### 许昌市公安局公安信息网

### “公安网IP扩容”项目

### 技术方案(实施方案)

**郑州恒信通讯科技有限公司**

**日 期：2018年12月5日**

## 1项目概述

### 1.1背景

公安信息网是连接全国各级公安机关的专用信息通信网络，目前许昌市公安网IP地址资源即将用尽，无法满足网络设备数量的日益增长。为了应对当前IP地址资源枯竭的形势，提高公安信息网IP地址资源的管理水平，在公安部的指导下，全国公安均已经开展了IP地址扩容工作，扩容后的公安信息网IP地址资源得以扩充，确保了公安信息网稳定运行。

随着公安信息网的迅速发展和信息化系统的不断扩展，许昌市公安局IP地址使用数呈快速增长态势。随之而来的就是IP地址管理的问题、设备的安全准入、终端的安全检查、有效地管理整个网络系统中的IP地址，规范IP地址的使用，提高公安信息网IP地址资源管理水平，符合公安部《公安信息网IP地址资源管理办法》的管理要求，已成为当前网络管理工作急需解决的问题。

### 1.2现状

当前，许昌市公安信息网IP地址的规划主要通过科信部门统一规划，分级管理，纸质备案，“一机两用”系统IP审计的方式管理；IP地址的使用则主要通过先使用再由“一机两用”扫描系统发现后，通过终端人工注册、登记备案的方式进行管理，并结合“一机两用”未注册阻断（ARP软阻断）对未注册设备进行阻断。

许昌市公安局网络计算机原有80个C类IP地址管理公安信息网4县5区近8000台终端及网络设备，此次IP地址扩容改造公安部分配了8个B类地址，IP地址的数量是之前的二十五倍,达到几十万个。伴随IP地址扩容，现有IP和新IP更换也将面临各种问题，极易出现各种无法预估的、影响公安网网络安全、信息安全的事件发生。

随着公安信息网IP地址资源扩容的实施和信息化的推进，终端数量也随之大量增长，而许昌市公安局部署的一台“一机两用”监控系统的数据库存储量已经达到146G，且在当前网络环境中的响应速度明显出现延迟，面对扩容后超量的IP管理，系统对终端管理能力将不能满足管理需求，无法保障“一机两用”监控系统的稳定运行与管理预期。

### 1.3存在的主要问题

没有统一、高效的IP地址资源管理分配手段、现有“一机两用”系统对IP扩容后超量的IP管理、扫描将会捉襟见肘，存在的问题提显而易见，主要表现为：存在多台设备使用同一个IP地址、已安装杀毒软件但无法扫描到、客户端注册器因服务器不稳定被自动卸载等情况，且排查耗时耗力，经常需要重复卸载、注册，严重滞后各级科信部门的工作效率和各警种的工作环境。

无法将IP地址规划、分配使用等资源以标准接口服务的形式提供给各应用系统使用。

缺少IP地址分配、注册、变更、注销等符合IP地址管理要求的在线管理流程。

通过现有入网管理系统注册的IP地址使用信息，因使用部门无长期、有效的审核机制不能确保信息规范性、准确性。

新入网设备扫描发现有延迟，存在10到30分钟甚至更久的真空期，不能及时对未知IP地址接入进行有效隔离。

现有监控系统数据库文件庞大，无数据备份以及双机热备措施，且现有服务器存储空间紧张。

### 1.4新旧IP地址更替面临风险

计算机注册人不规范，导致安全事件责任划分不清晰；

### 1.5需求分析

从IP地址管理要求上分析，要符合公安部《公安信息网IP地址资源管理办法》的管理要求。

现有设备的全网段扫描、发现、注册的方式在IP扩容后已经无法胜任，迫切需要进一步提升IP地址管理业务的办理效率以及精细化管理水平。

通过技术手段进一步明确IP地址使用人、单位等基础信息，为公安信息网使用行为审计以及事件溯源明确责任人。

提高未知入网设备的隔离能力，实现对未知IP地址的技术隔离，进一步加强终端设备入网管理。确保公安信息网安全、可靠、稳定运行。

针对现行公安网IP管理系统庞大的数据库，建设安全、稳定的运行环境。

建设目标：

建成一个全市统一的集IP规划、申请、变更、注销、监测等功能的IP地址全生命周期的管理系统。

通过软、硬手段增强对未知设备接入公安网的隔离。

缓解“一机两用”监控系统的管理压力；

提高“一机两用”监控系统的管理效率减少运行故障。

安全入网流程管理：实现计算机终端进入公安信息网首先进行安全检查，确保设备的安全性。

建设数据优化管理系统，保障监控系统的运行率。

### 1.6建设思路

##### 1.6.1终端计算机安全加固

系统通过对终端计算机安全加固，防止计算机出现一机两用事件。

**1.6.1.1硬件设备控制：**

可以对终端计算机的光驱、软驱、移动存储、蓝牙、无线网卡、PPPOE协议等功能进行管理。其中“禁用PPPOE”协议一项功能，用于禁止一些通过PPPOE协议来进行拨号上网的设备，如手机连接电脑拨号上网等，从而避免使用人员的误操作等原因造成公安网互联网的违规互联问题。

计算机IP管理功能：

系统可统一控制全网计算机，只允许规定的IP段可手动修改IP地址，超出规定的IP无法修改。无法修改IP地址的电脑，修改IP界面的“确认”按钮显示为灰色，无法点击。

系统可禁止计算机通过其他方式自动获取IP地址，保证计算机网络状态。

手机及热点共享控制功能

通过对计算机底层系统接口的控制，控制各种类型手机通过与计算机的共享上网模式导致计算机连接互联网，同时禁止计算机通过热点共享模式连接互联网。

**1.6.1.2外设网卡及随身WiFi限制**

通过智能对3/4G网卡及随身WiFi的是识别，从底层限制其在计算机上的使用。

**1.6.1.3设备网内控制规则**

对需要临时接入公安网的设备进行控制，设定其可接入公安网的生存周期，对超出生存周期的客户端进行提示、锁屏、关机、卸载等手段来阻止其继续在公安网使用。

**1.6.1.4设备离网控制规则**

对公安网设备进行控制，对于未经容许离开公安网的设备进行控制。可根据管理人员的需要设置离开公安网的生命周期；对超过生命周期的计算机可进行锁屏、锁屏并断开网络等手段来进行控制。

##### 1.6.2网络安全接入认证

**1.6.2.1强制入网认证：**

随着IP扩容后面临的各种问题，为适应不同模式下的公安信息网业务应用，网络接入控制系统应依托现有公安内网安全认证手段开展建设，目前许昌市公安信息网支持的认证模式包含“一机两用”客户端注册认证、PKI数字证书认证、防病毒软件安装强制认证、公安安全助手安装认证、PKI证书驱动入网认证。

“一机两用”客户端注册认证将对网络内计算机进行基于“一机两用”程序的认证，对未安装“一机两用”客户端程序计算机给予隔离及重定向。

PKI数字证书认证将管理网络内的人员PKI信息导出接入系统中，系统可以针对使用终端是否接入PKI进行认证。入网终端必须强制要求安装PKI证书驱动，对未PKI证书驱动的程序计算机给予隔离及重定向。

入网终端必须强制要求安装防病毒软件，对未安装防病毒软件的计算机给予隔离及重定向。

入网终端必须强制要求公安安全助手，对未公安安全助手的计算机给予隔离及重定向。

**1.6.2.2安全检查：**

安全检查是计算机终端入网的凭证，不安全的终端接入网络，将可能给网络带来无法估量的损失，例如病毒恶意传播，木马泛滥导致机密泄露，不安全策略配置导致对黑客入侵缺乏抵抗能力等。网络接入控制系统应着重针对以上问题，从终端安全加固做起，对终端可能存在的风险进行评估，并根据评估结果对终端存在的风险进行修复和加固。

用户及角色管理

在现有公安内部信息系统中，经常会对不同部门或者不同用户分配不同的管理或者访问控制权限，不同的管理和访问权限统一用角色进行划分。

网络接入控制系统应针对信息系统明确划分、区分层次结构，将部门、用户及角色有机结合起来，将角色与安检规范、安全域进行联动，实现对不同部门不同用户间不同的访问权限和规范。

**1.6.2.3安全域控制：**

安全域主要是用来控制不同用户不同角色的访问控制域，例如针对来宾用户不允许访问关键业务服务器，针对用户不能访问规定网络等，安全域控制可采用IP机制，且支持IP地址、IP段以及IP范围设置与文件目录地址设定。

**1.6.2.4入网认证日志：**

随着信息化脚步的不断迈进，许昌市公安局建设了大量的应用系统，在更加高效、便利服务于警务工作的同时，也存在安全隐患，建立详细、有效的入网日志能够更大限度确保公安信息网内数据的安全性。

网络接入控制系统应做到对全网用户的入网认证情况进行记录，可以详细记录用户入网认证的时间、用户名、认证类型、IP以及认证动作等。并且能够提供查询接口，便于查询特定用户在特定时间段内的上网情况。

##### 1.6.3数据监控及审计

**1.6.3.1桌面文件输出审计：**

对计算机的文件输出行为进行审计和管理，可根据情况审计或禁止使用打印输出、邮件输出、网络文件拷贝等文件输出行为。可根据需要禁止指定用户（组）的上述行为，或对指定用户（组）的上述行为进行审计。

**1.6.3.2移动存储设备监控和行为审计：**

通过对外部USB[移动存储设备监控和审计](http://127.0.0.1/vrveis/policy/list.asp?PolicyType=UDISK-ACTION-CONTROL)，可有效的防止信息泄漏。可以禁止USB移动存储设备的接入。保证某（些）客户端设备只允许本单位或本部门的USB移动存储设备接入。对通过USB设备进行的文件拷入、拷出的行为进行审计，记录文件名称和操作时间。可以禁止光盘的接入，设定光盘为只读状态。保证某（些）客户端设备只允许本单位或本部门的光盘可读写接入。

**1.6.3.3指定文件保护和审计功能：**

系统可保护指定的文件或文件夹，根据需要禁止本地和远程对其进行读取、修改、删除等操作。系统也可对指定的目录或文件进行读取、修改、删除等行为的审计。

**1.6.3.4用户权限变化监控功能：**

网络终端的权限一般不会被用户检查，正常的客户端用户权限极少改变，但是很多病毒和黑客的攻击很多是利用计算机上权限的变化实现的，计算机上权限的变化造成的危害往往是致命的，因此十分有必要对终端权限的变化进行监控，以告知终端用户和网络管理人员。

**1.6.3.5系统相关功能：**

当系统用户系统权限发生改变时，进行上报和客户端提示；

当系统用户系统组权限发生改变时，进行上报和客户端提示；

当系统用户增加时，进行上报和客户端提示；

当系统用户减少时，进行上报和客户端提示；

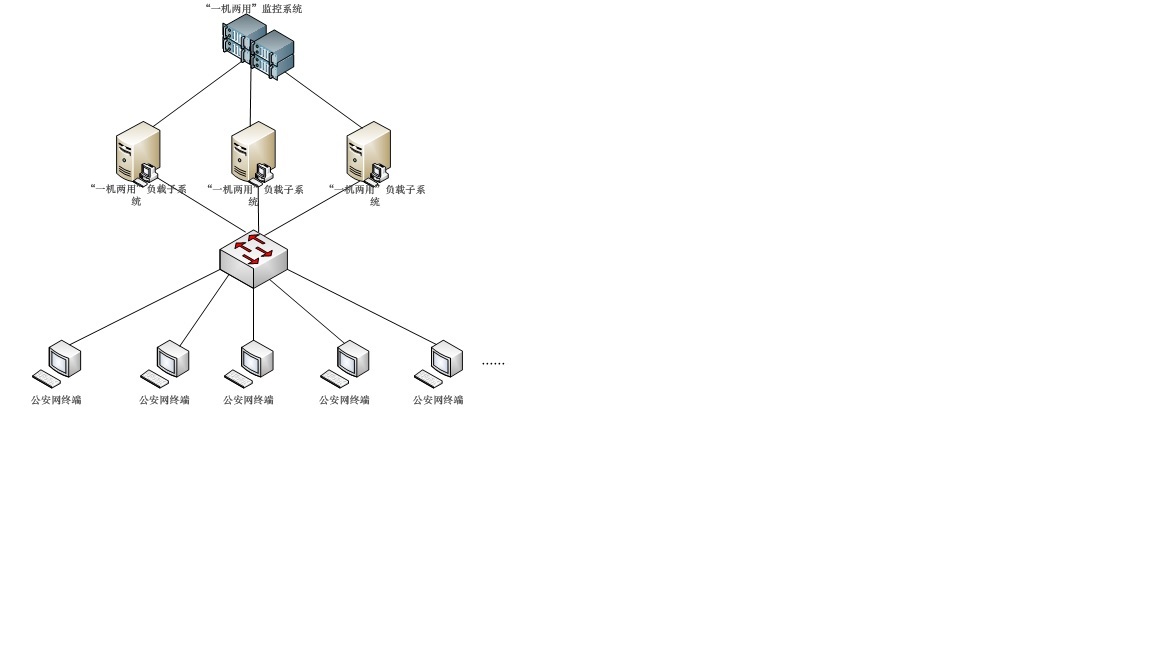
当系统用户组增加时，进行上报和客户端提示；

当系统用户组减少时，进行上报和客户端提示；

##### 1.6.4“一机两用”扫描器子系统

**1.6.4.1系统架构：**

“一机两用”扫描器子系统实现的架构如下：



注：根据实际情况制定“一机两用”扫描器子系统部署数量

**1.6.4.2部署方式：**

对于许昌市公安局，可使用5套“一机两用”扫描器子系统软件，即可管理所属区域内的所有设备。“一机两用”扫描器子系统结合公安网特殊情况，专门针对“一机两用”系统设计，无需另采购高性能机架式服务器，可部署在现有的一般性能计算机终端上即可实现扫描器均衡功能，实用性极强。

**1.6.4.3功能设计：**

“一机两用”扫描器子系统系统能有效地解决“一机两用系统”数据流量过大、网络负荷过重的问题，并且不需花费昂贵开支购置性能卓越的服务器，充分利用现有设备，其有灵活多样的部署方式，可把海量的数据流量合理地分配给多个扫描器均衡系统共同负担。即使是后期再增加大量的计算机终端，也只是简单地增加一个新的“一机两用”扫描器子系统即可，而不需改变现有网络结构、停止现有的服务。

为了降低“一机两用”的扫描压力，部署一定数量的“一机两用”扫描器子系统后，可在“一机两用”页面配置多个“一机两用”扫描器子系统的IP地址，“一机两用”系统无需进行扫描，由扫描器均衡系统按照配置的管理IP范围进行扫描，将扫描上来的数据实时汇总至“一机两用”系统，以实现扫描器均衡的目的。

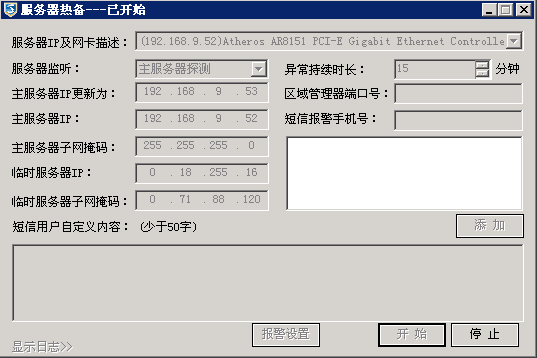
**1.6.4.4总结：**

本方案基于北信源安全管理体系核心理念，对“一机两用”扫描器子系统的解决方案进行了详细阐述，最终有效解决了IP扩容后计算机数量爆发式增长带来的管理难题，从而形成了完善的面对终端数量与日俱增的管理体系，保障了“一机两用”监控系统的稳定运行，为整个公安信息网安全管理体系建设打下坚实的基础。

##### 1.6.5双机热备

**1.6.5.1系统介绍：**

主机通过检测数据库和区域管理器状态信息，上报到报警平台，当主机发生数据库异常或区域管理器异常以及网络发生故障等原因导致无法正常使用时，通过向备机发送异常信息或者由备机自动探测主机是否存活功能，进行主备服务器的切换，备机替代主机继续工作。并将切换的信息上报给报警平台。切换过程中主机会更改为另一个IP地址，备机更改为主机的IP地址，并实现区域管理器和数据库的自动切换。



##### 1.6.6 IP迁移服务

本次许昌市公安信息网IP扩容改造还面临一项重要的工作，将原有在10.\*.\*.\*网段的公安网信息终端迁移到62.\*.\*.\*网段。常规的迁移工作有以下几个步骤：

1.停用“一机两用”监控系统的安全策略。

2.卸载老“一机两用”客户端。

3.把原有的10.\*.\*.\*IP地址修改为新增加的62.\*.\*.\*

4.重新注册新的“一机两用”客户端

此方法过于复杂容易出现失误且存在巨大的安全隐患，尤其是各种应用系统的服务器一旦出现问题，将会影响全市的警务工作和向上级部门的信息通信工作。因此，项目建设单位应配合许昌市公安局针对IP地址改造做好应对，根据本次建设内容做出具体的IP迁移方案和应急预案，保障IP迁移的安全性、准确性、时效性。

我公司提供的IP迁移服务为智能化IP地址管理方案，为许昌市公安局公安网的IP扩容与日常管理提供了有效的手段，解决了公安网中各种IP地址管理的问题，保障公安网IP扩容的稳定过度与安全运行。解决方案，具备IP地址池设置、IP地址自动分配，IP状态监管、IP状态监管日志跟踪、“一机两用”服务器IP变更等等功能，自动配置符合规范的IP地址、网关地址、子网掩码、DNS，实现了IP地址分配与更改的自动化、智能化管理。

##### 1.6.7 企业级服务器

为了跟好的配合此次项目实施还需要部署一台高性能的企业级服务器，配置要求如下：

2颗Intel Xeon E5620  2.4GHz处理器12MB L3 缓存；64GB ECC DDR3 1333 MHz内存；6\*300GB 3.5in SL HS 15K 6Gbps SAS HDD可热插拔硬盘；配置256MB高速缓存SAS RAID卡，配置电池保护，支持RAID0/1/1E/5/6/10/50/60；2块1000M高性能以太网卡；冗余服务器电源和风扇；DVD-RW

# 2实施方案

## 2.1实施目标

许昌市公安局因公安网IP进行扩容，面对海量的内网IP，一是要满足在保障公安网畅通的情况下对入网IP的过滤；二是能够对许昌市公安信息网全网段IP快速扫描，保障许昌市公安信息网的安全性、可靠性，稳定性；三是能够实现“一机两用”系统的双机热备和对终端电脑的安全加固、审计，同时提供全网IP扩容后的迁移服务。由于“一机两用”系统为全市公安信息网的重要载体，在本次升级的过程中，要确保公安网网络环境的稳定，不影响正常的公安业务。

## 2.2实施范围

项目部署范围：

部署范围包括：许昌市公安局所有公安内网用户。

项目进度实施计划

项目实施计划在技术细节上应按照投标应答文件和合同要求进单位，整体进度依据实施纲要及双方商定合同制定。

## 2.3验收标准制定

双方依据邀标文件和乙方应答文件协商审定本项目各系统验收标准。

验收标准的制定应根据：

1. IP扩容改造技术文件中所要求的技术指标以及承诺的功能；
2. 其他方面系统功能及指标，如技术培训、文档交付等。

### 2.3.1人员组织：

许昌市公安局和郑州恒信通讯科技有限公司双方应指派专门人员进单位工程的施工工作。双方各委托一名项目负责人，共同监督、管理、协调整个项目的实施。

#### 许昌市公安局人员组织

指定专门1人具体参与施工；

#### 郑州恒信通讯科技有限公司方面人员组织

项目工程实施组**：** 项目经理：胡双双 18595830859

### 2.3.2系统实施前期准备

#### 施工协调会

首先施工前期的协调会，通过协调会，明确许昌市公安局和工程实施方（郑州恒信通讯科技有限公司）的对于工程施工的任务分工和各自责任，协调实施的工作。

#### 2.3.3项目产品的安装部署

**实施进度概述**

根据用户要求，整个项目在26个工作日之内完成。

1．人员培训： 1个工作日

3．全网安装实施工期： 24个工作日

4、项目验收 1个工作日

**系统实施计划表**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 内容 | 时间 | 备注 |
|  | 制定实施计划 | 一个工作日 | （第1至2工作日） |
|  | 进行系统安装和使用培训 | 一个工作日 | （第1或2工作日） |
|  | 安装 | 5个工作日内 | （第2-7工作日） |
|  | 系统试运行、调试（包括试用点安装） | 21个工作日 | （第7-25工作日） |
|  | 系统评测、验收 | 一个工作日 | （第25-26工作日） |

### 2.3.4项目验收

#### 2.3.4.1 验收概述

在项目系统实施完毕并经过施工方仔细调试运单位后，由双方组织人员本着实事求是、科学规范、注重质量、讲求实效的原则, 依据项目邀标文件及应答，对项目的完成情况进单位总体评价验收。

验收包括：验收内容、验收组织和方式、验收结果等。

项目验收的主要依据如下：

1. 项目合同书；
2. 用户确认的项目实施方案书；
3. 相关安全技术规范和标准。

涉及该项目中的产品提供、产品安装、系统调试、技术培训、服务等，包括：项目执单位情况综合评价、项目文件验收等。

#### 2.3.4.2 验收内容

标准制定目的在于控制项目执单位质量，更好的服务于用户方，加强施工方对项目流程管理力度，保证本次项目安全系统安全、稳定、可靠运单位。

验收标准在项目实施前由双方着手商议制定，施工方在系统建设前、建设中、完工后向用户方提供个阶段的技术及相关文档，以便用户方及时了解项目进展。用户方在全面掌握整个技术方案、实施方案的基础上，同施工方共同制定本次项目验收具体标准。

郑州恒信通讯科技有限公司

日 期：2018年12月5日