

中华人民共和国通信行业标准

YD/T 3279—2017

基于承载网感知的 P2P 流量优化技术 网络匹配服务器发现协议

**Specification for carrier network aware P2P traffic optimization—
Network matching server discovery protocol**

2017-11-07 发布

2018-01-01 实施

中华人民共和国工业和信息化部 发布

目 次

前言.....II

1 范围..... 1

2 规范性引用文件..... 1

3 术语、定义和缩略语..... 1

 3.1 术语和定义..... 1

 3.2 缩略语..... 2

4 网络匹配服务器发现协议概述..... 2

5 通信流程..... 2

6 协议规范..... 4

 6.1 消息整体格式..... 4

 6.2 请求消息..... 4

 6.3 响应消息..... 5

7 安全性考虑..... 6

前 言

本标准是基于承载网感知的 P2P 流量优化技术系列标准之一。该标准系列包括：

- 基于承载网感知的 P2P 流量优化技术总体技术要求
- 基于承载网感知的 P2P 流量优化技术 网络匹配服务协议
- 基于承载网感知的 P2P 流量优化技术 网络匹配服务器发现协议
- 基于承载网感知的 P2P 流量优化技术 网络匹配服务器注册协议

本标准按照 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：中国科学院计算技术研究所、中国科学院声学研究所、华为技术有限公司、中国信息通信研究院。

本标准主要起草人：李彦君、张国清、傅川、张棣、周旭、张国强、宋海滨、杨景。

基于承载网感知的 P2P 流量优化技术

网络匹配服务器发现协议

1 范围

本标准规定了基于承载网感知的 P2P 流量优化框架中的网络匹配服务器发现协议，定义了网络匹配服务客户和网络匹配服务发现服务器两个功能实体之间的查询和响应消息及流程。

本标准适用于网络运营商和 P2P 内容提供商合作以利用承载网信息优化 P2P 流量的方案和系统。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

YD/T 1614—2007 公众 IP 网络安全要求——基于数字证书的访问控制

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

承载网 carrier network

网络运营商管理的用于支撑 Internet 应用和业务的网络，这里指 IP 网络。

3.1.2

基于承载网感知的 P2P 流量优化 carrier network aware P2P traffic optimization

能够感知承载网状况并用承载网信息优化 P2P 流量同时改善 P2P 性能的技术或方案。

3.1.3

网络匹配服务 network matching service

分布在 Internet 上，能够被 P2P 应用访问，根据承载网状况指导 P2P 应用与承载网匹配的功能服务。网络匹配服务是对基于承载网感知的 P2P 流量优化技术的实现。

3.1.4

网络匹配服务发现服务器 network matching server discovery server

用于提供网络匹配服务器的注册和发现功能。网络运营商将自己的网络匹配服务器的地址、端口和策略注册到网络匹配服务发现服务器上，网络匹配发现服务器负责将网络匹配服务器信息发送给网络匹配服务发现客户。

3.1.5

网络匹配服务发现客户 network matching server discovery client

网络匹配服务器发现协议的客户端。向网络匹配服务发现服务器提交网络匹配服务器发现请求，接收网络匹配服务发现服务器的响应消息。

3.2 缩略语

下列缩略语适用于本文件。

DDOS	分布式拒绝服务	Distributed Denial of Service
IP	互联网协议	Internet Protocol
IPv4	互联网协议版本 4	Internet Protocol Version 4
IPv6	互联网协议版本 6	Internet Protocol Version 6
P2P	对等网络	Peer to Peer
UDP	用户数据包协议	User Datagram Protocol

4 网络匹配服务器发现协议概述

网络匹配服务器发现协议是一个基于客户—服务器模式的无状态协议。它定义了网络匹配服务发现客户和网络匹配服务发现服务器两个功能实体之间的交互协议。网络匹配服务发现客户通过向网络匹配服务发现服务器发送请求获取授权给该网络匹配服务客户的网络匹配服务器信息。

网络匹配服务器通过不同的策略来授权允许访问该网络匹配服务器的客户。网络匹配服务器将这些策略注册到网络匹配服务发现服务器上。当网络匹配服务发现服务器接收到网络匹配服务发现客户的发现请求时，网络匹配服务发现服务器根据网络匹配服务发现客户提供的输入信息去查找策略库，返回给网络匹配服务发现客户满足策略的网络匹配服务器信息。

网络匹配服务器提供的授权方式是授权给某个网段，即由网络匹配服务提供商向默认网段内的主机和应用开放网络匹配服务。网络匹配服务器将授权策略集注册到网络匹配服务发现服务器上。

5 通信流程

网络匹配服务发现客户与网络匹配服务发现服务器的交互流程见图 1，相应的消息处理流程见图 2。图 1 中相关步骤说明如下：

- 步骤（1）：网络匹配服务发现客户向网络匹配服务发现服务器发送请求；
- 步骤（2）：网络匹配服务发现服务器提取请求消息的 IP 地址，向策略库发送查询请求；
- 步骤（3）：策略库返回授权给该 IP 地址的网络匹配服务器；
- 步骤（4）：网络匹配服务发现服务器构造响应消息，将网络匹配服务器的服务地址发送给网络匹配服务发现客户。

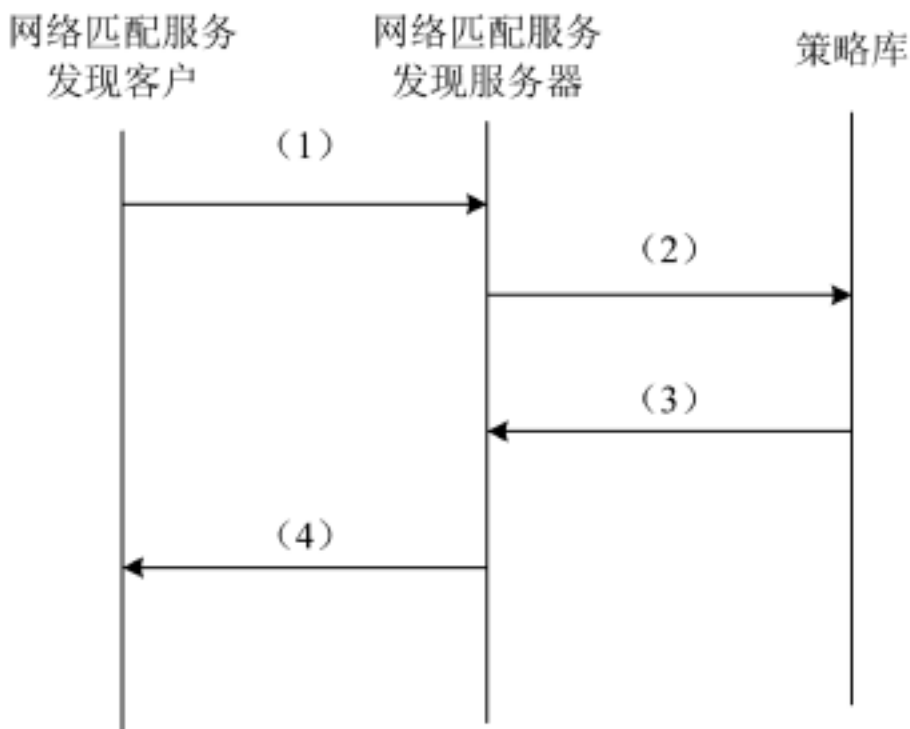


图 1 匹配网络服务发现交换协议交互流程

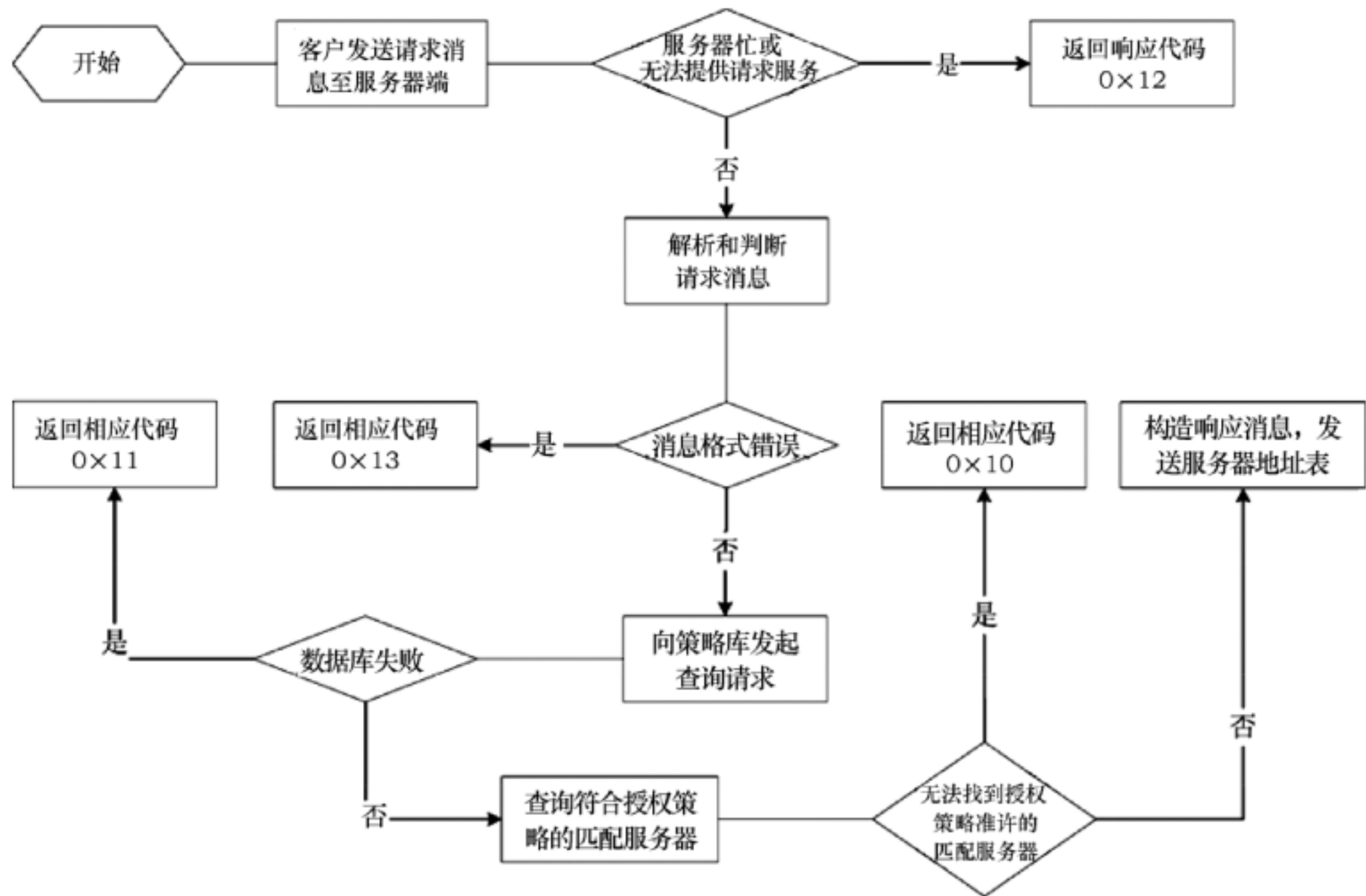


图 2 匹配网络服务发现交换协议消息处理流程

6 协议规范

6.1 消息整体格式

网络匹配服务发现协议依托 UDP 协议进行传输，网络匹配发现服务器将采用固定的端口号接收网络匹配服务发现客户的请求消息，具体的端口号分配在本标准中不作规定。

版本号 1 byte	消息类型 1 byte	消息体长度 2 byte
消息序列号 2 byte		填充字段
消息体		

图 3 网络匹配服务器发现协议的总体消息格式

图 3 给出了网络匹配服务器发现协议的总体消息格式。其中，各字段的含义如下。

- a) 版本号：当前版本号为 0x01，表示第一版本。
- b) 消息类型，取值如下：
 - 1) 0x01 请求消息；
 - 2) 0x02 响应消息。
- c) 消息体长度：指整个消息的长度，以字节为单位。可以通过总长度与首部长度确定消息体的起始位置与长度。
- d) 消息序列号：用于为请求消息和响应消息提供对应关系。若消息类型为请求消息，请求发起方按单调递增方式确定消息序列号；若消息类型为响应消息，响应方填入原请求消息头部的消息序列号。

6.2 请求消息

图 4 给出了网络匹配服务器发现协议的请求消息格式。其中，各字段的含义如下。

- a) 请求代码：请求类型，当前取值如下：
 - 1) 0x01 固定网络；
 - 2) 0x10 移动网络；
 - 3) 0x11 代理请求。
- b) 请求消息长度：指证书序列号与应用类型、请求匹配类型以及请求匹配术字段的总长度，以字节为单位。可以由此确定证书序列号的起始位置与长度。
- c) 保留字段：留作扩展使用，默认置 0。
- d) 应用类型：请求端的业务类型。
- e) 请求匹配类型，当前取值如下：
 - 1) 0x01 IPv4 匹配服务器；
 - 2) 0x02 Ipv6 匹配服务器。

- f) 请求匹配数：为一个 2 字节长度的字段，指明期望匹配服务发现服务器返回的匹配服务器地址数量。
- g) 数字证书：可选字段，其格式推荐使用 YD/T 1614—2007 所规定的数字证书格式。
- h)

请求代码 1 byte	请求消息长度 2byte	保留字段 1 Byte
应用类型 1 byte	请求匹配类型 1 byte	请求匹配数 2byte
数字证书 Variable Length		

图 4 网络匹配服务器发现协议的请求消息格式

6.3 响应消息

响应代码 1 byte	响应消息长度 2byte	保留字段 1 byte
响应实体		

图 5 响应消息的总体格式

图 5 给出了响应消息的总体格式。其中，各字段的含义如下。

- a) 响应代码：给出响应类型，取值如下：
 - 1) 0x01 成功；
 - 2) 0x10 不存在符合要求的网络匹配服务器地址；
 - 3) 0x11 后台数据库服务器失败；
 - 4) 0x12 拒绝服务；
 - 5) 0x13 查询请求格式错误。
- b) 响应消息长度：指响应实体与保留字段的总长度，以字节为单位。可以由此确定响应实体的起始位置与长度。
- c) 保留字段：留作扩展使用，默认置 0。

响应消息实体格式如图 6 所示。

IPv4记录个数 2 byte	IPv6记录个数 2 byte
IPv4地址 4 byte	
端口号 2 byte	优先级 2 byte
...	
IPv6地址 128 byte	
端口号 2 byte	优先级 2 byte
...	

图 6 响应消息的响应实体

7 安全性考虑

网络匹配服务发现协议中的请求和响应消息以及通信流程没有特别提供安全性验证。网络匹配服务发现服务器可采取其它措施，以防范可能的网络攻击，如 DDOS。协议没有特别规定网络匹配服务发现客户以何种方式获取网络匹配服务发现服务器的地址。网络匹配服务发现客户对网络匹配服务发现服务器的权威性不作判断。网络匹配服务客户和网络匹配服务器之间由网络匹配服务协议来提供认证机制，以确保网络匹配服务客户免于恶意网络匹配服务提供者的危害。
