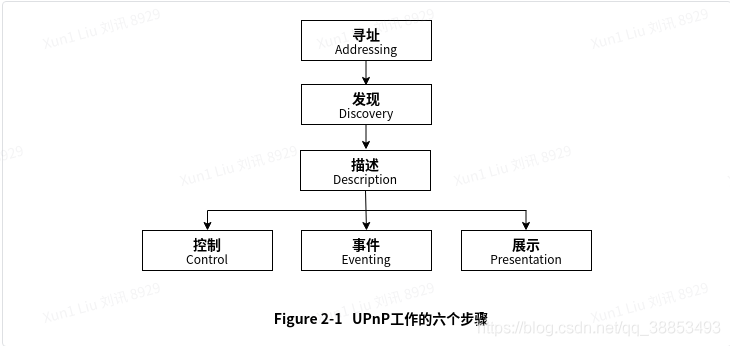
# 一、UPnP简介

****全称:****Universal Plug and Play（通用即插即用）

****应用:****主要用于设备的智能互联互通，简化家庭或企业中智能设备的联网过程。

# 二、UPnP工作原理

*UPnP工作主要分为以下六个步骤:*



## 2.1 寻址

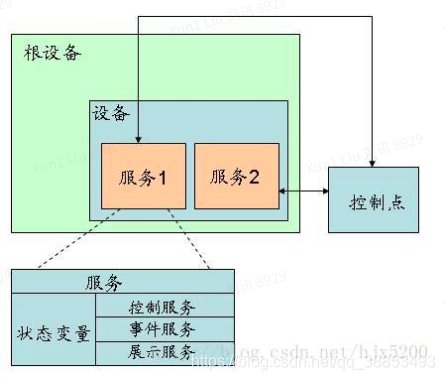
寻址就是获取一个可用的ip地址，有以下三种获取方式:

1. [DHCP](https://so.csdn.net/so/search?q=DHCP&spm=1001.2101.3001.7020" \t "https://blog.csdn.net/qq_38853493/article/details/_blank): 通过DHCP协议自动获取ip地址(首选)
2. Auto-IP: 通过Auto-IP协议，从169.254.1.0 ~169.254.254.255（也称169.254/16）获取一个局域网内唯一的IP地址
3. friendly name: 设备借助DHCP服务器到DNS服务器中注册设备主机名(/URL)和IP地址的映射关系

## 2.2 发现

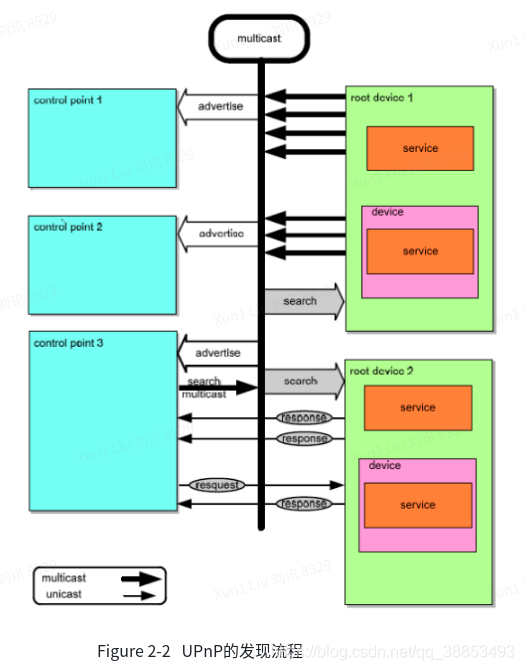
### 2.2.1 架构图

*设备是服务的载体，可以包含多种服务，也可嵌套多个设备。在这一步设备和控制点只完成了互相通信的一小部分，在这一步设备宣告了自己的存在和拥有的服务，以及其他的一些基本信息如设备的UUID，设备描述的URL地址等*



### 2.2.2 ****发现流程****

*****发现过程如下，粗箭头为多播，细箭头为单播*****



****控制点上线****

*当控制点(control points)上线后，就会进入发现阶段：向UPnP专用的多播地址发送SSDP发现报文，请求网络上的UPnP设备告知自己拥有的服务，设备收到该多播请求后，判断自己能满足该请求，则SSDP单播回复控制点；*

****设备上线****

*当设备上线后，就会进行通知操作：以多播方式发送SSDP通知报文，通知控制点自己所拥有的服务，且每隔一定的时间就要重新再通知一次，否则会被控制点cp判为离线*

这两种情况下的组播消息一般都是设备和服务的基本信息。如类型、唯一标识符、当前状态参数等。具体报文交互见2.3

### 2.2.3 报文交互

#### ****case1:控制节点上线，搜索网络上的设备和服务:****

*控制节点使用数据报套接字向239.255.255.250:1900发送一条多播请求，格式如下:*

M-SEARCH \* HTTP/1.1

HOST: 239.255.255.250:1900

MAN:"ssdp:discover"

MX:3

ST:UPnP:rootdevice

*设备收到多播请求，如果匹配请求，则将自身情况单播方式告知控制点。报文格式如下:*

HTTP/1.1 200 OK

CACHE-CONTROL: max-age=100

DATE: Sun, 15 Jan 2006 06:51:02 GMT

EXT:

LOCATION: http://192.168.14.1:1900/igd.xml

SERVER: TP-LINK Wireless Router WR541G/5, UPnP/1.0

ST: upnp:rootdevice

USN:uuid:upnp-InternetGatewayDevice-192168141678900001::upnp:rootdevice

#### ****case2:设备上线，通知控制节点自己的情况****

*设备采用多播方式通知网络上的控制节点自己的信息，且每隔一定时间(默认30min)需要通知一次，报文格式如下。*

NOTIFY \* HTTP/1.1

Host: 239.255.255.250:1900

NT: blenderassociation:blender

NTS: ssdp:alive

USN: someunique:idscheme3

AL: <blender:ixl><http://foo/bar>

Cache-Control: max-age = 7393(s)

#### ****case3:设备离线，通知网络控制点****

*一般设备离线会通知控制节点，不通知也没事，一定时间后不回复控制点，就会被判为离线并清除*

NOTIFY \* HTTP/1.1

Host: 239.255.255.250:1900

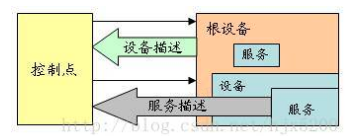
NT: someunique:idscheme3 （服务类型）

NTS: ssdp:byebye（通知消息的类型）

USN: someunique:idscheme3

## 2.3 描述

*CP获取了设备的基本信息UUID、URL之后还需要知道更多信息，如设备的状态，可执行的动作等。这时需要通过设备的URL访问设备，获取更多的服务描述信息。*

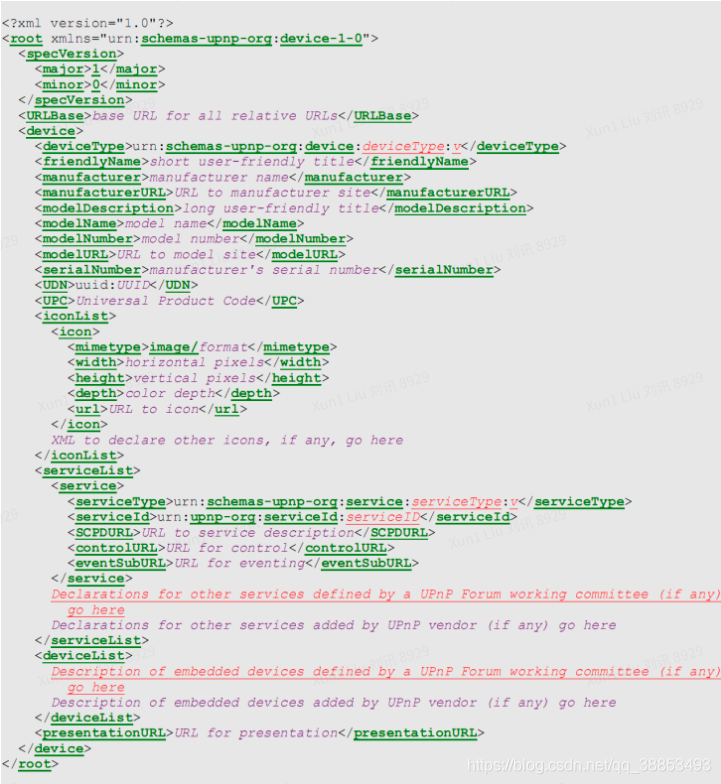


### ****2.3.1 设备描述****

*UPnP设备的描述以XML形式来表示，设备描述包括制造商信息、模块名称和编号、序列号等等。*

*对于一个物理设备可以包含多个逻辑设备，多个逻辑设备既可以是一个根设备其中嵌入多个设备，也可以是多个根设备的方式存在。描述模板如下:*

（图中红色字段为UPnP论坛定义；紫色字段为UPnP设备制造商定义；绿色字段为设备架构定义）



◆ ****<root>****

必需标签。<root>到</root>之间包含根设备属性信息，根设备服务信息，根设备的嵌入式设备信息。其中根设备的服务信息在<serviceList>标签内，根设备内部的嵌入式设备的信息在<deviceList>标签内。

◆****<UDN>****

必需标签。UPnP设备的唯一标识符，由一个小于64个字符的字符串组成。

◆ ****<deviceType>****

必需标签。UPnP设备类型，通常有UPnP论坛定义的标准设备和UPnP设备制造商定义的设备两种情况。UPnP 论坛定义的标准设备模型为“urn:schemas-upnp-org:device:deviceType:ver”，而UPnP设备制造商定义的设备模型为“urn:domain-name:device:deviceType:ver”。其中“deviceType”为设备类型，“ver”为最高支持版本，“domain-name”为UPnP设备制造商的域名，不超过64个字符。

◆ ****<friendlyName>****

必需标签。用户可见的设备名，由UPnP厂商指定一个小于64个字符的字符串。

◆****<service>****

当该设备提供服务时必需。<service>到</service>之间包含服务描述。有服务类型（<serviceType>）、服务ID（<serviceId>）、服务描述文件的URL（<SCPDURL>）、服务控制的URL（<controlURL>）和服务事件的URL（<eventSubURL>）。

◆ ****<serviceType>****

必需标签。服务类型，通常有UPnP 论坛定义的标准服务和UPnP设备制造商定义的服务两种情况。UPnP 论坛定义的标准服务模型为“urn:schemas-upnp-org:service:serviceType:ver”，而UPnP设备制造商定义的设备模型为“urn:domain-name:service:serviceType:ver”。其中serviceType”为服务类型，其余定义的意义与<deviceType>标签一致。

◆****<serviceId>****

必需标签。服务ID，在其设备描述中必须唯一。通常有UPnP 论坛定义的标准服务ID和UPnP设备制造商定义的服务ID两种情况。UPnP 论坛定义的标准服务ID模型为“urn:schemas-upnp-org:service:serviceID”，而UPnP设备制造商定义的设备模型ID为“urn:domain-name:service:serviceID”。其中serviceID”一般与该服务的<serviceType>中的“serviceType”一致，其余定义的意义与<deviceType>标签一致。

◆ ****<SCPDURL>****

必需标签。服务描述文件的URL，在其设备描述中必须唯一，获取该服务的描述文件时需要。

◆****<controlURL>****

必需标签。服务控制的URL，在其设备描述中必须唯一，向该服务发出控制请求时需要。

◆****<eventSubURL>****

必需标签。服务事件的URL，在其设备描述中必须唯一，对该服务进行事件订阅、续订、退订以及事件通知时需要。

### ****2.3.2 服务描述/SCPDURL****

*服务的描述包含服务运行时刻的状态，运行时间等等。服务描述也由设备制造商提供，采用XML描述，遵循UPnP框架协议。*

（图中红色字段为UPnP 论坛定义；紫色字段为UPnP设备制造商定义；绿色字段为设备架构定义）



◆ ****<actionList>****

当该服务提供动作时必需。服务的动作列表，包含该服务的所有动作描述信息，每个动作使用一个<action>标签描述。

◆ ****<action>****

必需标签。动作描述，<action>到</action>之间包含一个动作的描述。有动作名称（<name>），与该动作相关的参数表（<argumentList>）。

◆****<argument>****

必需标签。动作的参数描述，<argument>到<argument>之间包含一个该动作的相关参数描述信息。有参数名（<name>），是输入参数还是输出参数（<direction>），如果需要返回时还包含返回值的描述（<retval>），以及与该参数对应的状态变量名（relatedStateVariable）。

◆****<serviceStateTable>****

当该服务存在状态变量时必需。该服务的状态变量表，<serviceStateTable>到</serviceStateTable>之间包含所有的状态变量描述，每一个状态变量使用一个<stateVariable>标签描述。

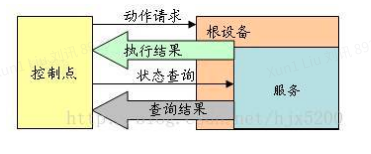
◆****<stateVariable>****

必需标签。状态变量，<stateVariable>到</stateVariable>之间包含一个状态变量的描述信息。有状态变量名（<name>）、该状态变量的数据类型（<dataType>），推荐包含该状态变量的默认值（<defaultValue>）、状态变量的可取值列表（<allowedValueList>）、数值型状态变量的取值范围（<allowedValueRange>）。

## 2.4 控制/controlURL

### 2.4.1 控制流程

*拿到设备和服务描述后，怎么控制设备呢？设备描述提供Control URL，控制点CP通过SOAP协议向Control URL发送操控请求，SOAP协议含有消息Body，指示如何控制设备。可能还要传参数，比如想播放一个视频，要把视频的URL传过去；设备收到后要respone，表示能不能执行调用，出错的话会返回一个错误代码。*



### 2.4.2 报文交互

*控制流程交互使用的是SOAP报文，具体格式如下:*



所有的SOAP消息都使用XML编码，一条SOAP消息就是一个普通的XML文档，文档包括下列元素：

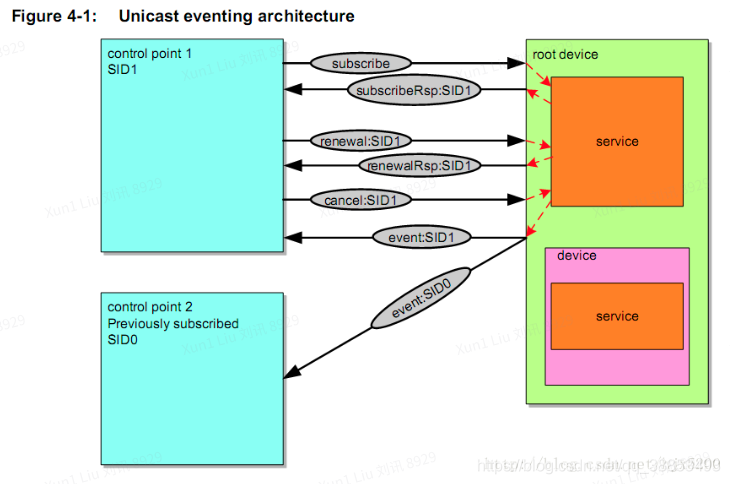
1. Envelope（信封）元素，必选，可把此XML文档标识为一条SOAP消息。
2. Header（报头）元素，可选，包含头部信息（包含了使消息在到达最终目的地之前，能够被路由到 一个或多个中间节点的信息，可能会定义认证信息、事务信息、本地信息）。
3. Body(主体)元素，必选，包含所有的调用和响应信息。
4. Fault 元素，位于Body内，可选，提供有关处理此消息所发生错误的信息。
5. Attachment（附件）元素，可选，可通过添加一个或多个附件扩展SOAP消息。

## 2.5 事件/eventSubURL

### 2.5.1 订阅发布流程

*当设备上的服务在运行，其状态变量发生改变之后，就产生了一个事件。控制点可以订阅这个事件，保证能及时捕获事件信息，做出响应的控制动作。*

下面是一个单播事件的结构图，控制点是subscriber(订阅者)，设备是publisher(发布者)。



订阅者向发布者发送订阅消息，更新订阅消息，退订消息。发布者向订阅者推送订阅

### 2.5.2 订阅发布报文交互

*事件的订阅和推送这块用的通信协议是GENA(General Event Notification Architecture) ，通过HTTP/TCP/IP传送。*

#### ****A.订阅请求****

****【订阅者】****

##### ****订阅请求****

*订阅者向发布者发送一个包含发布者URL、服务标识符和事件消息交付URL的订阅消息*

*请求订阅消息格式如下，采用SUBSCRIBE方法的请求，没有消息体，但该消息与最后一个http标头之间需要空一行。*

SUBSCRIBE publisher\_path HTTP/1.1

HOST: publisher\_host publisher\_port

CALLBACK: <delivery URL>

NT: upnp:event

TIMEOUT: second-requested subscription duration

消息解析：

(1)命令行

SUBSCRIBE 开始订阅或续订，方法由GENA定义

*publisher\_path 事件触发URL(设备描述中的服务元素eventSubURL子元素)路径组成*

HTTP/1.1 HTTP版本

(2)标头

HOST host:事件触发URL的域名或ip; port:端口，默认80

CALLBACK 事件消息发往的位置，UPnP厂商定义，如果有多个url则挨个尝试，直至成功

NT 同CALLBACK一样为GENA规定，通知类型必须采用upnp:event形式

SID 订阅不采用SID标头

TIMEOUT 订阅有效期，second+整数/infinite(无限)

****【发布者】****

##### ****接受订阅：****

*如果资源足够，发布者应当30s(包含预计传输时间)内接受订阅。发布者接受订阅后，返回唯一订阅标识符和订阅持续时长，并尽快发送第一个初始化消息。*

HTTP/1.1 200 OK

DATE：when response was generated

SERVER: OS/version UPnP/1.0 product/version

SID: uuid:subscription-UUID

TIMEOUT: second-actual subscription duration

(1)标头

DATE 响应生成时间，建议采用RFC1123日期；例 Tue, 30 Oct 2018 15:33:48 CST

SERVER 操作系统名称/版本 UPnP/1.0 产品名称/版本

SID GENA规定的标头，订阅标识符，必须以唯一UUID开头，由UPnP厂商规定单一url

TIMEOUT 定期，论坛推荐厂商规定。一般>=1800s; 格式second+整数/infinite

##### ****拒绝订阅****

*若发布者不能接受订阅，或者订阅请求存在错误，发布者应该在30s(包含传输时间)内反馈以下一个错误进行响应。*

表2-1 HTTP状态代码 表示一个错误取消订阅 表

|  |  |  |
| --- | --- | --- |
| 错误码 | 错误说明 | 详细描述 |
| 400 | 不兼容标头 | 如果SID标头和一个NT或CALLBACK一起出现，则会引起该错误 |
| 412 | CALLBACK缺少或无效 | CALLBACK缺失或者不包含有效的HTTP Url,则会引起该错误 |
| 无效NT | NT标题不符合upnp:event, 则会引起该错误 |
| 5XX | 不能接受订阅 | 发布者不接受订阅，返回HTTP500系列错误代码 |

注意：其他错误可能被UPnP下层协议栈返回

#### B****.发布消息****

【发布者】

##### ****发布消息****

*发布者保留订阅者列表，当一个或多个状态变量被事件触发时，发布者向订阅者传递以下信息：*

*1）唯一订阅标识符*

*2）事件*delivery*URL*

*3) 事件编号*

*4）订阅持续时间*

*如果订阅者未响应，会一直发布直到订阅期满。如果需要修复订阅，比如订阅者丢失一条或多条信息，则需要取消后重新订阅*

NOTIFY delivery\_path HTTP/1.1

HOST:delivery\_host delivery\_port

CONTENT-TYPE: text/xml

CONTENT-LENGTH: Bytes in body

NT: upnp:event

NTS:upnp:propchange

SID:uuid:subscription-UUID

SEQ:event key

<e:propertyset> xmlns:e="urn:schemas-upnp-org :event-1-0>

<e:property>

<variableName>new value</variableName>

<e:property>

Other variable names and values (if any) go here.

</e:propertyset>

(1)命令行

NOTIFY 通知消息，方法由GENA定义

交付路径 交付URL(订阅消息中的CALLBACK标头)路径组成，事件消息的目的地，单一、相对的url.

HTTP/1.1 HTTP版本

(2)标头

HOST 要求delivery*URL*(订阅消息中的CALLBACK标头)的域名或ip地址和端口，端口默认80

CONTENT-TYPE 固定为****text/xml****

CONTENT-LENGTH:消息体长度，以字节为单位，取整

NT 通知类型，固定****upnp:event****

NTS 通知子类型，固定****upnp:propchange****

SID 订阅标识符

SEQ 事件编号，整数类型：初始化消息编号为0，给特定订阅者每发送一条消息后+1，长度为8字节，溢出后回到1。

(3)消息体

****<propertyset>****

a.要求Xmlns名字空间属性必须为urn: ****schemas-upnp-org :event-1-0****，所有子元素必须符合这一名字空间

b.propertyset包含子元素特性，特性要求事件消息中的变量名称和值重复一次，值必须符合名字空间

c.子元素****variableName****是更改的状态变量名称(服务描述中stateVariable的子元素)

****为满足架构的可扩展性，处理上述xml时要遵循灵活的XML处理框架(FXPP),设备和控制点必须忽略:****

****(a)任何未知元素和其子元素或内容****

****(b)任何未知属性和值****

****【订阅者】****

##### ****确认订阅消息****

要确认收到这一事件消息，订阅者必须30s内做出响应。确认消息格式如下

HTTP/1.1 200 OK

****错误反馈****

*如果事件消息存在错误，则订阅者必须30s内返回下面一种错误进行响应*

表2.5.2-B 事件消息错误码说明

|  |  |  |
| --- | --- | --- |
| 错误码 | 错误说明 | 详细信息 |
| 400 | NT或NTS标头缺少 | 如果NT或NTS标头缺少，订阅者必须返回该HTTP错误码 |
| 412 | SID缺少 | 如果SID标头缺少或为空，订阅者必须返回该HTTP错误码 |
| 无效SID | 如果SID不是已知订阅，返回该错误码，且服务收到此错误码，则终止此SID |
| 无效NT头 | NT标头不符合upnp:event,则返回该错误码 |
| 无效NTS头 | NTS标头不符合upnp:propchange,则返回该错误码 |

注:其他错误可能会被upnp下层协议栈返回

#### C****.到期续订****

****【订阅者】****

##### ****到期续订****

*订阅者必须在订阅到期之前通过发送续订消息进行续订，除非你不想在订阅了。如果到期不续订，发布者则默认你已退订。*

SUBSCRIBE publisher\_path HTTP/1.1

HOST: publisher\_host publisher\_port

SID: uuid: subscription UUID

TIMEOUT: second-requested subscription duration

注:采用SUBSCRIBE方法的请求没有消息体，但该消息与最后一个HTTP标头之间必须空一行

（1）命令行

SUBSCRIBE 开始订阅或续订，方法由GENA定义

*publisher\_path 事件触发URL(设备描述中的服务元素eventSubURL子元素)路径组成*

HTTP/1.1 HTTP版本

(2)标头

HOST host:事件触发(eventSubURL) URL的域名或ip; port:端口，默认80

SID 订阅标识符

TIMEOUT 订阅有效期，second+整数/infinite(无限)

****【发布者】****

##### ****接受续订****

*要接受订阅，发布者要重新分配一个订阅持续时间，且必须以与响应新订阅请求相同格式发送一个响应，但不需要发送初始化事件。*

具体报文看【B.接受订阅】

##### ****拒绝续订****

*若发布者不能接受续订，或者续订请求错误，发布者发送下列一个错误进行响应，该响应要在30s(包括发送时间)内发出。*

表2-1 HTTP状态代码续订错误表

|  |  |  |
| --- | --- | --- |
| 错误码 | 错误说明 | 详细描述 |
| 400 | 不兼容标头 | 如果SID标头和一个NT或CALLBACK一起出现，则会引起该错误 |
| 412 | 无效SID | 如果SID标头缺少或为空，则会引起该错误 |
| 5XX | 不能接受订阅 | 发布者不接受续订，返回HTTP500系列错误代码 |

注意：其他错误可能被UPnP下层协议栈返回

#### D****.取消订阅****

****【订阅者】****

****取消订阅****

*当订阅者不再需要来自特定服务的消息，便取消订阅。*

UNSUBSCRIBE publisher\_path HTTP/1.1

HOST: publisher\_host publisher\_port

SID: uuid: subscription UUID

注:采用UNSUBSCRIBE方法的请求没有消息体，但该消息与最后一个HTTP标头之间必须空一行

（1）命令行

UNSUBSCRIBE 取消订阅，方法由GENA定义

*publisher\_path 事件触发URL(设备描述中的服务元素eventSubURL子元素)路径组成*

HTTP/1.1 HTTP版本

(2)标头

HOST host:事件触发(eventSubURL) URL的域名或ip; port:端口，默认80

SID 订阅标识符

****【发布者】****

****同意取消****

*要取消订阅，发布者必须30s内以下面格式发送一条响应*

HTTP/1.1 200 OK

****取消失败****

*如果取消请求出现错误，发布者必须30s内返回以下一种错误进行响应*

表2-1 HTTP状态代码 表示一个错误取消订阅 表

|  |  |  |
| --- | --- | --- |
| 错误码 | 错误说明 | 详细描述 |
| 400 | 不兼容标头 | 如果SID标头和一个NT或CALLBACK一起出现，则会引起该错误 |
| 412 | 无效SID | 如果SID标头缺少或为空，则会引起该错误 |

注意：其他错误可能被UPnP下层协议栈返回

## 2.6 展示

*控制点获取设备的URL后，通过设备URL可获取该设备表达的URL，和HTML界面，并加入到CP的浏览器中。控制点就是根据这个HTML界面，及会话机制实现对设备的控制，订阅收取事件等。*

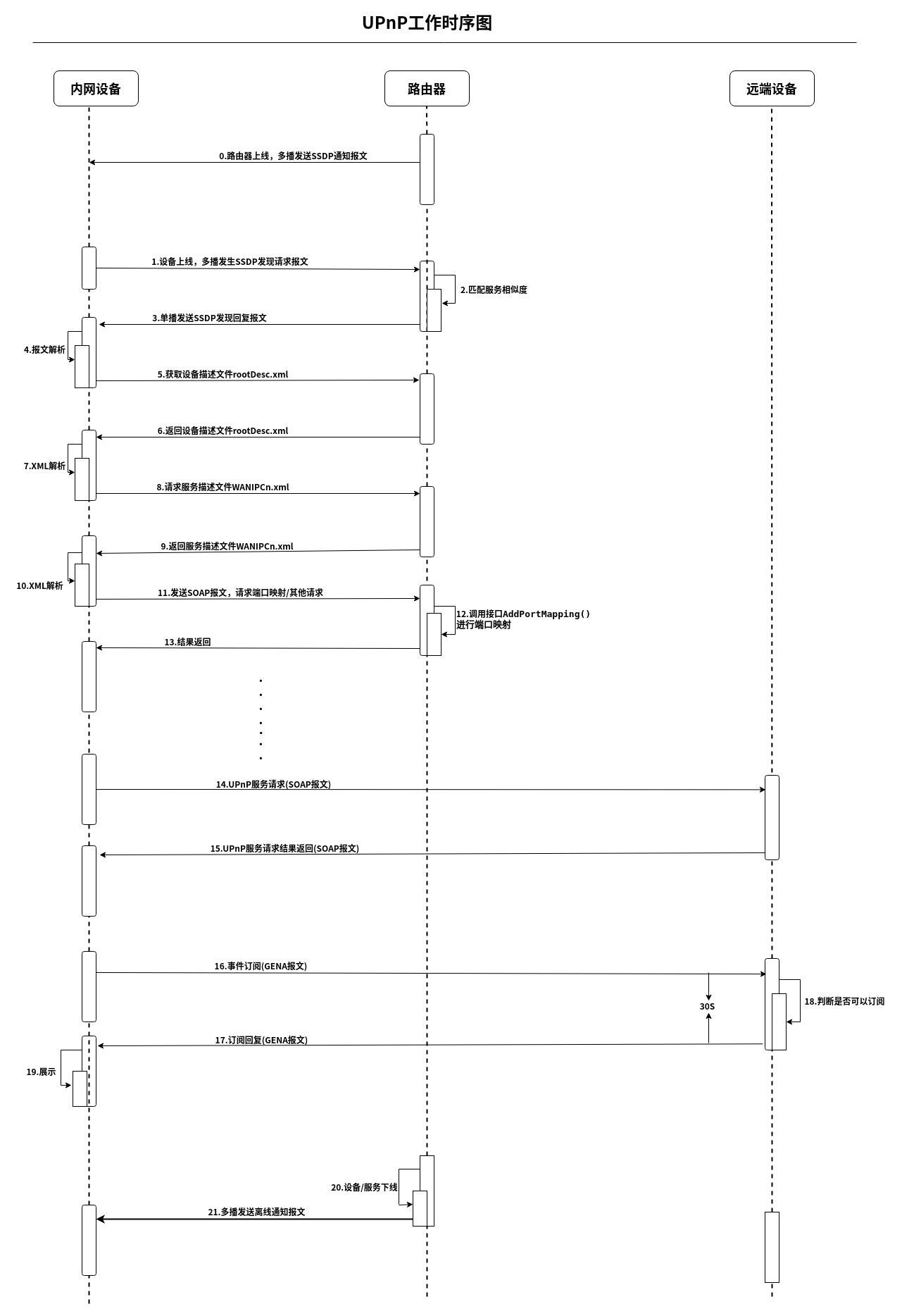
# 三、路由器所承担的角色

## 3.1 角色描述

*路由器其实是作为一个设备的角色存在，它提供自动端口映射等服务。对于一台内网电脑，UPnP可以使网关或路由器的NAT模块做自动端口映射，将监听的端口从网关或路由器映射到内网电脑上。 同时，网关或路由器的网络防火墙模块开始对Internet上其他电脑开放这个端口。*

## 3.2 UPnP工作时序

UPnP工作时序图如下



## 3.4 端口映射实例

*添加端口映射的接口是 "AddPortMapping"，参数如下*

<NewRemoteHost></NewRemoteHost>\n" "<NewExternalPort>ExternalPort</NewExternalPort>\n" "<NewProtocol>Protocol</NewProtocol>\n" "<NewInternalPort>InternalPort</NewInternalPort>n"

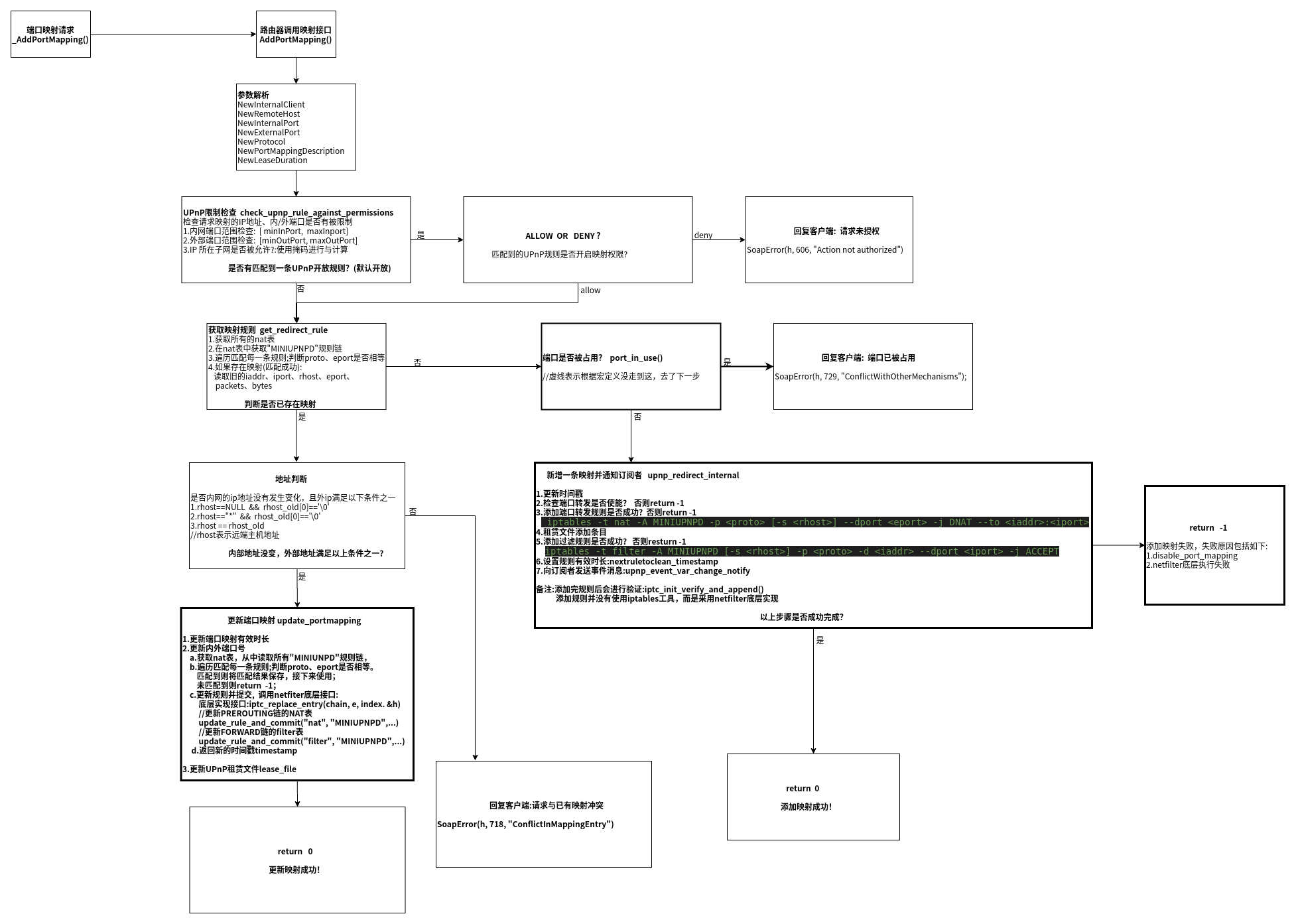
"<NewInternalClient>InternalClient</NewInternalClient>\n"

"<NewEnabled>1</NewEnabled>\n"

"<NewPortMappingDescription>PortMappingDescription" "</NewPortMappingDescription>\n"

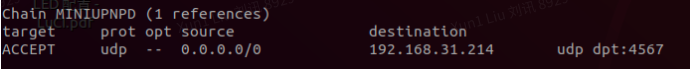
"<NewLeaseDuration>LeaseDuration</NewLeaseDuration>\n"

【路由器端口映射流程图解如下】



映射后在nat表和filter表中各添加了一条端口映射规则如下:

IMG_267



源码自行参看github upnp开源项目；

## 3.5 UPnP理解

*本身内网主机上公网的过程就采用到端口映射原理，但这个过程是路由器定义的，而UPnP采用自动端口映射原理，所要映射的端口是由内网主机/设备来定义的，根据服务和设备特性可以设置映射有效时长，这也极大增加了P2P的通信效率。*

*另外你也可以自己在路由器上手动设置映射，但没有自动映射方便省时省事，一旦把某端口映射到一台内网电脑后，那么这个端口就不能被其他电脑使用，你要手动释放。*

# 四、路由器开启UPnP的优缺点

## ****3.1 优点:****

1.使局域网内设备网速更流畅且稳定、加快P2P软件访问网络的速度

2.方便智能监控设备直接透传到因特网，无需做烦琐的映射端口设置

3.方便在因特网使用ERP、CRM、第三方远程桌面等软件

## ****3.2 缺点:****

1.假死: UPnP未对缓冲区进行检查和限制，使用中不断消耗网络资源，会导致网络设备假死，路由器能ping通但无法上网。

2.黑客攻击: "请求-响应"阶段会造成"拒绝服务"攻击， 业务端口会被利用。

3.发热: 高强度资源消耗会使路由器发热量会增加，对路由器寿命有不利影响。

【注】文章内容和图片部分来源于网页其他作者，在此感谢诸君付出，若有侵权，联系删除。