**使用手册**

# **目录**

[1. 系统访问说明 1](#_Toc145956088)

[2. 系统登录 1](#_Toc145956089)

[2.1. 模块说明 1](#_Toc145956090)

[2.2. 操作步骤 1](#_Toc145956091)

[3. 流量采集 2](#_Toc145956092)

[3.1. 模块说明 2](#_Toc145956093)

[3.2. 操作步骤 3](#_Toc145956094)

[3.2.1. 流量采集功能 3](#_Toc145956095)

[3.2.2. 流量下载功能 4](#_Toc145956096)

[3.2.3. 流量详情查看功能 4](#_Toc145956097)

[4. 业务分类 5](#_Toc145956098)

[4.1. 模块说明 5](#_Toc145956099)

[4.2. 操作步骤 8](#_Toc145956100)

[4.2.1. 业务类别映射功能 8](#_Toc145956101)

[4.2.2. 文件上传功能 9](#_Toc145956102)

[4.2.3. 特征提取功能 10](#_Toc145956103)

[4.2.4. 业务分类模型训练功能 11](#_Toc145956104)

[4.2.5. 业务分类功能 12](#_Toc145956105)

[5. 异常检测 13](#_Toc145956106)

[5.1. 模块说明 13](#_Toc145956107)

[5.2. 操作步骤 14](#_Toc145956108)

[5.2.1. 查看异常检测历史功能 14](#_Toc145956109)

[5.2.2. 启动异常检测功能 14](#_Toc145956110)

[5.2.3. 查看异常检测详情功能 15](#_Toc145956111)

[6. IP地址画像 16](#_Toc145956112)

[6.1. 模块说明 16](#_Toc145956113)

[6.2. 操作步骤 17](#_Toc145956114)

# 系统访问说明

在完成系统部署并启动后，可使用任一现代浏览器终端访问系统页面。

# 系统登录

## 模块说明

落地页面如下图所示：



该页面由多个链接组成，可以在这里看到系统的主要功能，以及联系方式等。

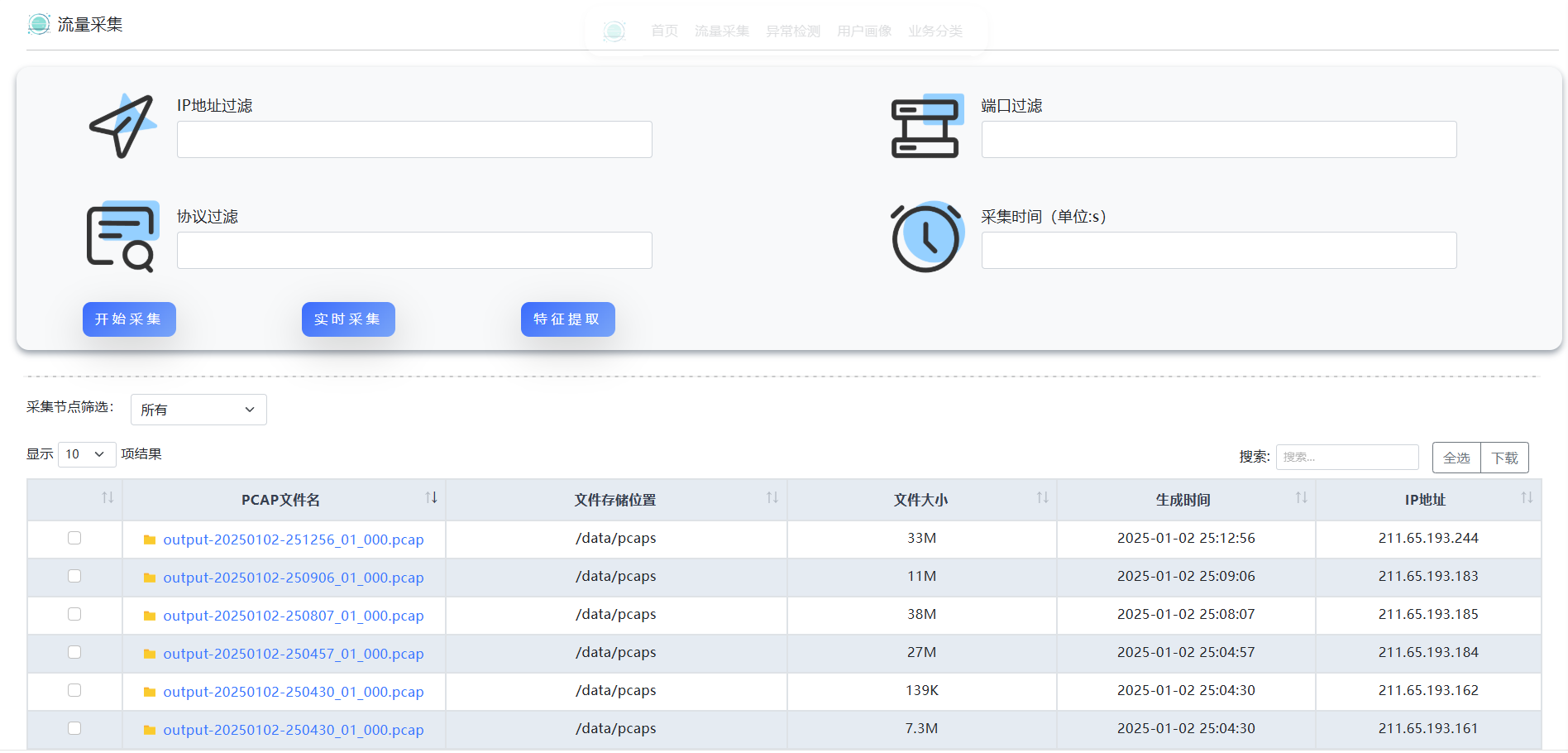
## 操作步骤

1. 在浏览器中输入“localhost:?”，自动跳转至落地页
2. 点击功能按钮，进入各个功能页。

# 流量采集

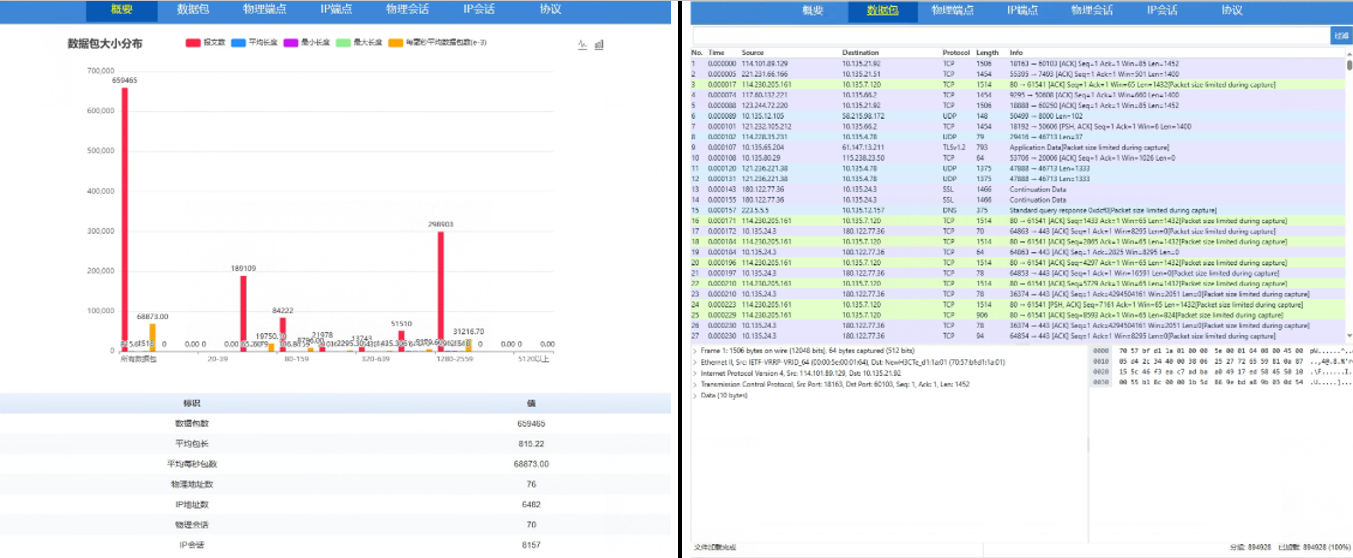
## 模块说明

流量采集模块页面如下图所示，上边为导航栏，上边的导航栏用于切换模块操作。下方区域是流量采集模块的展示内容，在还未进行流量采集操作是，该区域由两部分组成，上面是一个输入表单，用于输入采集的条件，包括采集的IP地址、端口、协议以及采集时间。下面是一个表格，显示了当前服务器中已采集的流量信息。



进行流量采集后流量采集模块的前端页面会变化成如上图所示，中间区域新增了一个显示当次流量采集的统计信息，并使用图片的形式进行展示。包括采集的包数量随时间的变化趋势以及丢包情况。

本模块还提供流量详情查看功能，可在线查看报文的统计信息和详细内容，其页面如下图所示。



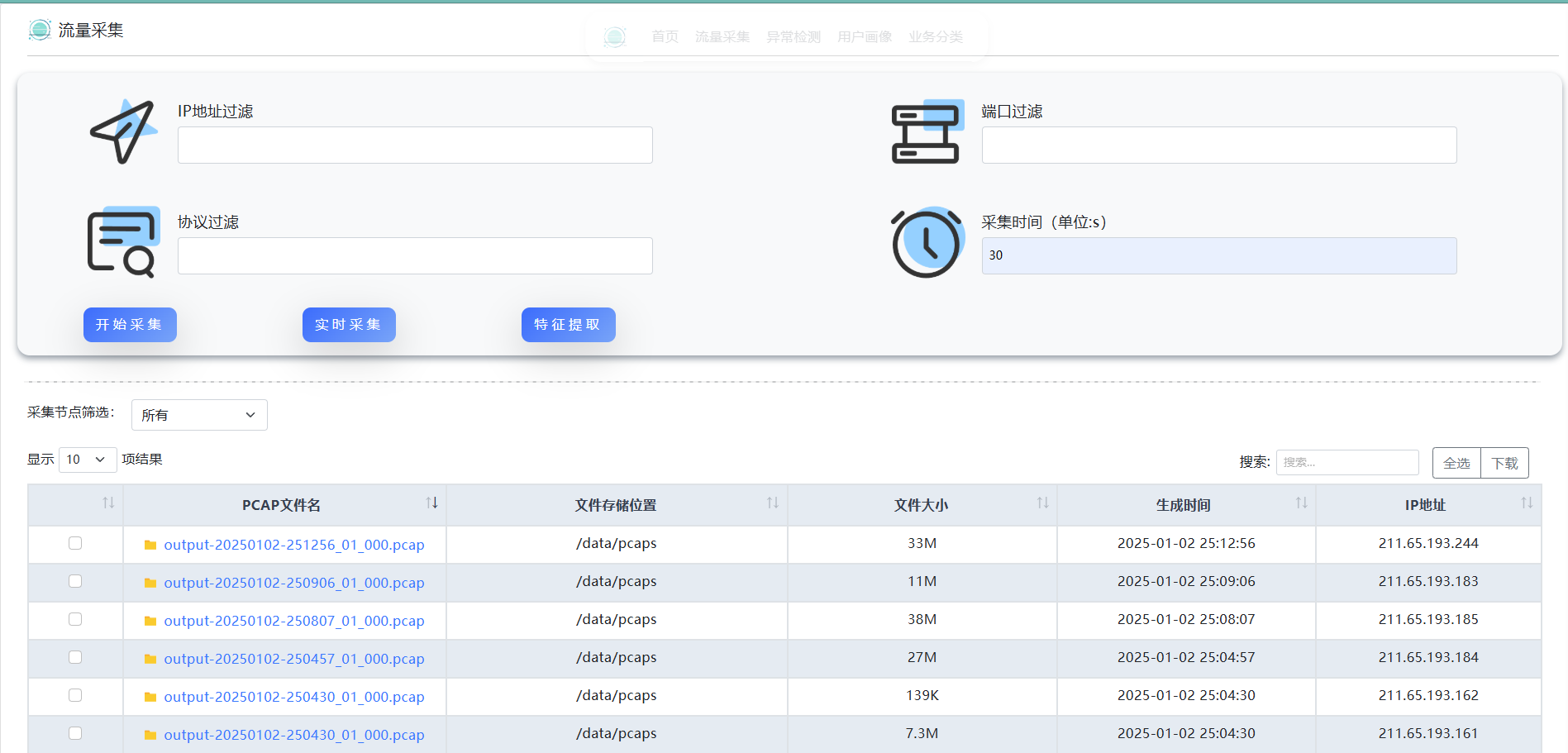
本模块还提供在线特征提取功能，可实时进行流特征提取，其页面如下图所示。



## 操作步骤

### 流量采集功能

1. 点击导航栏的“流量采集模块”；
2. 根据需要输入流量采集过滤条件；
   1. 若不输入IP地址过滤项，则默认抓取所有被管网内IP地址产生的流量；
   2. 若不输入端口过滤项，则默认抓取所有端口的流量；
   3. 若不输入协议过滤项，则默认抓取所有协议的流量；
   4. 若不输入采集时间项，则默认抓取10秒钟的流量；
3. 点击“开始采集”按钮，等待采集结果；
   1. 若输入的IP地址项不正确，则提示输入有误；
   2. 若采集成功，则显示当次流量采集的统计信息，并使用图片的形式进行展示。包括采集的包数量随时间的变化趋势以及丢包情况。
   3. 若采集失败，则系统进行提示。



### 流量下载功能

* 1. 选中需要下载的流量包左侧的复选框（全选可使用右上角的“全选”按钮）
  2. 点击右上角的“下载”按钮，即可通过浏览器下载流量包



### 流量详情查看功能

1. 在“流量采集”页面中点击需要查看的流量包文件名
2. 在弹出的新窗口查看流量详情
3. 点击页面顶端的“导航栏”可切换至相应的“统计信息”
4. 点击“导航栏”中的数据包，稍等片刻可切换至报文详情页面
   1. 输入过滤语句以过滤特定报文（默认为空字符串）
   2. 点击“过滤”按钮以使用新的过滤语句重新加载报文详情页面
   3. 点击选中感兴趣的报文条目以显示报文详细内容





### 流特征提取功能

1. 根据需要输入流量采集过滤条件；
   1. 若不输入IP地址过滤项，则默认抓取所有被管网内IP地址产生的流量；
   2. 若不输入端口过滤项，则默认抓取所有端口的流量；
   3. 若不输入协议过滤项，则默认抓取所有协议的流量；
   4. 若不输入采集时间项，则默认抓取10秒钟的流量；
2. 点击“特征提取”按钮；
   1. 若输入的IP地址项不正确，则提示输入有误；
   2. 若采集成功，则显示当次流量采集的统计信息，并使用图片的形式进行展示。包括采集的包数量随时间的变化趋势以及丢包情况。
   3. 若采集失败，则系统进行提示。
3. 点击停止即可停止流特征提取，点击导出可以导出特征文件。

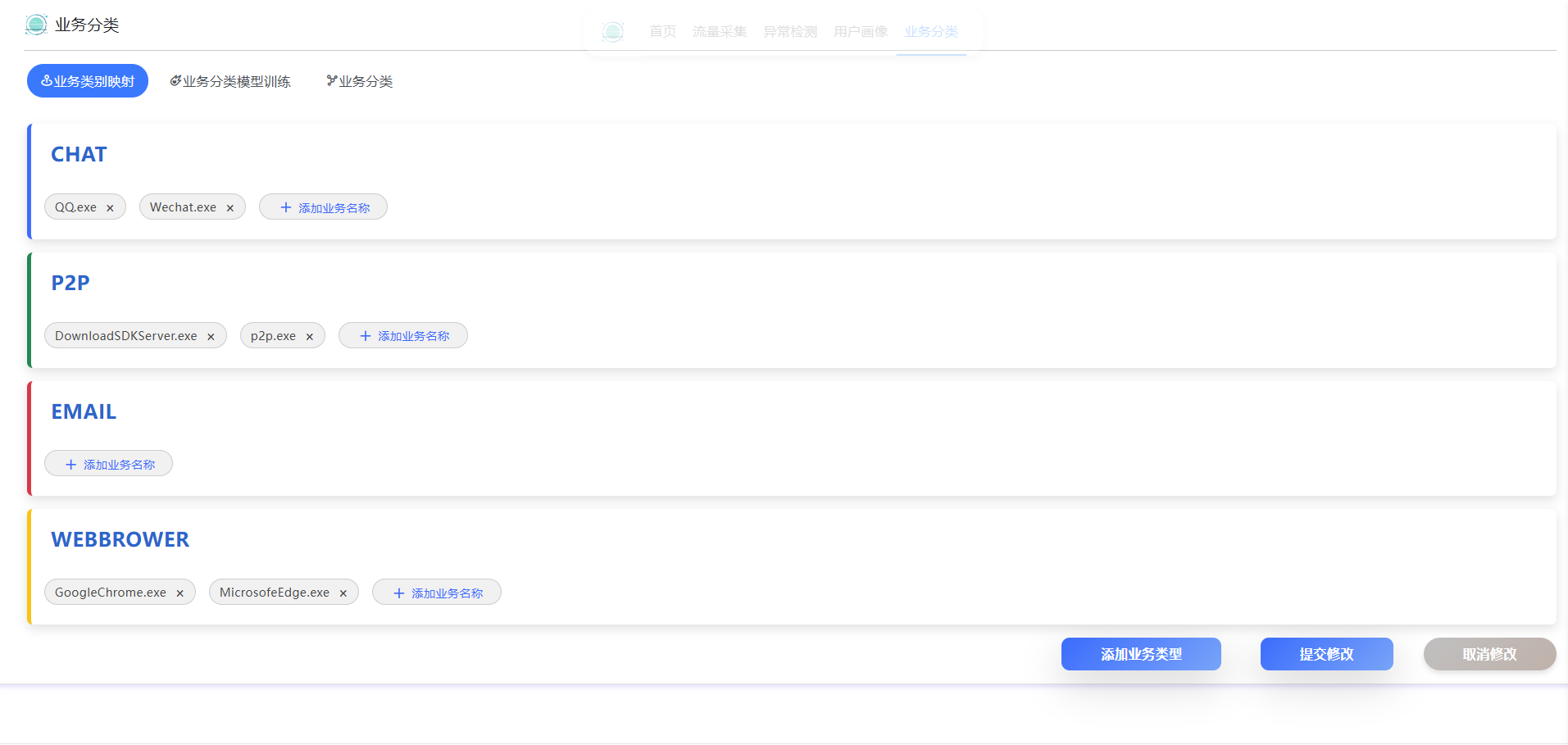


# 业务分类

## 模块说明

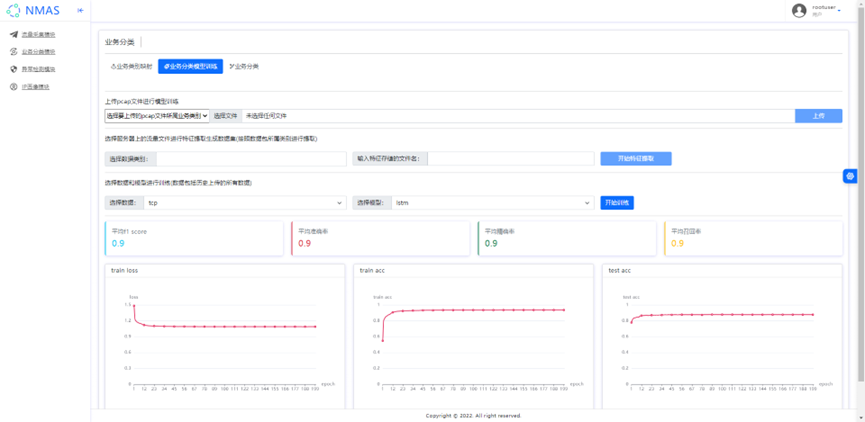
业务分类模块总共包括三个功能，分别是业务类别映射功能、业务分类模型训练功能以及业务分类功能。

业务类别映射功能页面如下图所示，该页面显示了当前所使用的分类业务类型以及各业务类型对应的程序名称。该页面可以是的用户能够自定义需要分类的业务类别和各类别对应的程序。



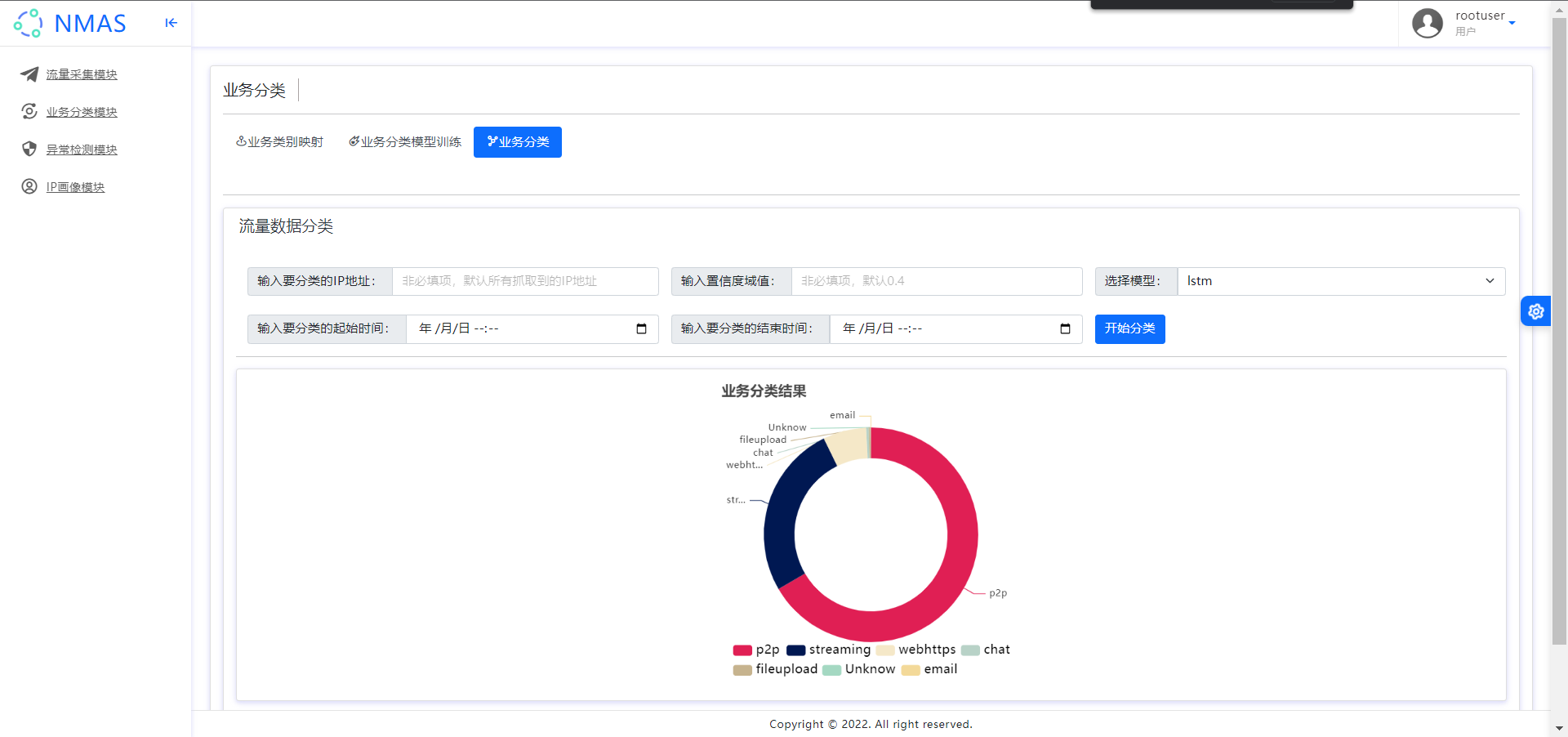
进行模型训练前的业务分类模型训练功能页面如下图所示，在该页面能够进行上传pcap文件用于模型训练、选择上传的流量文件进行特征提取以及基于提取的特征进行模型训练这三个行为，在进行完模型训练后在该页面底部会展示该次模型训练的结果，包括模型的f1 score、准确率、精确率和召回率。





进行分类前的业务分类功能页面如下图所示，在该页面能够选择流量分类的各个参数，包括要分类的IP地址、分类的置信度、分类使用的模型以及分类数据的时间段。在完成业务分类后，在该页面底部会通过饼图的方式展示该次业务分类的结果。

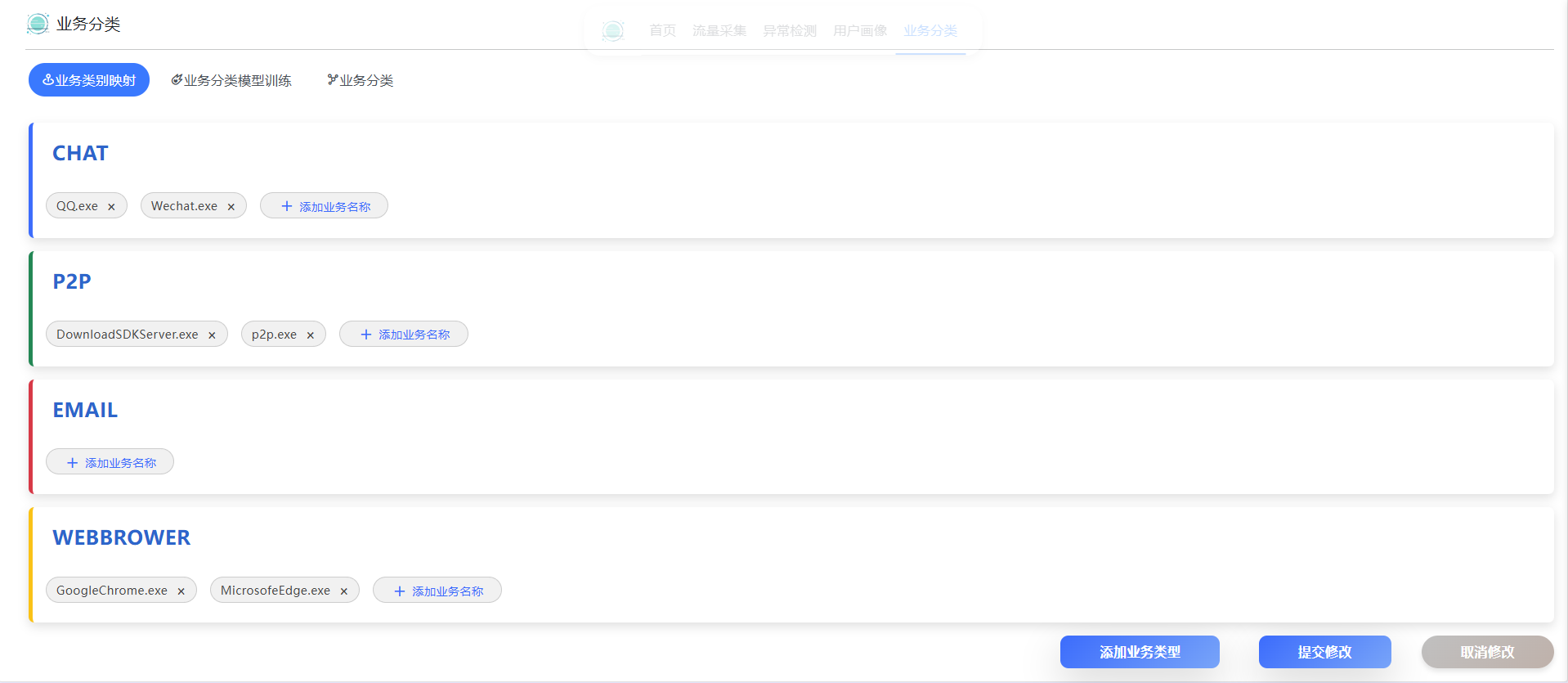




## 操作步骤

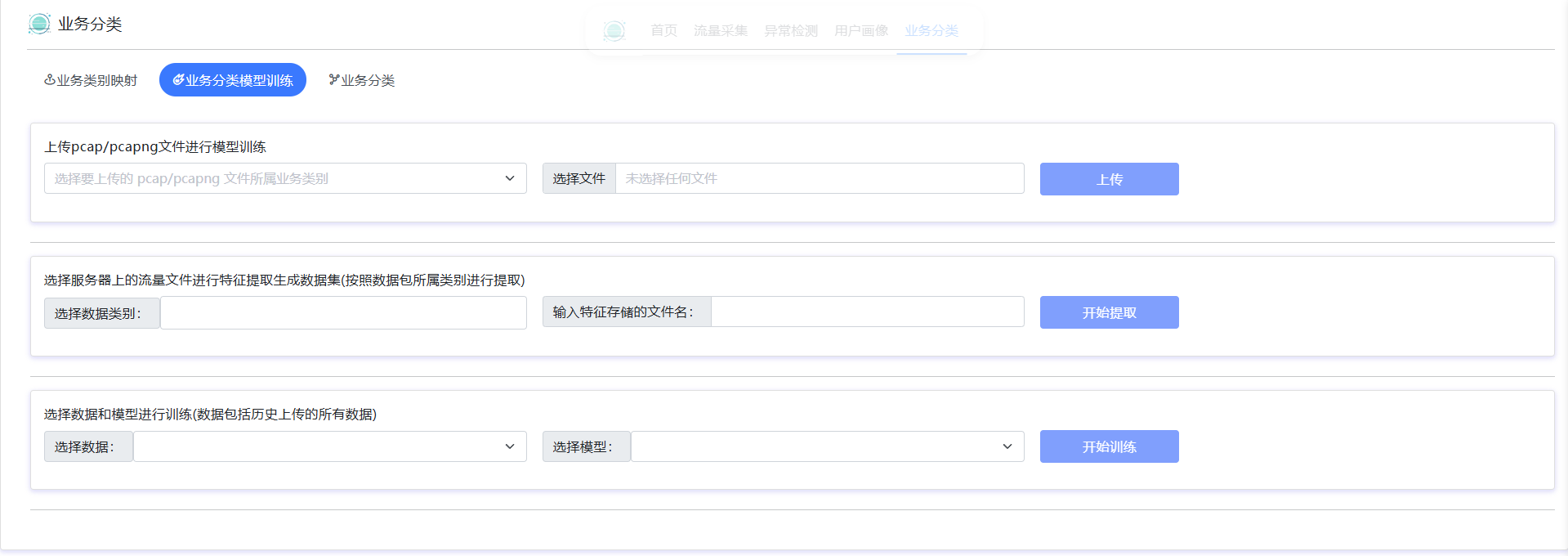
### 业务类别映射功能

1. 点击导航栏的“业务分类模块”；
2. 点击导航栏的“业务类别映射”；
3. 根据页面修改业务类别和各业务类别包含的程序；
   1. 若要添加新的业务类别，则点击添加业务类别按钮，然后跳转到4.1步；
   2. 若要给某一个业务类别添加新的程序，则点击该业务类别区域的添加业务名称按钮，然后跳转到4.2步；
   3. 若要删除现有的业务类别，则点击要删除业务类别区域最右边的“×”图标；
   4. 若要删除某一类业务类别中的某一个程序，则点击该程序区域右边的“×”图标；
4. 弹出对话框；
   1. 在弹出的对话框中输入要添加的业务类别，然后点击“是”按钮；
   2. 在弹出的对话框中输入要添加的程序名称，然后点击“是”按钮；
5. 重复步骤1和步骤2直至完成所有修改，然后点击“提交修改”按钮；
   1. 页面根据后端返回结果提示是否修改成功。



### 文件上传功能

1. 点击导航栏的“业务分类模块”；
2. 点击导航栏的“业务分类模型训练”；
3. 选择要上传的pcap/pcapng文件所属业务类别；
4. 选择要上传的pcap/pcapng文件；
5. 点击“上传”按钮；
   1. 若未选择要上传的文件所属业务类别则无法点击“上传”按钮
   2. 若未选择文件则提示未选择文件。
   3. 若选择的文件不是pcap/pcapng文件，则提示选择的文件格式错误。
   4. 页面根据后端返回结果提示文件是否上传成功。

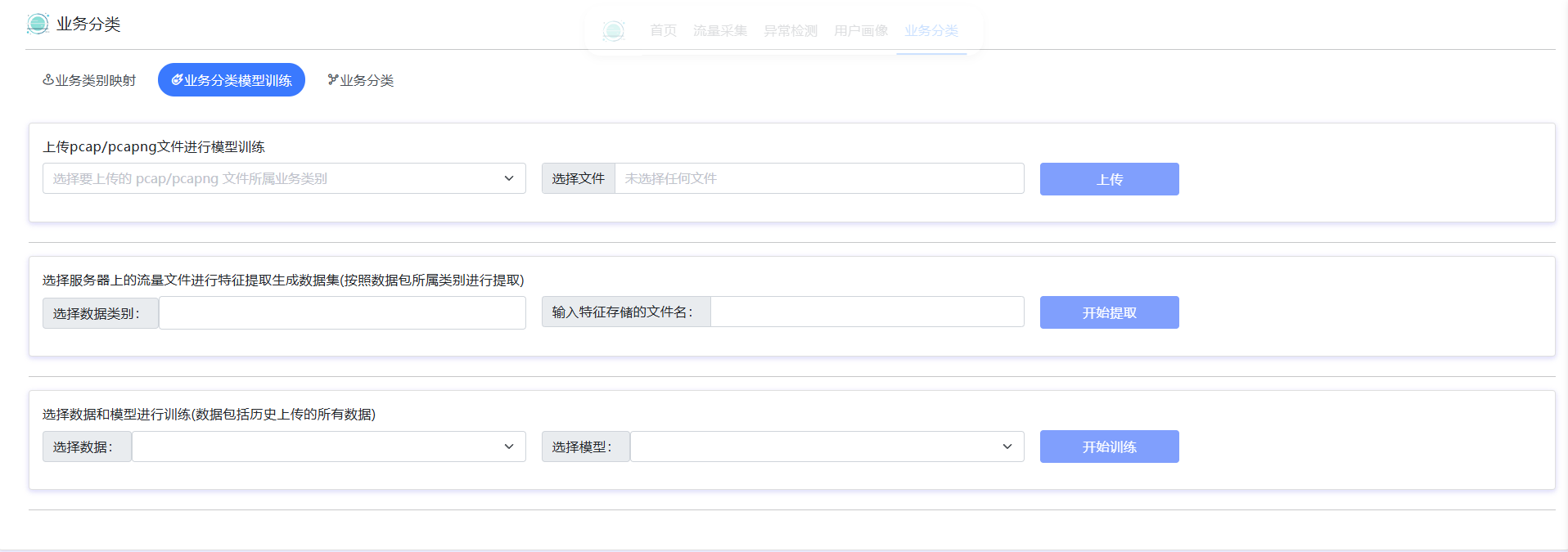


### 特征提取功能

1. 点击导航栏的“业务分类模块”；
2. 点击导航栏的“业务分类模型训练”；
3. 选择要进行特征提取的数据类别；
4. 输入存储特征提取结果的文件名；
5. 点击“开始特征提取”按钮；
   1. 若未选择数据类别和未输入存储特征提取结果的文件名则无法点击“开始特征提取”按钮。
   2. 页面根据后端返回结果提示特征是否提取成功。

### 业务分类模型训练功能

1. 点击导航栏的“业务分类模块”；
2. 点击导航栏的“业务分类模型训练”；
3. 选择训练要使用的数据，该数据为特征提取功能提取出的特征数据；
4. 选择训练要使用的模型；
5. 点击“开始训练”按钮，等待训练结果；
   1. 若未选择要进行训练的数据和未选择要进行训练的模型则无法点击“开始训练”按钮；
6. 若后端返回训练成功；
   1. 若选择的模型是lstm模型，则显示该次训练的平均f1 score、平均准确率、平均精确率和平均召回率；并绘制训练过程中loss、训练集准确率和测试集准确率的变化情况。
   2. 若选择的模型是classic模型，则仅显示该次训练的平均f1 score、平均准确率、平均精确率和平均召回率。
7. 若后端返回训练失败，则系统提示训练失败。



### 业务分类功能

1. 点击左侧导航栏的“业务分类模块”；
2. 点击中间导航栏的“业务分类”；
3. 根据需要输入流量分类参数条件；
   1. 若不输入要分类的IP地址项，则默认分类所有被管网内IP地址产生的流量；
   2. 若不输入置信度域值项，则默认为0.4；
   3. 若不选择分类模型，则无法点击“开始分类”按钮；
   4. 若选择要分类的起始时间和结束时间，则默认分类最新还未分类的流量数据；
4. 点击“开始分类”按钮，等待分类结果
   1. 若输入的IP地址项不正确，则提示输入有误；
   2. 若输入的置信度项不正确，则提示输入有误；
5. 若后端返回分类成功，则使用饼图绘制分类结果。
6. 若后端返回分类失败，则系统提示分类失败。



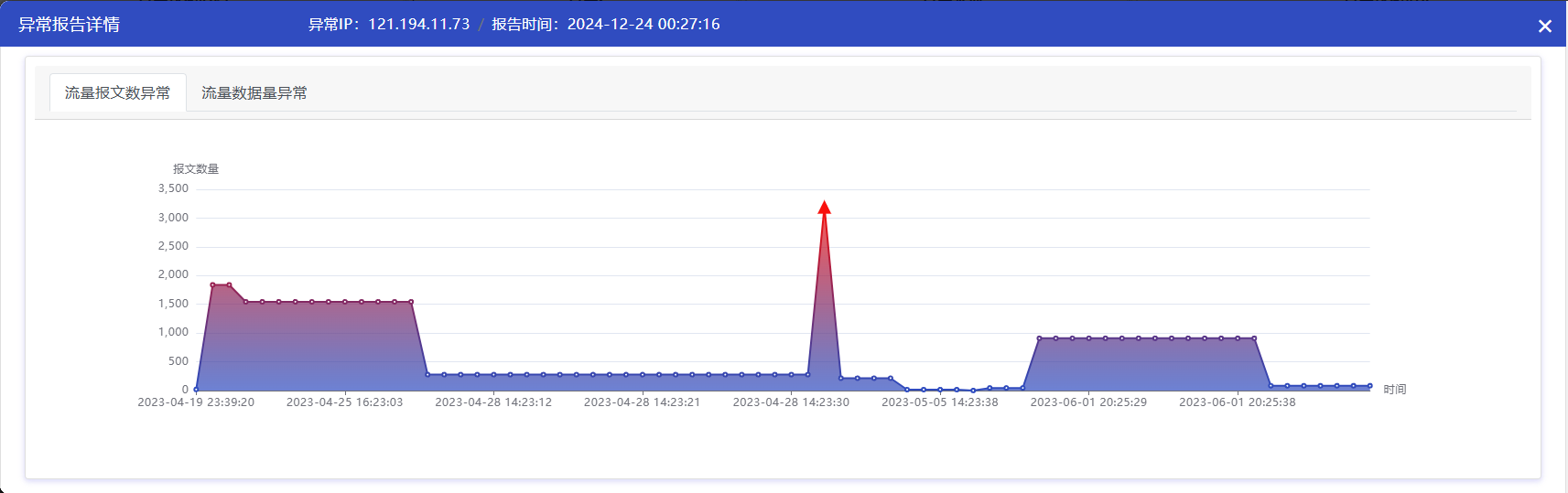
# 异常检测

## 模块说明

异常检测模块能够对四种异常进行检测，即“流业务类型异常”、“流量报文数异常”、“流量数据量异常”、“流量时间异常”。该模块按照IP地址为粒度进行异常检测，展示所有检测轮次检测出的异常IP地址以及检测出的异常，并能够查看异常检测的详细结果，其页面如下图所示。



该页面包括一个“开始检测”按钮和一个展示异常检测历史的表格，通过点击“开始检测”按钮能够手动进行异常检测。异常检测历史表格有四列，异常检测时间表示此次异常检测轮次的时间，异常IP表示此次检测出异常的IP地址，异常类型表示此次异常检测此IP地址检测出的异常类别，异常检测报告内是一个按钮，点击后跳转到此次异常检测的详情页面，如下图所示：



该页面展示了此次异常检测某IP地址所检测出来的异常详情，对于流业务类型异常，系统通过表格进行展示，展示了异常流的一些信息，包括流的源IP地址、宿IP地址、源端口、宿端口、协议号、报文数、字节数和持续时间。对于其他三种异常类型，即流量报文数异常、流量数据量异常和流量时间异常，系统通过折线图的形式进行展示，并通过红色三角形标注出异常点。

## 操作步骤

### 查看异常检测历史功能

1. 点击导航栏的“异常检测模块”，等待后端返回结果；
2. 若后端成功返回异常检测历史，则显示一个表格，记录了异常检测历史结果；
3. 若后端返回失败，则系统提示获取异常检测历史结果失败。

### 启动异常检测功能

1. 点击导航栏的“异常检测模块”，等待后端返回结果；
   1. 若后端成功返回异常检测历史，则显示一个表格，跳转到步骤2；
   2. 若后端返回失败，则系统提示获取异常检测历史结果失败，直接结束；
2. 点击“开始检测”按钮，并等待后端返回异常检测结果；
3. 若后端返回检测成功；
   1. 系统提示检测成功并提示新检测出的异常数目，并更新表格。
4. 若后端返回检测失败；
   1. 系统提示检测失败。



### 查看异常检测详情功能

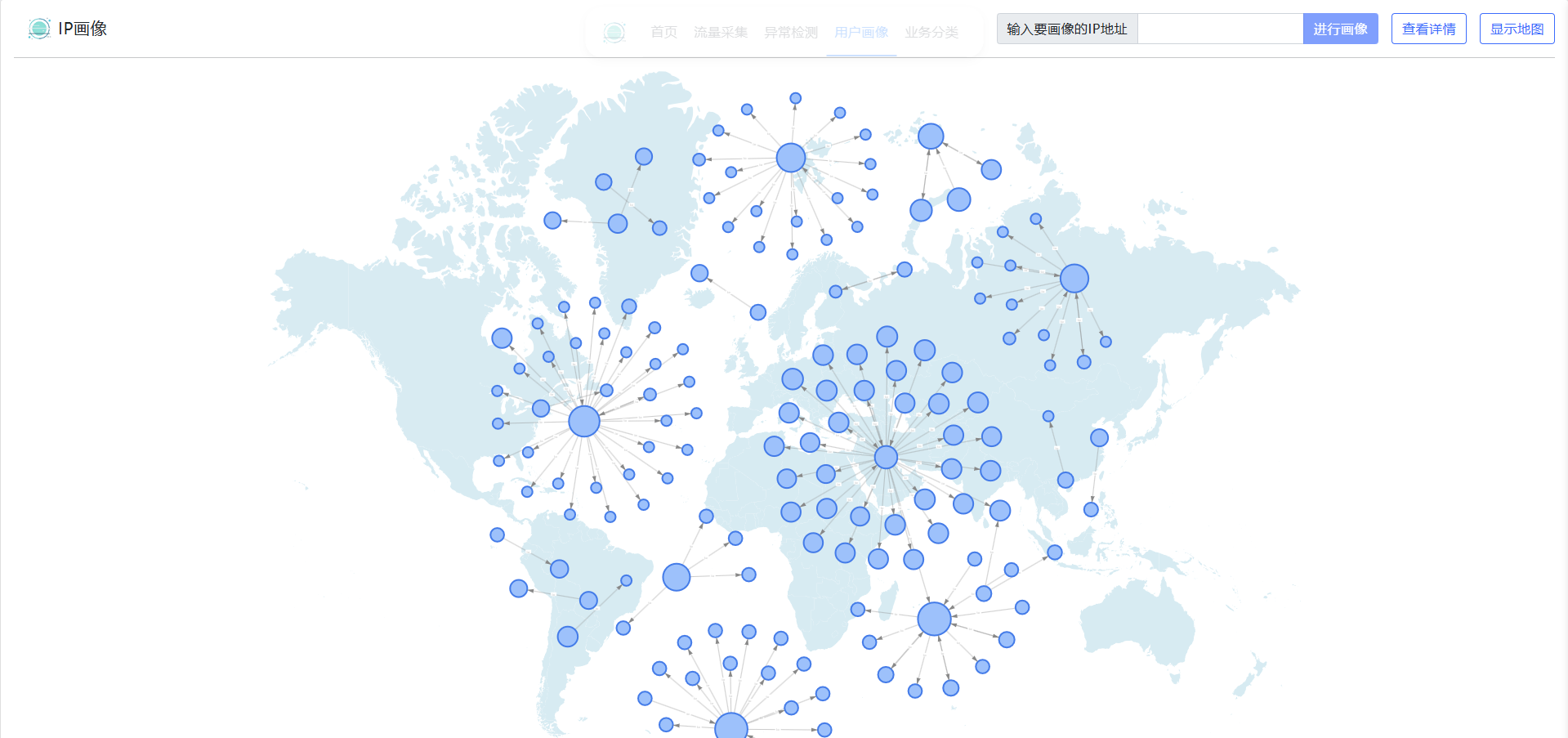
1. 点击导航栏的“异常检测模块”，等待后端返回结果；
   1. 若后端成功返回异常检测历史，则显示一个表格，跳转到步骤2；
   2. 若后端返回失败，则系统提示获取异常检测历史结果失败，直接结束；
2. 点击要查看详情的异常检测报告列，等待页面跳转以及后端返回查看异常检测详情结果；
3. 若后端返回检测成功；
   1. 进行页面跳转，并在新页面展示异常检测详细信息。
4. 若后端返回检测失败；
   1. 进行页面跳转，并在新页面提示获取异常检测详细信息失败。



# IP地址画像

## 模块说明

IP地址画像模块能够基于IP地址的历史流量数据对所选择的IP地址进行画像，其页面如下图所示。

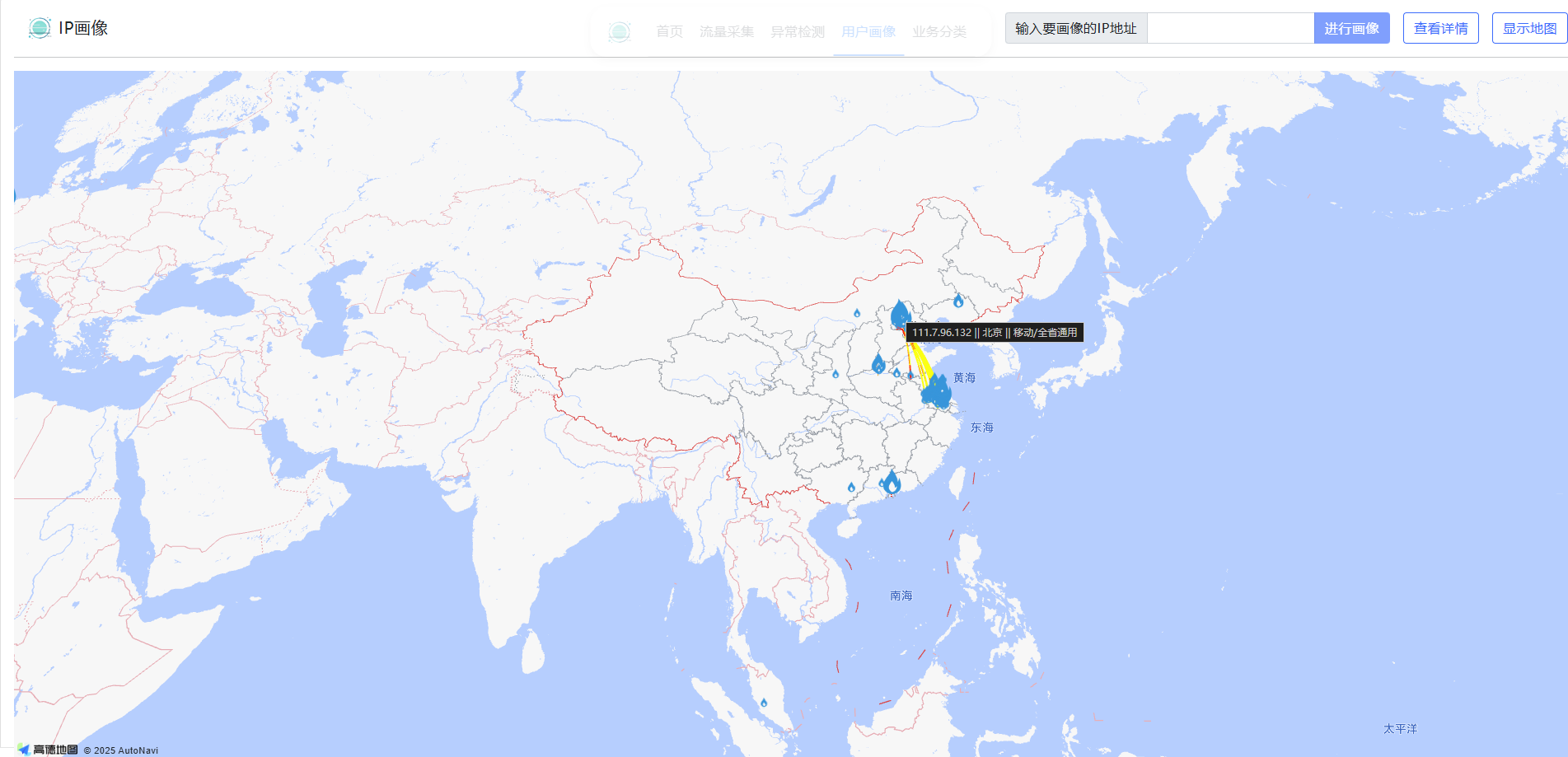


该页面上方是一个输入框和按钮，这里可以通过手动的输入IP地址的方式对输入的IP地址进行画像。下方是通过知识图谱展示的数据库中前300个IP地址的连接情况（由于前端浏览器资源限制，展示过多IP地址会造成浏览器无法运行），可以通过点击知识图谱中的节点查看该节点IP地址的画像结果。画像结果的详细信息通过一个对话框进行展示，如下图所示。



在画像详情中，通过图表的形式展示了该IP地址所抓取流量的报文总数、字节总数、流持续时间均值和流的业务分类结果。

该模块提供根据地理位置显示IP功能，可以看到各个地区之间IP的关系。



## 操作步骤

1. 点击导航栏的“IP画像模块”，等待后端返回结果；
   1. 若后端成功返回前300个IP地址的连接关系，则通过知识图谱的方式进行展示；
   2. 若后端未成功获取前300个IP地址的连接关系，则知识图谱部分为空白；
2. 选择要查看画像的IP地址；
   1. 通过输入的方式，输入要查看画像的IP地址，点击进行画像按钮，等待后端返回该IP地址画像结果；
   2. 通过点击知识图谱上IP地址节点的方式，等待后端返回该IP地址画像结果；
3. 若后端返回画像成功，则通过一个对话框展示画像结果。
4. 若后端返回画像失败，则系统提示画像获取失败。
5. 点击“显示地图”按钮，可以看到在地图上显示的IP地址。

