赁维护期内，我方对于系统故障在 1 小时内响应，在 2 小时内确定故障原因和解决方案，在 12 小时内排除故障，24 小时内不能修复的，保证线路稳定运行。

电子政务外网网络发生故障，我方将坚持故障处理的同时及时进行故障上报的原则，以实现加强协调调度、快速抢通的目标。

我方发生本地电子政务外网故障投诉或发现设备告警后，相关专线维护负责人应第一时间到达客户现场进行故障处理。若超过 2 小时故障未恢复，上报分公司主管副总经理。若超 4 小时故障未恢复，上报分公司总经理，同时将故障处理情况上报市公司网络部集客支撑班。若超 4 小时故障仍未恢复，由市公司网络部将故障具体情况上报分管网络副总经理。故障结束后分公司应在 24 小时内上报故障处理报告。

12.5.6应急保障措施

12.5.6.1网络应急预案

12.5.6.1.1应急预案简介

为保证采购人网络的稳定运行，我方将针对本项目制定针对性的应急响应方案，主要内容涵盖如下：

- (1) 成立应急领导指挥小组；
- (2) 制定应急响应计划；

- (3)定期进行应急演练（如主备板卡切换、主备核心设备切换等……）；
- (4)重大事件阶段保障（对于采购人认为的关键时刻提供定制化支持）；
- (5)制定应急响应备品备件计划，保证在危机事件发生时，采购人可以得到有效备品备件支持。

12.5.6.1.2 应急预案方法论

应急方案的设计涉及到技术和非技术领域各层面的内容，一个完整符合用户实际情况的的应急方案，究其根本是帮助用户建立起一套完整的应由组织体系、服务体系和技术体系三个部分组成的应急响应体系。



(1) 组织体系

一个科学的应急响应体系必须有一个配套的组织体系，要根据不同的系统和应用组建信息安全应急响应小组，指派负责人；要挑选政治合格、技术过硬、肯于服务的技术人员作为应急响应小组成员；要根据任务和需要对小组成员进行合理的分工，并明确岗位职责；要制定严格的工作制度和 workflows；要建立严格的安全保密制度；要有良好的内外合作机制。

(2) 服务体系

应急响应体系是一种安全服务，一个应急响应小组至少应能提供一种或多种服务，如：计算机事件分析，现场事件响应，事件响应支持，事件响应协调等。

除此之外，还可提供事件处理咨询、脆弱性处理、人员技术培训、入侵信息的预警等其它一些安全服务。这完全取决于应急响应小组的应急处理能力和用户的实际需要。为保证这些服

务的质量,需要对服务的对象、内容、目标、流程、策略等进行科学的界定。

(3) 技术体系

技术体系是应急响应体系中的核心部分。为实施应急响应所要求和规定的服务,必须有一定的技术基础。根据应急响应方法论的工作过程,应急响应技术体系的主要包括:

预案库是专门为可能发生的、紧急的、破坏性的事件而设计的,其目的是能迅速地对事件进行合理的、科学的、有序的处理,将事件造成的影响或损失减至最小。

预警的目标是防患于未然,即在事件发生前及时发现不安全迹象,并能快速地通报给有关部门和人员。要实现预警功能,我们应做好风险分析、完整性检验、系统审计、报警通知等方面的工作。

抑制的目的是限制潜在的损失和破坏。目前实施抑制的主要技术手段是对网络上的不安全因素进行隔离或设置诱骗系统。

根除工作主要包括事件分析、取证、补救三个方面的内容。因为信息系统受到攻击后,查明原因、消除影响、根除攻击源是必须要做的工作。

备份与恢复对一个用户或企业至关重要。事实证明,大量有关企业生产、销售的数据维系着企业的生存,是企业珍贵的无形资产。这些数据一旦因为系统遭到攻击或不可避免的自然灾害造成丢失,将会给企业带来重大的经济损失。

知识汇总是将安全事件的种类、发生条件、危害程度、处理过程、响应方法和经验等作详细的记录,以供今后在工作中参考借鉴,这是一种经验总结的过程。

交流与协作是应急响应工作中一个不可缺少的部分,它起到了信息汇总和分析中心的作用。

12.5.6.1.3 应急处置基本原则

应急处置遵循“依靠技术、加强管理、预防为主、快速响应、及时恢复”的总原则。另外应做到以下几点:

➤ 统一领导, 分工协作

统一领导下,明确各部门、各单位职责,督促相关部门遵照“统一领导、归口负责、综合协调、各司其职”的原则,协同配合,有效地处置突发事件和应急情况。

➤ 明确责任, 依法规范

濮阳市各部门、各单位,要按照“属地管理、分级响应、及时发现、及时报告、及时救治、

及时控制”的要求，依法对信息安全突发事件进行防范、监测、预警、报告、响应、指挥、协调和控制。

> 统筹协调，加强调查

统筹安排濮阳市各部门、各单位应急工作任务，充分利用现有的信息安全服务设施和技术力量。各部门、各单位应在明确职责的基础上，加强协调，密切配合，保障信息安全。

> 防范为主，加强监控

贯彻预防为主的思想，树立常备不懈的观念，宣传普及信息安全防范知识，做好应对信息安全突发事件的思想准备、预案准备、机制准备和工作准备，增强公共防范意识以及基础网络和重要信息系统的信息安全综合保障水平。

> 快速处理，尽快恢复

突发重大信息安全事件时，能够及时发现和预警，准确判断并及时采取有效措施，迅速控制事件影响程度和范围，确保信息系统尽快恢复正常，尽可能减少突发事件给企业带来的负面影响和损失。

12.5.6.1.4 应急指挥机构及职责

成立网络应急工作小组，按照“谁主管谁负责”原则，对于较大和一般突发公共事件进行先期处置等工作，并及时报领导处理并备案。

发生一般网络事件，事发半小时内向单位主管领导口头报告，在 1 小时内出具书面报告；较大以上网络安全事件或特殊情况，立即报告。

网络应急指挥机构组织人员及职责如下：

应急指挥领导小组

设置应急指挥小组，履行应急值守、信息技术支持和综合协调职责，发挥运转枢纽作用；组织、协调突发信息安全事件的处置和善后工作；对突发信息安全事件进行事件调查，并组织事后评估。

应急处置小组

设置应急处置小组，负责处置电子政务外网网络安全事件、机房安全事件、网络入侵、重大病毒破坏、数据库安全事件等的处置。

专家组

由有关专家和厂商专业技术人员分别组成应急处置技术专家组，为信息安全事件应急管理

提供决策建议和技术支持，参加突发信息安全事件的应急处置和事件恢复工作。

12.5.6 应急保障与小组架构

主要指做好应急准备、应急监测、应急预案及应急处置等工作。

应急保障目的

建立、健全电子政务外网应急响应体系，规范应急响应工作内容和流程，提高应急响应能力，确保信息系统的安全和业务的连续性，减少应急事件带来的负面影响及损失。

应急保障原则

责任人原则

明确应急响应工作的组织机构，保证各项工作责任到人，应急响应领导小组统一负责重大应急事件的组织和指挥工作。

分级处置原则

明确重大事件的等级范围、划分依据，制定相应的应急响应流程，确保处置的有效、准确。

有效防备原则

建立重大事件的预案制度。完善重大事件监控和管理机制，积极采取有针对性的应急准备，防备重大事件的恶化。



应急保障小组委员岗位职责如下表所示：

岗 位 职 责	职 责
应急响应领导小组	负责审核和批准重大事件应急响应总体规划、重大事件报告。 负责统筹规划重大事件应急基础设施建设。 授权应急响应联合工作组启动特定应急预案。
应急响应联合工作组	组建、完善应急响应体系。 定期组织信息系统的风险评估和整改。 定期组织应急预案的演练。 制定重大事件报告。 负责重大事件特定系统应急预案的启动和停止。
应急响应资源支持组	负责应急行动的资源保障工作,包括车辆安排、人员安排等。
应急响应业务支持组	负责制订业务系统应急预案。 负责评估重大事件对业务工作所造成的影响。 从业务角度,为领导小组及联合工作组决策提供信息和建议。 根据应急响应工作的需要,采取相应的应急处置措施。 编写应急响应业务工作报告。
应急响应技术支持组	负责制订系统技术应急预案。 从技术角度,为领导小组及联合工作组提供信息和建议。 根据应急响应工作的需要,组织施行技术处置措施。 编写应急响应技术工作报告。

12.5.6.1.6 应急事件级别定义

根据网络与信息安全突发公共事件的可控性、严重程度和影响范围,一般分为四级:I级(特别重大)、II级(重大)、III级(较大)、IV级(一般)。国家有关法律法规有明确规定的,按国家有关规定执行。

I级(特别重大):重要网络与信息安全系统发生全市性大规模瘫痪,事态发展超出相关

主管部门的控制能力，对国家安全、社会秩序、经济建设和公共利益造成特别严重损害的突发公共事件。

II 级（重大）：重要网络与信息安全系统造成全市性瘫痪，对国家安全、社会秩序、经济建设和公共利益造成严重损害，需要跨部门、跨地区协同处置的突发公共事件。

III 级（较大）：某一区域的重要网络与信息安全系统瘫痪，对国家安全、社会秩序、经济建设和公共利益造成一定损害，但不需要跨部门、跨地区协同处置的突发公共事件。

IV 级（一般）：重要的网络与信息安全系统受到一定程度的损坏，对公民、法人和其他组织的权益有一定影响，但不危害国家安全、社会秩序、经济建设和公共利益的突发公共事件。

根据经验，我可将运维故障时间级别分为简单应急故障和重大应急故障，其相应流程如下：

简单应急故障流程

运维技术支持组接收到一线工程师或用户反映出来的问题后，对问题故障的严重性进行判断。

如果运维技术支持组判断此问题不属于重大问题，联机查看问题现象，判断问题原因。

如果问题属于业务系统本身问题，就将问题转给业务系统开发商（或相关业务运维组）；

如果问题属于主机硬件、配置的问题，就将问题转给系统运维集成商；

确属于集成平台问题，判断问题原因，在小组内部讨论解决办法，解决问题。

重大应急故障响应流程

我方工程师或用户工程师在接到重大问题后告知运维技术支持组，运维技术支持组分析并判断问题类型，立即通知应急管理小组，进入重大应急故障响应流程。如果问题属于业务系统本身问题，就将问题转给系统运维集成商；如果问题属于主机硬件和系统问题，就将问题转给系统运维集成商；如果确属于集成平台问题，判断问题原因，在小组内部讨论解决办法，解决问题。

如果问题严重并且无法远程解决，必须经过迅速判断后立即赶赴现场了解情况、现场调试，同时向应急管理小组提出申请；应急管理小组确认后，立即赶赴现场。经用户确认后，调试并解决问题。

12.5.6.1.7 应急预案管理

网络应急事件的应急处理应遵循严格的审批制度，并按一定的操作流程执行，具体流程如下：

(1) 故障上报: 巡检人员或用户人员发现问题出现, 初步对故障情况诊断, 确定故障类型及可能的发生时间, 判断为重大信息安全事件和较大信息安全事件发生时, 信息中心负责人应立即报告信息应急领导小组。

(2) 应急调度: 在接到应急响应请求后, 应急领导小组全体成员应立即反应, 并在重大故障出现时全部到达事件现场, 对于 A 级服务级别的产品立即通知原厂商到达现场; 研究决定并宣布进入应急状态, 启动应急预案。

(3) 排查诊断: 应急小组现场研究由管理小组统一现场指挥; 全体运行值班人员和现场技术人员都要服从现场指挥的领导。

(4) 处理与恢复: 技术组制定并实施完成现场处置技术方案。按照预案优先的原则, 优先执行技术应急处理预案。在实施技术应急预案时, 记录方案实施的过程。

(5) 事件升级: 当管理小组确定启动业务应急处理方案时, 应急小组负责具体实施业务应急处理方案, 各应急处理组行使各自职权, 协助组织实施业务应急方案。

(6) 持续服务: 协调组负责信息发布渠道的畅通、对外解释文稿的统一拟订、舆论疏导等方面, 并且提供人员、备品备件、物资等方面保障措施。

(7) 针对于本项目的应急体系, 制定两种应急处理流程: 简单应急故障流程、重大应急故障响应流程, 完成对用户的应急事件的全面覆盖并达到指导作用。

系统恢复流程

当信息系统恢复正常后, 由项目经理牵头, 组成评估小组, 进行检查评估。

评估小组应将评估情况写出专题材料, 作为故障、问题处理依据。由用户领导根据评估材料, 决定是否进行恢复操作, 发出解除应急状态通知。

用户信息部门启动应急故障恢复方案。

由现场指挥组织, 事件关闭后, 针对在应急处理工作中故障发生情况、处理过程、处理结果以及遇到的问题汇总, 形成信息安全事件处理结果报告, 提交应急管理小组, 并由技术维护组确认, 并归档保存。

应急承诺: 硬件维保满足 7*24 小时的应急响应时效如下:

类别	网络故障	软件故障	硬件损坏更换	咨询类、技术需求支援
电话响应时间	5 分钟	5 分钟	5 分钟	5 分钟
到达现场时间	20 分钟	20 分钟	20 分钟	24 小时

故障处理时间	2 小时	4 小时	24 小时	48 小时
--------	------	------	-------	-------

应急响应流程

项目网络保障流程分为上报阶段、信息收集阶段、预案启动阶段、预案实施阶段、应急保障结束阶段和后期处置阶段等。

突发事件发生时，出现异常重大网络中断和异常网络设施损坏的局点项目支持小组，立即将情况按照该投标项目技术流程上报客户和我方，项目组根据严重程度上报该投标项目网络保障应急小组。

项目网络保障应急小组根据我方或客户上报，进行决策判断，必要情况下启动应急保障流程。需要客户进行协调的，立即上报客户。

预案实施阶段，项目网络保障应急小组协调应急保障队伍，建立现场应急保障指挥机构，并组织应急保障队伍迅速进行网络保障和网络恢复工作。遵循先核心、后区域，先重点、后一般的原则，通过备用资源的启用、应急保障措施的启用和应急故障专家紧急排除，完成网络应急故障处理。

应急保障工作任务完成后，由采购人确定应急保障排除后，应急保障任务正式结束。

我方负责对异常重大网络中断和异常网络设施损坏原因进行调查、分析和处理，对事故后果进行评估，并对采购人汇报事故责任处理情况，以便于采购人对网络进行监督检查。

基本处理流程

值班人员平时应做好应急事件的监控工作，对于突发事件应认真分析、准确判定故障发生的数据域，负责跟踪该事件直至其结束。对于不在运维中心的故障，应在第一时间通知负责人去现场处理，密切关注事件流程及进展情况，并做好登记工作上报领导。

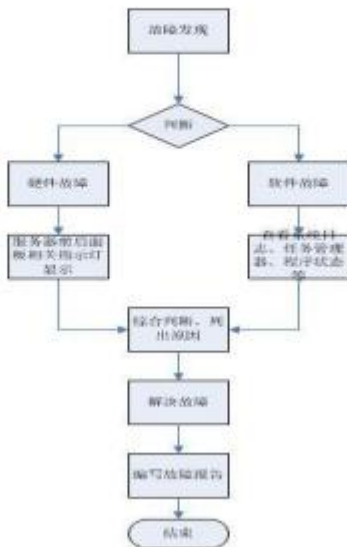
正常情况下，要求值班人员在 30 分钟内进行事件确认。如果属于一般事件则按照事件流程进行分派处理，否则应迅速启动《应急预案》，并严格按照《应急预案》所规定的步骤快速实施应急处置，及时汇报上级领导，掌握实时处理情况。

在处理过程中，如需其他部门去现场增援处理，应及时向上级领导部门汇报，协调沟通，尽快联系技术工程师或原厂商技术支持赶赴现场援助处理。

机房应急开关机具体措施

机房各设备关闭顺序如下：





后期处置

故障排除后，应急小组向各部室发出故障解除、系统恢复正常运行通知。

系统恢复运行后，相关操作人员尽快通知参保单位和个人办理社会保险业务事项，并对故障发生前所进行过的业务操作进行检查，核对业务数据是否正确或有无丢失，不正确或有丢失的应马上更正或补录，确保数据的正确和完整。对在故障期间采用手工受理的事项，应及时在系统中补充完善。

所领导组织有关人员及有关技术专家组成事件调查组，对事件发生原因、性质、影响、后果、责任及应急处置能力、恢复重建等问题进行全面调查评估，总结经验教训，完善信息系统应急处理预案，整改信息系统存在的隐患。

应急保障

预留一定数量的设备，用于预防或应对信息系统突发事件。

选择熟悉信息系统软硬件的专业公司作为信息系统应急处理的社会应急支援单位，提供技术支持和服务。信息系统服务器以及存储设备要与专业厂商签定维保协议，明确备用设备的供应时间。

强化信息安全宣传教育，提高信息安全防御意识。每年至少组织开展一次全局范围内的信息网络安全教育，提高技术信息安全防范意识和能力。

12.5.6.2 基础专线接入网络应急保障方案

12.5.6.2.1 预防性保障措施

(1) 加强基础资料核查管理，提升快速应急能力

做好基础资料核查和管理工作，为保障期间发生重大故障、或突发情况做好应急调整数据支撑，前完成维护资料的整理，有力支撑业务的故障处理、投诉响应和紧急需求。

(2) 做好电子政务外网检查，消除网络隐患

做好各市直重点单位的隐患排查和倒换测试，排查范围为各市直重点单位机要局移动核心机房段线路巡检和应急准备工作，机房环境、安全状况、设备运行、标签和线缆、电源接地等项目是否符合要求等，并做好隐患排查处理记录。对于巡检发现的问题和隐患予以整改，及时消除隐患。

(3) 做好端到端故障监控，加强客情沟通

故障提前发现，通过网管平台进行网络运行情况分析，对有可能影响网络安全运行的隐患彻底排除；做好保障期间业务的监测，各级网管监控通过告警第一时间发现故障。

提前与客户沟通，建立客户一对一沟通机制，发生故障后保证维护人员和客户能够第一时间联系，及时处理故障。

(4) 做好应急物资储备，提升故障处理效率

做好备品备件的核查工作，清查设备备品备件是否有库存不足或正在返修的情况，及时与设备厂家联系解决，保证保障期间备品备件能及时调用。

出现主备用光缆单条故障，或其他可能造成影响的环路中断时，在抢修同时对另一方向光缆进行重点保障。

(5) 加强应急演练，强化人员物资调配能力

加强故障抢修力量，制定快速响应和故障通知上报机制。实行全天 24 小时故障抢修，确保故障发生后，5 分钟故障通知，30 分钟到达现场。针对光缆、设备等不同故障场景制定相应处理方案，保证规定实现内完成故障处理。

12.5.6.2.2 应急巡检与故障处理方案

保障专线日常巡检

- 1、分公司制定巡检计划，每季度至少对客户机房巡检一次，每周对移动侧机房巡检一次。
- 2、维护人员每天对电子政务外网网络运行情况、双路由完好情况进行检查，发现问题及时处理。

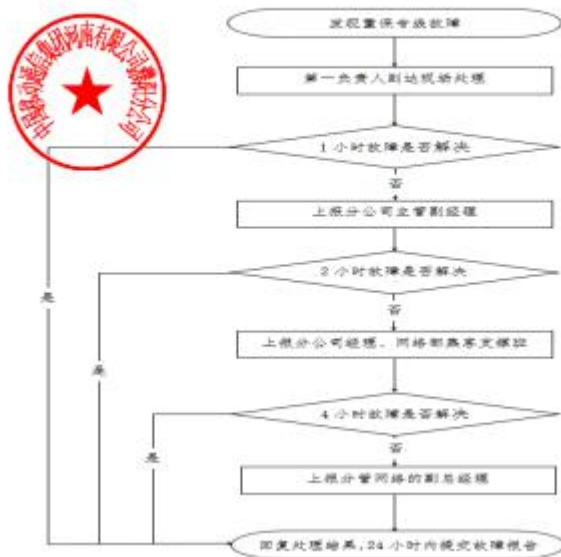
明确责任分工

成立应急保障指挥小组和抢修小组，发生故障后，维护人员第一时间响应，并快速处理故障。

按故障上报流程逐级上报故障

保障期间，电子政务外网网络发生故障，分公司要坚持故障处理的同时及时进行故障上报的原则，以实现加强协调调度、快速抢通的目标。

故障上报流程：保障期间，分公司发生本地电子政务外网故障投诉或发现设备告警后，相关专线维护负责人应第一时间到达客户现场进行故障处理。若超过 2 小时故障未恢复，上报分公司主管副总经理。若超 4 小时故障未恢复，上报分公司总经理，同时将故障处理情况上报市公司网络部集客支撑班。若超 4 小时故障仍未恢复，由市公司网络部将故障具体情况上报分管网络副总经理。故障结束后分公司应在 24 小时内上报故障处理报告。



故障处理原则

- (1) 遵循先抢通、后抢修；先重点、后一般的原则；
- (2) 维护人员应保持良好的状态，实行 24 小时值班，所有人员应坚守工作岗位待命；
- (3) 主动与上级有关部门联系，及时通报有关情况；
- (4) 在执行保障任务和业务恢复过程中，应顾全大局，积极搞好企业间的协作配合，与客户做好沟通解释；
- (5) 出现复杂情况故障时，第一时间协调相关维护、实施人员，逐步故障处理，直至故障恢复。

故障处理时限

- 1、全业务应急保障领导小组和成员必须 24 小时开机，在接到应急任务后，必须在 30 分钟内赶到指定地点汇合。
- 2、对于城区重保专线故障，必须在 30 分钟内到达现场，2 小时内完成故障处理；对于乡村重保专线业务，必须在 2 个小时内赶到现场，并根据业务保障等级要求时限完成故障处理。

12.5.6.2.3 重要场景应急预案

市三单位光网终端

(1) 市三单位光缆完全中断

当判定为光缆整体中断时，采取先抢通的方式，通过一切可以采取的方式先接通光缆，同时布放替代光缆，当原有光缆采取非正常方式接通时，替代光缆布放完成后将业务割接至新光缆。

(2) 光缆部分纤芯故障，有空余可用纤芯

当判定为个别纤芯问题时，将业务紧急调整至剩余可用纤芯，并同时开始布放替代光缆，布放完成后将新光缆与原有光缆组成双线路保护。

(3) 光缆部分纤芯故障，无空余可用纤芯

当个别纤芯故障，剩余纤芯被占用时，核实占用业务，临时断开业务保障等级较低的业务，将政务外网调整至释放纤芯，同时布放替代光缆，布放完成后将新光缆与原有光缆组成双线路保护，并恢复临时断开的业务。

接入侧传输设备故障

建立传输设备应急备件库，几个单位为一个小组配备 PTN910 与 Metro100 各一套，网络部储备 PTN950/960、Metro1000 各一套。当单位内出现传输设备故障，调用储备设备时，需同时将设备使用情况上报网络部，当同一组出现一处以上设备故障时，由网络部通知临近小组调配应急设备一套，同时网络部将储备设备增发至被调用单位。对于有备件服务的设备，同时通知厂家启动备件服务，对于无备件服务的设备，需当天将故障设备发回厂家维修。

客户节点网络故障

当确定故障点位于客户内网时，第一时间通知对应客户经理，并以书面形式将判断依据与故障情况上报网络部与政企部。同时尽最大努力配合客户定位处理故障，在故障处理完成并确认业务恢复后，方可离开现场。若客户认可故障判断并同意我方人员提前离开，维护人员仍需与客户保持沟通，每 30 分钟跟进处理情况，直至业务恢复。

12.5.6.2.4 应急保障注意事项

- 1、在应急保障中，维护物资与应急保障车辆应随时待命，发生故障后，保证维护人员与

维护物资能够第一时间到位，不得出现因应急物资滞后影响整个应急保障任务情况。

2、在平时的应急保障工作中，首先要保障现有的业务不受影响。

3、在应急保障过程中，如遇到方案不能执行，要及时上报领导小组协调解决，不得拖延时间。

4、在完成应急方案的实施后，要进行密切的网络运行关注。并在完成保障任务后，要及时总结经验，并加强宣传。

5、各专业严格按照全业务应急保障流程进行相关工作。

12.5.6.3 网络安全各场景应急预案

12.5.6.3.1 预案概述

协助优化和完善应急预案，并按照方案定期组织应急演练，提供《应急演练方案》、《应急响应分析报告》。每年协助开展应急安全演练。

演练背景

随着日益严峻的网络安全形势，渗透、DDOS 等网络攻击日益加剧；黑色产业链也时时刻刻影响着诸多企事业单位网络系统、数据的安全平稳运行。

通过应急演练服务协助客户组织相关单位及人员，依据有关网络与信息安全应急预案，模拟应对突发事件的活动。演练内容针对可能突然发生的、无法预期的或难以预期的，严重影响或可能严重影响网络与信息系统安全稳定运行的事件。

通过应急演练，进一步加强对应急处理预案的理解，使预案的要求进一步落到实处；同时通过演练检验预案中网络安全事件等级划分、响应流程等的合理性，发现预案存在的不足之处，为今后补充完善预案提供参考。

演练目的

通过演练，检验应急响应流程的合理性，优化应急响应处置流程，提高安全事件处理的协同性，达到培训网络安全运维人员安全技术能力。

演练方式

演练由两大模块组成，包含事中攻击与应急处置防护、事后溯源两大类。开展攻防演练项目，通过“讲”，普及网络安全知识，提升员工整体网络安全意识；通过“练”，模拟网络攻击应急处置防护，增强应对突发网络安全事件的能力；通过“演”，以互动体验和大屏展示的

方式，让运维保障人员熟悉应急响应的处置流程。

演练实施

演练分为三个阶段：准备阶段、实施阶段、总结阶段。

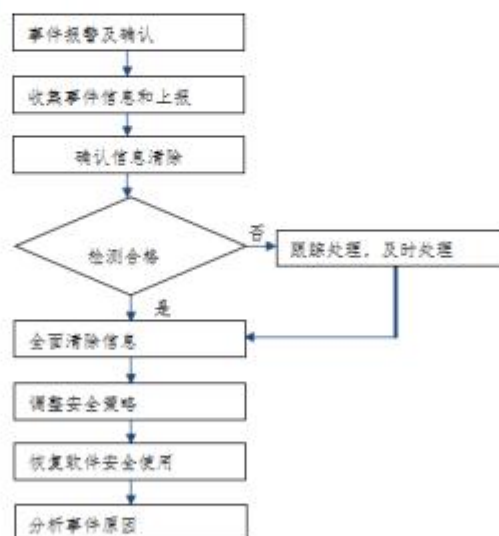
准备阶段

准备阶段主要工作内容包括：

- (1) 编制应急演练方案。
- (2) 组织制定演练场景。根据演练目标与实际环境，制定信息安全攻防演练的具体场景：

实施阶段

- (1) 组织技能培训，针对演练内容与所需的技能、工具等进行集中专项培训；
- (2) 演练正式实施，正式组织演练实施。
- (3) 演练具体实施规范流程。



总结阶段

对信息安全攻防演练进行全面总结，领导及嘉宾进行点评。

网络与信息安全事件种类繁多，每种类型的事件有着自己的特征和应急处理方法，典型的事件包括拒绝服务攻击、网页篡改（网站挂马）、恶意程序、系统故障等。掌握这些典型事件

的应对方法可以参考网络安全事件处置进行规范具体流程。

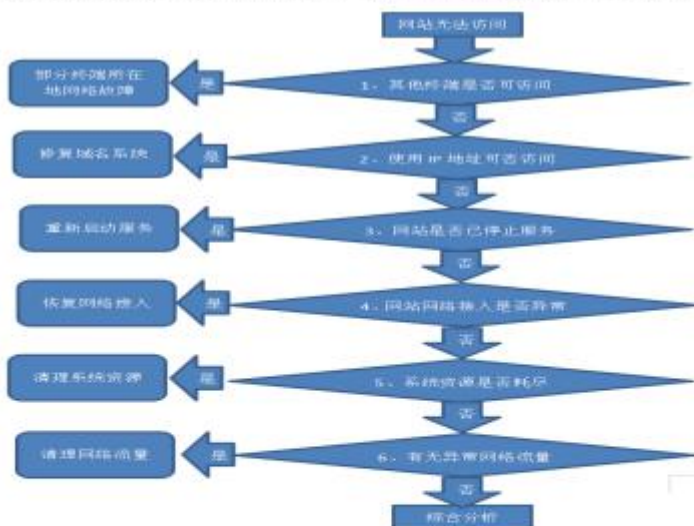
12.5.6.2 拒绝服务攻击事件应急处置

拒绝服务 (Denial of Service, DOS) 攻击是一种以事件所造成的后果命名的攻击方式, 是最为常见的攻击方式, 其结果是造成目标网络与信息系统可用性被破坏。伴随着大规模僵尸网络的盛行, 资源耗尽型拒绝服务攻击格外便于实现并可能造成严重的后果。

拒绝服务攻击事件表现为网络与信息系统无法正常访问或响应明显变慢。由于存在不依赖系统漏洞的拒绝服务攻击, 因此并不是每一种类型的拒绝服务攻击都是可以有效处置的。从拒绝服务的后果表现上看, 可以分为两种情况: 完全不可访问, 可访问但访问速度明显下降。

当出现网站完全不可访问时, 极有可能是遭受了大规模的分布式拒绝服务攻击, 但从技术原理上看, 其他网络或系统故障也可能造成同样的现象。对于网络与信息安全事件应急处置工作而言, 应当优先考虑并排除易于处理的情况。

当监测系统监测发现, 或接到报告和投诉, 相应的分析确认与紧急处置步骤如下:



拒绝服务攻击按照是否可根除可以分为两类, 第一类是由于系统存在的软件漏洞, 配置漏洞等原因引发的事件, 第二类是消耗资源发动的、不依赖漏洞的事件。

对于第一类事件，通过修补系统的软件漏洞和配置漏洞即可避免事件再次发生。对于第二类事件，无法彻底的修复事件，但可以在一定范围内降低事件造成的破坏，主要措施如下：

1、升级系统，包括对网络接入带宽、相关设备性能进行升级，必要时对最可能成为性能瓶颈的网站服务器采取负载均衡等措施，提高对外服务的硬件基础。

2、部署流量清洗设备，对网络异常流量进行适当的处理，减轻流量攻击造成的影响。

3、优化系统，包括对网络结构、系统配置的优化，将有限的资源尽可能用于核心服务。在完成拒绝服务时间的处置工作后，有必要对系统进行评估，对于因安全漏洞引发的事件，还应全面加固系统，防止系统存在其他可被用于拒绝服务攻击的安全漏洞。

12.5.6.3.3 网页篡改事件应急处置

网页篡改是一种根据事件表现而界定的网络安全事件，这类事件做明显的表现就是网页内容出现异常。例如网站的首页或其他页面被替换、网页内容中存在非授权的增加、删除、修改等。

对于网页篡改而言，紧急处置的方法根据网站保障目标的不同可能有所差异，但至少应当及时保存被篡改网页的截屏、修改相关系统重要账户口令，并将网站所在主机的系统日志、web日志以及监控审计系统日志等相关日志信息进行保存，以便在事件分析确认时能够提供必要的

数据。

当发现网页内容异常后，可参考以下流程进行分析确认与应急处理工作：



12.5.6.3.4 踝意勒索病毒传播事件应急处置

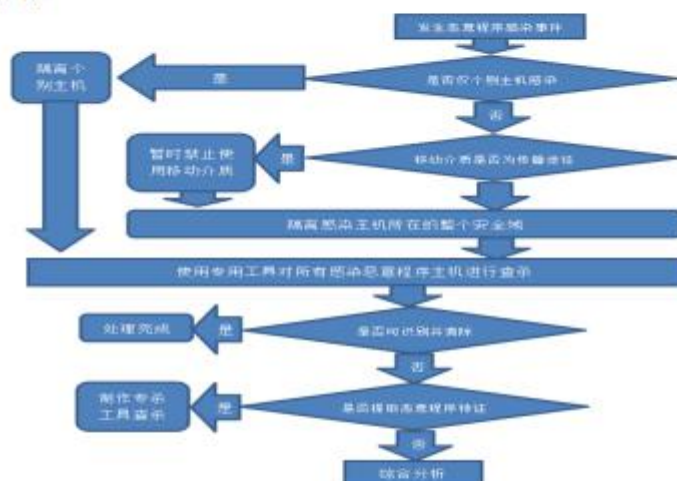
恶意程序主要包括计算机病毒、蠕虫、木马、僵尸程序等。计算机病毒和蠕虫是最为常见的恶意程序,对用户计算机的破坏力也比较强。近年来,随着黑客地下产业链的不断发展,木马和僵尸程序以及一些助长其传播的恶意程序已经逐步成为黑客最常利用的手段,也越来越成为需要重点关注和防范的对象。

338

缓慢或其他异常情况，在做好紧急处置的前提下即可开展事件的分析确认和应急处置。

对于恶意程序事件通告，紧急处置主要包括两部分的内容：一是隔离，将存在疑似感染恶意程序的终端、服务器、其他主机或安全域进行有效隔离；二是保留关键信息，如异常现象的图片、影像，相关主机的各类日志等。

当发现感染或者可能感染恶意程序时，可参照下图的分析处置流程开展事件的分析确认与应急处置工作：



在对恶意程序进行清除后，还需要了解该类恶意程序感染的原因，如系统存在安全漏洞、系统中使用的某种应用程序存在安全漏洞等。在了解这些原因后，及时对本单位存在这些安全漏洞的服务器、办公终端进行漏洞修补，避免事件再次发生。

12.5.6.3.5 数据破坏事件应急处置

数据安全有两个方面，即数据完整性的破坏和数据保密性的破坏。本节所提及的数据破坏专指数据完整性的破坏，是指因软硬件损坏、网络攻击或误操作造成数据全部或部分丢失，既不包括数据保密性的破坏，也不包括因加密后的数据因口令遗忘等非技术原因造成的数据不可访问。

造成数据破坏或丢失的原因很多，外部环境造成的物理损坏、存储设备自身的老化故障、软件或人为误操作或恶意操作等都可能造成数据不可访问。

数据破坏可分为物理破坏、逻辑破坏两种类型，如下表所示。

类别	描述	示例
物理破坏	用于存储数据的存储介质遭到破坏出现故障	机械硬盘盘片划伤 固态硬盘存储芯片损坏
逻辑破坏	因病毒或人为原因造成的数据不可访问。	数据被删除 数据被勒索软件加密

1、物理破坏

物理破坏是指对存储数据的载体进行的破坏，造成存储介质无法工作，进而导致数据的丢失。很多情况都会造成数据的物理破坏，如自然灾害、人为破坏等。

2、逻辑破坏

逻辑破坏是指保存数据的存储介质完好，工作正常，但存储介质中的数据遭到了破坏，如病毒的破坏导致文件打开乱码或无法打开，人为因素造成的数据删除、覆盖等导致数据丢失等。

数据破坏事件的发现有两种情况，一种是发现介质不可读，另一种是发现某些文件丢失或不完整。当发现介质不可读时，所能采取的措施是确定的，即如果数据已经进行了备份，则启用备份数据，如果需要修复出现故障的介质，除非本单位具备对存储介质硬件的修复能力，否则只能送交专业机构进行修复处理。

对于发现文件丢失或不完整的情况，则可参考下图所示的分析处置流程开展事件的分析确认与应急处置工作：



数据恢复完毕后，应结合引起事件的原因，加强事先的准备，如加强备份工作或调整备份频率、加强对硬件设备的例行检查等，以减小数据破坏可能造成的损失。

12.5.6.4 其他场景应急预案流程

12.5.6.4.1 机房空调设备应急流程

若空调损坏，应第一时间通知厂家上门进行维修，并及时报告信息部相关领导请示，获得授权后按机房设备关闭顺序关闭各类设备。

12.5.6.4.2 消防设备应急流程

一旦机房发生火灾，应遵照下列原则：首先确保人员安全；其次保护关键设备、数据安全；三是保护一般设备安全：

人员疏散的程序是：机房工作人员立即按响火警警报，并通过 119 电话向公安消防请求支援，所有人员戴上防毒面具，所有不参与灭火的人员按照预先确定的线路，迅速从机房中撤出：

人员灭火的程序是：首先切断所有电源，启动自动喷淋系统或使用灭火器，灭火值班人员

戴好防毒面具，从指定位置取出泡沫灭火器进行灭火。

12.5.6.3 电源设备应急流程

在紧急情况发生时，应按如下步骤进行关机：

- (1) 确认所有负载均已安全关机。
- (2) 关闭 UPS 负载电源。
- (3) 将 UPS 的系统启用开关切换到 off 的状态。
- (4) 将 DC 电池连接断路器切换到 off 的位置。
- (5) 将所有电池拉出到红色电池断开线以外。
- (6) 断开 PDU 上的断路器。
- (7) 将 PDU 后面总输入断路器切换到断开位置。
- (8) 将每个上行主电路断路器切换到断开位置。

12.5.6.4 灾害性事件应急流程

一旦发生灾害性事件，应急小组每一位成员都应有责任在第一时间进入机房抢救服务器及存储设备。

应急小组对网络设备的损坏程序进行评估。如网络设备损坏无法使用，立即联系相关厂商，进入维保服务程序。

根据网络设备修复和恢复系统所需时间，由所领导小组决定是否启用备份设备。

12.5.6.4.5 其他突发事件应急流程

应急小组立刻派出进入现场，制定相应措施，根据实际情况灵活处理，并按要求报告所领导小组。

12.5.6.5 应急预案演练

协助优化和完善应急预案，并按照方案定期组织应急演练，提供《应急演练方案》、《应急响应分析报告》。每年协助开展 2 次应急安全演练。

演练背景

随着日益严峻的网络安全形势，渗透、DDOS 等网络攻击日益加剧；黑色产业链也时时刻刻影响着企业事业网络系统、数据的安全平稳运行。

通过应急演练，帮助客户组织相关单位及人员，依据有关网络与信息安全应急预案，模拟应对突发事件的活动。演练内容针对可能突然发生的、无法预期的或难以预期的，严重影响或可能严重影响网络与信息系统安全稳定运行的事件。

通过应急演练，进一步加强对应急处理预案的理解，使预案的要求进一步落到实处；同时通过演练检验预案中网络安全事件等级划分、响应流程等的合理性，发现预案存在的不足之处，为今后补充完善预案提供参考。

演练目的

通过演练，检验应急响应流程的合理性，优化应急响应处置流程，提高安全事件处理的协同性，达到培训网络安全运维人员安全技术能力。

演练方式

演练由两大模块组成，包含事中攻击与应急处置防护、事后溯源两大类。开展攻防演练项目，通过“讲”，普及网络安全知识，提升员工整体网络安全意识；通过“练”，模拟网络攻击应急处置防护，增强应对突发网络安全事件的能力；通过“演”，以互动体验和大屏展示的方式，让运维保障人员熟悉应急响应的处置流程。

实现方案及流程

演练实施

演练分为三个阶段：准备阶段、实施阶段、总结阶段。

准备阶段

准备阶段主要工作内容包括：

编制应急演练方案。

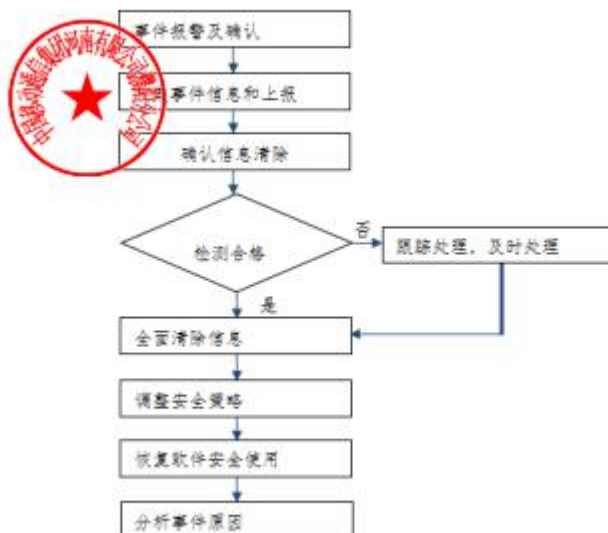
组织制定演练场景。根据演练目标与实际环境，制定信息安全攻防演练的具体场景：

实施阶段

组织技能培训，针对演练内容与所需的技能、工具等进行集中专项培训；

演练正式实施，正式组织演练实施。

演练具体实施规范流程。



总结阶段

对信息安全攻防演练进行全面总结，领导及嘉宾进行点评。

典型网络安全事件处置

网络与信息安全事件种类繁多，每种类型的事件有着自己的特征和应急处理方法，典型的事件包括拒绝服务攻击、网页篡改（网站挂马）、恶意程序、系统故障等。掌握这些典型事件的应对方法可以为我校网络安全事件处置进行规范具体流程。

拒绝服务攻击事件应急处置

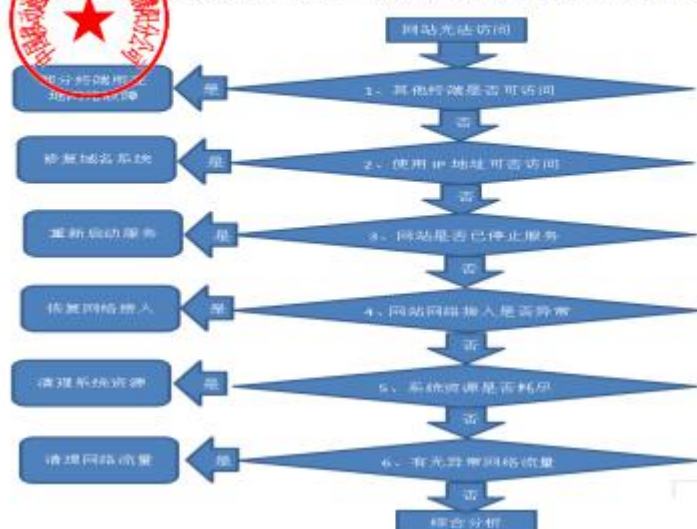
拒绝服务（Denial of Service, DOS）攻击是一种以事件所造成的后果命名的攻击方式，是最为常见的攻击方式，其结果是造成目标网络与信息系统可用性被破坏。伴随着大规模僵尸网络的盛行，资源耗尽型拒绝服务攻击格外便于实现并可能造成严重的后果。

拒绝服务攻击事件表现为网络与信息系统无法正常访问或响应明显变慢。由于存在不依赖系统漏洞的拒绝服务攻击，因此并不是每一种类型的拒绝服务攻击都是可以有效处置的。从拒绝服务的后果表现上看，可以分为两种情况：完全不可访问，可访问但访问速度明显下降。

当出现网站完全不可访问时，极有可能是遭受了大规模的分布式拒绝服务攻击，但从技术原理上看，其他网络或系统故障也可能造成同样的现象。对于网络与信息安全事件应急处置工

作而言，应当优先考虑并排除易于处理的情况。

当监测系统监测发现或接到报告和投诉，相应的分析确认与紧急处置步骤如下：



拒绝服务攻击按照是否可根除可以分为两类，第一类是由于系统存在的软件漏洞，配置漏洞等原因引发的事件，第二类是消耗资源发动的、不依赖漏洞的事件。

对于第一类事件，通过修补系统的软件漏洞和配置漏洞即可避免事件再次发生。对于第二类事件，无法彻底的根除事件，但可以在一定范围内降低事件造成的破坏，主要措施如下：

- 1、升级系统，包括对网络接入带宽、相关设备性能进行升级，必要时对最可能成为性能瓶颈的网站服务器采取负载均衡等措施，提高对外服务的硬件基础。
- 2、部署流量清洗设备，对网络异常流量进行适当的处理，减轻流量攻击造成的影响。
- 3、优化系统，包括对网络结构、系统配置的优化，将有限的资源尽可能用于核心服务。在完成拒绝服务时间的处置工作后，有必要对系统进行评估，对于因安全漏洞引发的事件，还应全面加固系统，防止系统存在其他可被用于拒绝服务攻击的安全漏洞。

网页篡改事件应急处置

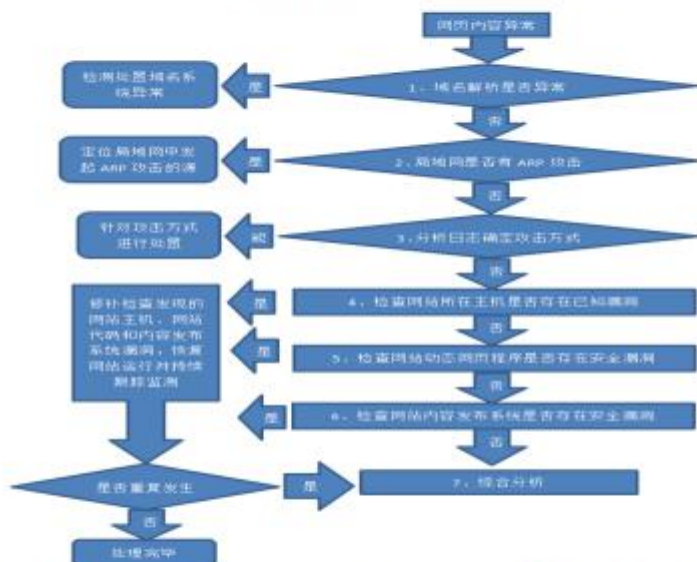
网页篡改是一种根据事件表现而界定的网络安全事件，这类事件做明显的表现就是网页内容出现异常。例如网站的首页或其他页面被替换、网页内容中存在非授权的增加、删除、修改

等。

对于网站篡改而引发的紧急处置的方法根据网站保障目标的不同可能有所差异，但至少应当及时保存被篡改网页的备份、修改相关系统重要账户口令，并将网站所在主机的系统日志、web 日志以及监控审计系统日志等相关日志信息进行保存，以便在事件分析确认时能够提供必要的

数据。

当发现网页内容异常后，可参考以下流程进行分析确认与应急处理工作：



分析事件是为了找到攻击者实施攻击的方法，以采取措施避免事件重复发生。由于信息技术的复杂性，即使是准确定位了事件发生的技术原因与实施路径，也很难完全在原有系统上根除。也就是说，当攻击者实施攻击并获得了系统的控制权后，是否安装了后门程序、安装了哪些后门程序，是难以准确掌握的。因此对于此类事件，当发现了后门程序，尤其是系统级的后门程序时，应当在全新的主机上重新安装部署环境和网站程序，以防由于系统存在后门而造成的再次被控制。同时，还应持续地对网站进行监测，以确保避免由于事件处置不彻底而再次发生。

恶意勒索病毒传播事件应急处置

恶意程序最简单的理解就是一种带有恶意目的的程序代码，这种恶意目的既有可能是直接

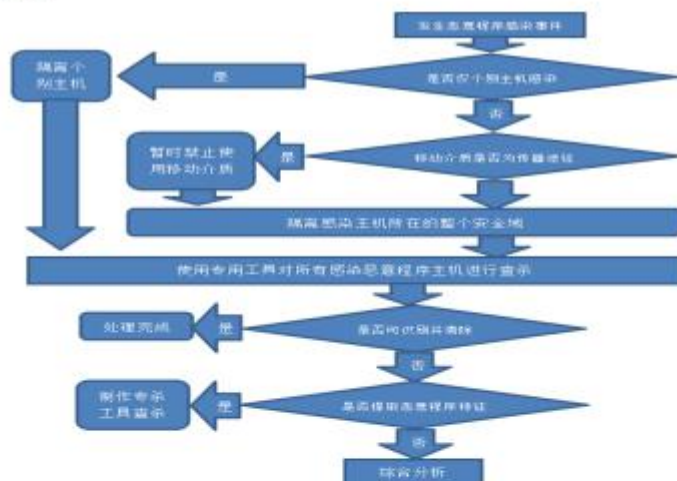
破坏系统运行、破坏系统数据、窃取敏感信息，也可能是以此为跳板，对其他网络与主机发起攻击。

恶意程序主要包括计算机病毒、蠕虫、木马、僵尸程序等。计算机病毒和蠕虫是最为常见的恶意程序，对用户计算机的破坏力也比较强。近年来，随着黑客地下产业链的不断发展，木马和僵尸程序以及一些助长其传播的恶意程序已经逐步成为黑客最常利用的手段，也越来越成为需要重点关注和防范的对象。

当发现网络与信息系统感染恶意程序时，如发现网络流量异常、协议组成异常、主机响应缓慢或其他异常情况，在做好紧急处置的前提下即可开展事件的分析确认和应急处置。

对于恶意程序事件而言，紧急处置主要包括两部分的内容：一是隔离，将存在疑似感染恶意程序的主机、安全域与其他主机或安全域进行有效隔离；二是保留关键信息，如异常现象的图片、影像，相关主机的各类日志等。

当发现感染或者可能感染恶意程序时，可参照下图的分析处置流程开展事件的分析确认与应急处置工作：



在对恶意程序进行清除后，还需要了解该类恶意程序感染的原因，如系统存在安全漏洞、系统中使用的某种应用程序存在安全漏洞等。在了解这些原因后，及时对本单位存在这些安全漏洞的服务器、办公终端进行漏洞修补，避免事件再次发生。

数据破坏事件应急处置

数据安全有两个方面，即数据完整性的破坏和数据保密性的破坏。本节所提及的数据破坏专指数据完整性的破坏，是指因软硬件损坏、网络攻击或误操作造成数据全部或部分丢失，既不包括数据保密性的破坏，也不包括因加密后的数据因口令遗忘等非技术原因造成的数据不可访问。

造成数据破坏或丢失的原因很多，外部环境造成的物理损坏、存储设备自身的老化故障、软件或人为误操作或恶意操作等都可能造成数据不可访问。

数据破坏可分为物理破坏、逻辑破坏两种类型，如下表所示。

类别	描述	示例
物理破坏	用于存储数据的存储介质遭到破坏出现故障	机械硬盘盘片划伤 固态硬盘存储芯片损坏
逻辑破坏	因病毒或人为原因造成的数据不可访问。	数据被删除 数据被勒索软件加密

1、物理破坏

物理破坏是指对存储数据的载体进行的破坏，造成存储介质无法工作，进而导致数据的丢失。很多情况都会造成数据的物理破坏，如自然灾害、人为破坏等。

2、逻辑破坏

逻辑破坏是指保存数据的存储介质完好，工作正常，但存储介质中的数据遭到了破坏，如病毒的破坏导致文件打开乱码或无法打开，人为因素造成的数据删除、覆盖等导致数据丢失等。

数据破坏事件的发现有两种情况，一种是发现介质不可读，另一种是发现某些文件丢失或不完整。当发现介质不可读时，所能采取的措施是确定的，即如果数据已经进行了备份，则启用备份数据，如果需要修复出现故障的介质，除非本单位具备对存储介质硬件的修复能力，否则只能送交专业机构进行修复处理。

对于发现文件丢失或不完整的情况，则可参考下图所示的分析处置流程开展事件的分析确认与应急处置工作：



数据恢复完毕后，应结合引起事件的原因，加强事先的准备，如加强备份工作或调整备份频率、加强对硬件设备的例行检查等，以减小数据破坏可能造成的损失。

12.5.6.6应急响应服务

应急响应服务方案将对客户信息安全应急响应体系进行设计，包含需求调研、风险评估、应急策略制订、预案编写、评审和发布等几个阶段工作；提供 7*24 小时的安全应急响应服务，包括且不限于如下情景的安全应急响应：网络阻塞、DDoS 攻击问题、服务器遭劫持问题、系统异常宕机问题、恶意入侵、黑客攻击问题、病毒爆发问题、内部安全事故；在安全事件爆发时在接到客户的应急响应请求后提供实质性响应，必要时到达现场进行排查，处理完成后及时输出《XX 事件应急响应报告》。

服务内容与流程

建立应急响应预案

根据客户的信息安全组织和信息安全现状，结合客户业务系统的特点，分析业务系统可能会发生的安全事件类别以及可能造成的影响范围、严重程度等，和客户一起，建立相应的应急响应预案，并指导客户对预案进行演练。

通过建立应急响应预案，可以在安全事件发生前进行演练防患于未然，当安全事件发生时，

可根据预案进行快速响应，从而在最短的时间内找到安全事件源头，恢复系统的正常运行。

判定安全事件类型

从网络安全系统、IDS 日志记录、桌面日志中判断安全事件类型。查明安全事件原因，确定安全事件的威胁和破坏的严重程度。查明安全事件原因，确定安全事件的威胁和破坏的严重程度。

抑制事态发展

抑制事态发展是为了将事故的损害降低到最小化。在这一步中，通常会将受影响系统和服务隔离。这一点对保持系统的可用性是非常重要的。

排除系统故障

针对发现的安全事件来源，排除潜在的隐患，消除安全威胁，彻底解决安全问题。

恢复信息系统正常操作

在根除问题后，将已经被攻击设备或由于事故造成的系统损坏做恢复性工作，使网络系统能在尽可能短的时间内恢复正常的网络服务。

客户信息系统安全加固

对系统中发现的漏洞进行安全加固，消除安全隐患。

重新评估客户信息系统的安全性能

重新评价客户系统的安全特性，确保在一定的时间内，不发生同类的安全事件。

安全态势监控

定期跟踪国内外的安全漏洞发布平台（如 CNCERT、CNVD），及时发现新近出现的安全漏洞，通过电话、邮箱等方式，及时向客户通告最新的针对业务的（或具有重大影响的）安全漏洞、安全病毒、安全攻击、安全技术等安全态势信息，并提供有参考意义的安全防护建议，保证客户信息安全工作的前瞻性和预判性。