**大带宽透传项目需求说明**



2013年5月13日

目录

[目录 2](#_Toc350577959)

[1. 前言 3](#_Toc350577960)

[1.1需求描述及背景 3](#_Toc350577961)

[1.2名词解释 3](#_Toc350577962)

[2. 系统功能 3](#_Toc350577963)

[2.1客户端 4](#_Toc350577964)

[2.1.1 登录 4](#_Toc350577965)

[2.1.2 客户端主界面 5](#_Toc350577966)

[2.1.3 IP查询结果界面 5](#_Toc350577967)

[2.1.4 路由信息查看界面 6](#_Toc350577968)

[2.1.5 日志查询界面 7](#_Toc350577969)

[2.2后台管理系统 7](#_Toc350577970)

[2.1.1 登录 7](#_Toc350577971)

[2.1.2 后台管理系统主界面 8](#_Toc350577972)

[2.1.3 权限管理 8](#_Toc350577973)

[2.1.4 配置管理 8](#_Toc350577974)

[2.1.5 IP查询记录 9](#_Toc350577975)

[2.1.6 路由查询 9](#_Toc350577976)

[2.1.7 后台数据库 9](#_Toc350577977)

[3. 安全核心技术 9](#_Toc350577978)

[3.1协议的选择 9](#_Toc350577979)

[3.2加密技术 10](#_Toc350577980)

[3.3检测服务器部署 10](#_Toc350577981)

[3.4检测方式 10](#_Toc350577982)

[3.5系统架构选择 10](#_Toc350577983)

[3.6 防屏蔽技术 11](#_Toc350577984)

[3.7 反镜像技术 11](#_Toc350577985)

[3.8服务器反跟踪 11](#_Toc350577986)

[4. 权限控制 11](#_Toc350577987)

[4.1 客户端权限 12](#_Toc350577988)

[4.2节点服务器权限 12](#_Toc350577989)

[4.3主控服务器权限 12](#_Toc350577990)

[5. 总结 13](#_Toc350577991)

# 前言

## 1.1需求描述及背景

**存在问题：** 目前联通个别省分公司存在将带宽违规租赁给第三方公司或其他运营商的现象，带宽在其他省份的倒卖，对带宽流入省份的联通带宽市场造成严重扰乱；

**解决方式**：省间相互监督，发现问题投诉到集团进行处理，手段较为原始；

**取证方式**： 互联网出口位置的民间查询网站（如ip138）查询，没有更科学准确的手段；

**实际困难**：从事第三方带宽租赁的公司，具有专门的技术力量来针对类似的IP查询系统进行数据处理，一旦他们发现是在进行IP查证，将会采取篡改请求结果、镜像网站服务器等，造成取证不准确 。

## 1.2名词解释

透传：是指非法将电信、联通的带宽，通过VPN等加密方式，想办法给小运营商使用，减轻小运营商的带宽成本。

C/S结构：客户端/服务器结构，是软件[系统体系结构](http://baike.baidu.com/view/3928625.htm)，通过它可以充分利用两端硬件环境的优势，将任务合理分配到Client端和Server端来实现，降低了系统的通讯开销。

# 系统功能

系统主要功能包括：

**数据加密** ：所有传输的请求、回复数据均采用私有的加密方式，保证数据的准确性，即便请求被发现，数据依然不能被篡改或镜像；

**IP管理** ：对IP地址库进行管理维护，根据IP地址库的变化，进行更新升级；

**节点管理** ：对所有部署在各省的专用监测系统的节点进行管理，动态随机分配访问请求到各个节点服务器；

**数据解析** ：对客户端访问归属进行分析判断，对于实时反馈用户端结果，并对访问的大量数据分析整理；

**用户管理**：提供用户账号注册、认证功能，对所有访问需要进行授权后进行，并对账号的访问进行记录和分析；

**授权管理**：检测系统的后台管理界面有严格的权限控制，可对每项功能进行独立授权，且后台管理系统不对外公布，仅集团指定的管理人员能够进行访问，省公司只有监测客户端的使用权限；

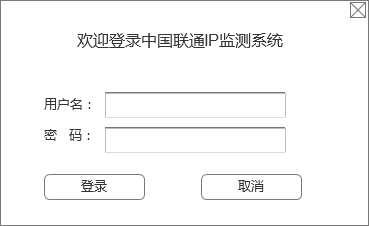
**数据库**：建立专门的数据存储数据库，存储监测数据，便于及时分析及生成报表；

## 2.1客户端

客户端应支持主流操作系统环境。用户每次使用时，自动检测是否有新版本，并自动进行版本更新。

[Yu]自动更新模块

### 2.1.1 登录

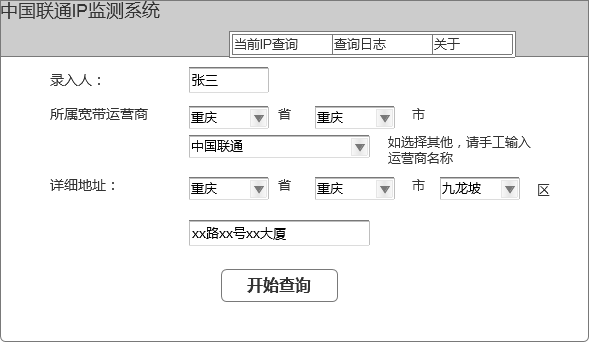


* 用户使用本客户端必须输入账号，密码。

[Yu]需要中心服务器提供认证接口, 从安全角度考虑，管理员创建用户的时候冣好需要提供网卡的物理地址作为认证的一部分。

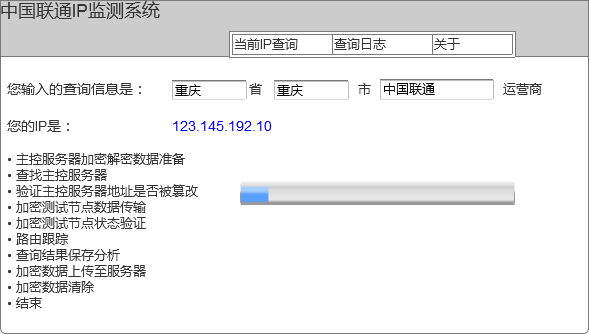
通讯用SSL加密

### 2.1.2 客户端主界面



* 用户需手工输入姓名
* 用户在下拉菜单中选择当前所在省及地市运营商。如果运营商不在下拉列表内，选择其他，再手工输入。
* 用户输入所在的详细地址
* 点击“开始查询”。

### 2.1.3 IP查询过程界面



* 过程界面显示用户输入的查询信息；
* 过程界面显示用户当前的IP地址；
* 以进度条方式，并逐步显示查询步骤

[Yu]

1. 需要从中心服务器得到目标服务器列表

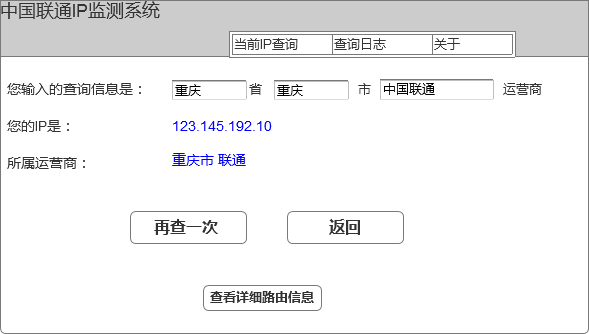
2. 逐个访问目标服务器，得到相应的路由数据－》同时实时显示测速，路由信息

3. 打包上传数据到中心服务器

4. 清除本次查询数据

5. 加密？？？一般保证传输过程的安全，本地如果没有数据存储不需要加密?

### 2.1.4 IP查询过程界面



* 查询界面展示用户手工输入的信息及查询结果；
* 显示当前IP地址；
* 显示根据IP查询出的地区（省、市）；
* 显示根据IP查询出的宽带运营商；
* 显示查询出的用户操作系统信息；
* 用户选择“再查一次”，重新发起查询请求，并返回查询结果；
* 用户选择“返回”，返回客户端主界面。
* 用户可以选择“查看详细路由信息”获取更详细的IP访问路由信息。

### 2.1.5 路由信息查看界面



* 查看更详细的IP访问路由信息。
* 返回如“tracert”命令返回信息。
* 除每一段路由经过IP地址外，增加IP解析字段，包含省、市、网络运营商信息。

[Yu]需要按目标服务器分组显示

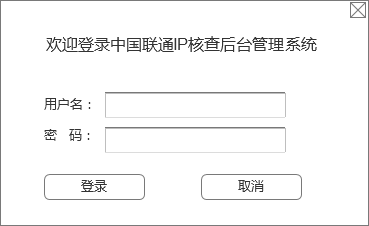
### 2.1.6 日志查询界面



* 日志查询提供本账号下所有的查询操作记录，包括“查询时间”，“用户输入信息”，“IP”及“查询结果”。 [Yu]s查询结果是什么内容？
* 用户可以查询一年内所有的操作记录
* 用户可以选择导出，将记录导出（单条，多条）为txt格式

## 2.2后台管理系统

### 2.1.1 登录



* 采用Web页面登录。
* 每次登录必须输入用户名及密码。
* 该管理系统使用者为集团系统管理员。

### 2.1.2 后台管理系统主界面



* 集团系统管理员可以进行权限分配，访问节点服务器配置操作。
* 集团系统管理员可以查看全国所有的IP查询记录。
* 后台管理系统存储一年内的数据。

### 2.1.3 权限管理

* 系统管理员可以进行账号权限及可查看信息的配置。

### 2.1.4 配置管理

* 系统管理员定期/不定期进行检测节点服务器的配置。

### 2.1.5 IP查询记录

* 系统管理员可以查看全国IP查询记录。
* 展示信息同客户端“日志查询界面” 。
* 提供条件查询。

### 2.1.6 路由查询

* 系统管理员可以查看全国路由查询记录。
* 展示信息同客户端“路由信息查询界面” 。
* 提供条件查询。

### 2.1.7 后台数据库

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **省编码** | **地市编码** | **用户IP** | **用户物理位置** | **访问时间** | **检测节点编号** | **检测节点IP** | **路由信息** |
| SD | BZ | 61.1.1.23 |  | 20120801083210 |  |  |  |
| SD | DZ | 61.1.1.21 |  | 20120801083220 |  |  |  |

# 安全核心技术

## 3.1协议的选择

大带宽透传检测系统采用了标准协议，主要提供FTP、HTTP等多种TCP/IP协议支持，用于模拟用户的实际请求，这样可以使检测系统的请求淹没在众多的常规网络请求中，从而不易被试图篡改结果的人发现，进而避免被破解。

## 3.2加密技术

私有数据加密方法，所有传输请求，回复数据均采用私有的加密方式：保证数据的准确性，即时数据被发现，数据依然不能被篡改或者镜像。进一步保证了所传输的数据的正确性、有效性。

## 3.3检测服务器部署

检测服务器采用多点部署的方式，在节点服务器在存储传递数据时容易被跟踪，从而被人篡改或者屏蔽。现在采用的多点检测技术，地址不定期的变化，从而防止检测服务器被跟踪。

## 3.4检测方式

对于ip138等对互联网出口位置的查询方式，很容易被镜像，造成查询数据的错误。为了避免这个错误的出现，我们增加了一个路由的检测，这样可以更加清楚的了解到数据传输所经历的流程。

现在我们采用的是IP检测和路由结合的检测方式，保证检测数据的准确性。

## 3.5系统架构选择

CS架构：即Client/Server (客户机/服务器) 结构。主要由客户端直接与服务器连接，传输数据。

BS架构：B/S结构即浏览器和服务器结构。

Client/Server是建立在局域网的基础上的。Browser/Server是建立在[广域网](http://baike.baidu.com/view/21956.htm) 的基础上的。

按我们现在的需求，是需要隐藏自身的IP地址，以免被跟踪，保证节点服务器在传输储存数据时数据不被篡改。

现在再分析CS和BS架构在隐藏IP地址上的优劣势：

**CS的优势**

·CS相对BS方式，数据传输加密，安全性能更高。

·CS可以隐藏目的服务器的IP地址，避免被异网运营商破解屏蔽无法使用。

·客户端通过域名方式访问中心服务器，其中中心服务器的IP地址会不定期的变更，客户端制定域名解析服务器进行域名解析，可以由有效防止对中心服务器的请求被劫持和篡改。

**BS方式的风险**

·不管网站采用的是域名还是IP地址方式，在访问的时候必定会暴露目标服务器的IP地址，在地址有限时很容易被对方屏蔽后无法使用。

所以现在所需要的是保证服务器的IP地址可以被隐藏，所以我们综合考虑采用CS架构。

·BS方式是采用标准的http协议进行数据传输，使用浏览器请求的发送和处理，上行请求和下行回复信息均无法实现有效的加密，极易造成数据的劫持和篡改。

## 3.6 防屏蔽技术

通过内置大量的主控IP并且不断更新实现的。

## 3.7 反镜像技术

根据之前的民间查询网站的查询方式，即只对IP地址进行查证，这样容易造成网址被镜像，造成查询结果不正确。

如今我们为了保证查询结果的正确性，增加了对路由的检测，从而完善了之前的查询方式。这样就很有效的防止了网址镜像。

## 3.8服务器反跟踪

主控服务器不定期更换IP地址，修改域名解析到新地址检测节点服务器不定期更改IP地址，主动向主控服务器报告，主控服务器接收到客户端检测请求，从检测节点中随机抽取2——5个节点，回复给客户端。

# 权限控制

大带宽透视监测系统主要流程如下：

·监测客户端通过域名加密请求主控服务器

·主控服务器加密下发检测节点信息

·检测客户端按收到的检测节点，依次进行测试访问、路由分析

·监测客户端件检测结果加密上传主控服务器

由以上流程划分各自的权限如下：

## 4.1 客户端权限

·客户端的物理地址

·客户登录账号、密码、登录日志

·客户端输出的IP地址

·路由访问信息

·客户端所在网络的运营商

·主控服务器的域名

·检测节点信息

## 4.2节点服务器权限

·主控服务器的下行指令

·客户端的加密请求

·主控服务器IP地址

·客户端输出的IP地址

·路由访问信息

## 4.3主控服务器权限

·客户端输出的IP地址

·节点服务器信息

·客户端的物理地址

·客户登录账号、密码、登录日志

·路由信息

·客户端所在网络运营商

# 总结