

---

## 上网行为管理 协议分析系列

——中国移动飞信协议分析

**相关主题:** 上网行为管理,PatrolFlow,信息安全网关,带宽管理,流量控制,P2P 控制,BT 下载,邮件监控,IM 控制,游戏监管,聊天监控,内容审计,多链路负载均衡,Web 推送,防火墙,防毒墙

正文内容:

```
POST /nav/getsystemconfig.aspx HTTP/1.1
User-Agent: IIC2.0/PC 2.2.0230
Content-Type: application/x-www-form-urlencoded; charset=utf-8
Host: nav.fetion.com.cn
Content-Length: 75
Connection: Keep-Alive

HTTP/1.1 100 Continue

<config><client type="PC" version="2.2.0230" platform="w5.1" /></config>

HTTP/1.1 200 OK
DATE: Wed, 11 Apr 2007 08:19:39 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Content-Language: zh-cn
Set-Cookie: ASP.NET_SessionId=3siqq555hhsjllshshsssw32; path=/; HttpOnly
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 202

<?xml version="1.0" encoding="utf-8" ?><config><client version="2.0.0.0"><compatible>
2.0.0.0</compatible><date>2006-7-27 18:48:27</date><pc-live-update
value="http://221.130.45.198/" /></client></config>
```

//此处返回升级服务器地址

查看是否有升级

GET /UpdateInfo.ashx?Version=2.2.0230&Switch= HTTP/1.1

User-Agent: IIC2.0/PC 2.2.0230

Host: 221.130.45.198

Connection: Keep-Alive

HTTP/1.1 204 No Content

Connection: close

Date: Wed, 11 Apr 2007 08:19:39 GMT

Server: Microsoft-IIS/6.0

X-Powered-By: ASP.NET

X-AspNet-Version: 2.0.50727

Cache-Control: private

Content-Length: 0

//开始取配置文件

POST /nav/getsystemconfig.aspx HTTP/1.1

User-Agent: IIC2.0/PC 2.2.0230

Host: nav.fetion.com.cn

Content-Length: 262

Connection: Close

HTTP/1.1 100 Continue

```
<config><user mobile-no="13412344321" /><client type="PC" version="2.2.0230"
platform="W5.1"/><servers version="0"/><service-no version="0"/><parameters
version="0" /><hints version="0" /><http-applications version="0" /><client-config
version="0" /></config>
```

HTTP/1.1 200 OK

Connection: close

Date: Wed, 11 Apr 2007 09:41:41 GMT

Server: Microsoft-IIS/6.0

X-Powered-By: ASP.NET

X-AspNet-Version: 2.0.50727

Content-Language: zh-cn

Set-Cookie: ASP.NET\_SessionId=1kl1h550rvost2ujpr0prfy; path=/; HttpOnly

Cache-Control: private

Content-Type: text/html; charset=utf-8

Content-Length: 5644

```
<?xml version="1.0" encoding="utf-8" ?><config><servers
version="12"><apply-sub-service>HTTP://221.130.45.201/nav/ApplySubscribe.aspx</apply
-sub-service><crbt-portal>http://221.130.46.134/crbt/default.aspx</crbt-portal><get-gene
ral-info>HTTP://221.130.45.201/nav/GeneralGetInfo.aspx</get-general-info><get-pic-code
>HTTP://221.130.45.201/nav/GetPicCode.aspx</get-pic-code><get-svc-order-status>HTTP
://221.130.45.201/nav/GetSvcOrderStatus.aspx</get-svc-order-status><get-system-status>
HTTP://221.130.45.201/nav/GetSystemStatus.aspx</get-system-status><get-uri>HTTP://2
21.130.45.205/hds/geturi.aspx</get-uri><http-tunnel>HTTP://221.130.45.203/ht/sd.aspx<
/http-tunnel><j2me-adapter></j2me-adapter><matching-portal></matching-portal><port
al>http://www.fetion.com.cn/</portal><sipc-proxy>221.130.45.203:8080</sipc-proxy><ssi
-app-sign-in>https://221.130.45.201/ssiportal/SSIAppSignIn.aspx</ssi-app-sign-in><ssi-ap
p-sign-out>http://221.130.45.201/ssiportal/SSIAppSignOut.aspx</ssi-app-sign-out><sub-se
rvice>https://221.130.45.201/nav/Subscribe.aspx</sub-service></servers><service-no
version="1"><help-desk>10086</help-desk><ivr>125862</ivr><mms></mms><rbt>125
30</rbt><sms>161</sms></service-no><parameters
version="4"><batch-sms-max-receivers>8</batch-sms-max-receivers><forbidden-share-co
ntent-type>exe;bat;cmd;msi</forbidden-share-content-type><ivr-invite-timeout>60</ivr-in
vite-timeout><max-ivr-participants>8</max-ivr-participants><max-msg-convert-sms>3</
max-msg-convert-sms><max-msg-length>400</max-msg-length><max-share-content-size
>10485760</max-share-content-size><max-sms-length>182</max-sms-length><max-sms
-unicode>70</max-sms-unicode><offline-max-share-content-size>2048000</offline-max-s
hare-content-size><portrait-file-type>image/pjpeg;image/jpeg;image/bmp;image/x-window
s-bmp;image/png;image/gif</portrait-file-type><single-sms-max-length>70</single-sms-m
```

ax-length><temp-group-max-share-content-size>2048000</temp-group-max-share-content-size><max-blacklist>128</max-blacklist><max-buddies>300</max-buddies><max-buddy-list>64</max-buddy-list><max-chat-buddies>20</max-chat-buddies></parameters><hints version="4"><i-not-log-on>您没有登录，不能发送消息</i-not-log-on><i-not-online>您当前的状态设置为“{0}”</i-not-online><participants-not-online>一些参与者可能无法及时回复您的消息</participants-not-online><user-busy>{0}可能无法及时回复您的消息，因为{1}的状态为{2}。</user-busy><user-in-blacklist>对方在您的黑名单中，您不能和他会话</user-in-blacklist><user-offline>{0}已离线，不能立即收到您的消息。您发送的消息将被保存下来并延迟发送。</user-offline><user-sms-status>{0}没有登录，您的消息将会以短信发送到对方的手机。每条消息最多{1}个字符，根据您输入的内容长度，消息可能会被拆为2~{2}条短信。</user-sms-status></hints><http-applications version="5"><crbt-common-access>HTTP://221.130.45.205/hds/CrbtCommonAccess.aspx</crbt-common-access><del-portrait>HTTP://221.130.45.205/hds/DeletePortrait.aspx</del-portrait><delete-msg-history>HTTP://221.130.45.205/hds/DeleteMessageHistory.aspx</delete-msg-history><get-ad>HTTP://221.130.45.205/hds/GetAd.aspx</get-ad><get-personal-ext-info>HTTP://221.130.45.205/hds/getpresenceinfo.aspx</get-personal-ext-info><get-personal-info>HTTP://221.130.45.205/hds/getpersonalinfo.aspx</get-personal-info><get-portrait>HTTP://221.130.45.205/hds/getportrait.aspx</get-portrait><get-tab-info>HTTP://221.130.45.205/hds/GetTabInfo.aspx</get-tab-info><query-msg-history>HTTP://221.130.45.205/hds/QueryMessageHistory.aspx</query-msg-history><record-share-content-op>HTTP://221.130.45.205/hds/recordsharecontentevent.aspx</record-share-content-op><relay-upload-share-content>HTTP://221.130.45.206/hds/RamRelayUploadShareContent.aspx</relay-upload-share-content><set-personal-info>HTTP://221.130.45.205/hds/setpersonalinfo.aspx</set-personal-info><set-portrait>HTTP://221.130.45.205/hds/setportrait.aspx</set-portrait><set-tone-info>HTTP://221.130.45.205/hds/SetToneInfo.aspx</set-tone-info><upload-share-content>HTTP://221.130.45.205/hds/BlockUploadShareContent.aspx</upload-share-content></http-applications><client-config version="5"><item key="sms-mode-main-desc" value="您可以发送短信与好友进行交流、使用语音聊天，还可以邀请您 的手机好友加入 Fetion 服务" /><item key="sms-mode-invite-buddy" value="hy" /><item key="sms-mode-invite-ivr" value="yy" /><item key="sms-mode-no-contact-list" value="目前您还没有好友，可以通过登录后邀请，获取好友或将手机通讯簿的联系人导入为 Fetion 好友" /><item key="online-no-buddies" value="目前您还没有好友，可以通过菜单中的导入手机联系人、移动速配交友、用飞信号和手机号添加好友的方式来添加好友。" /><item key="online-garden-desc" value="" /><item key="mobile-no-dist" value=""></c

```
v="cmcc"><d s="13500000000" e="13999999999"/><d s="13400000000"
e="13489999999"/><d s="15900000000" e="15999999999"/><d s="15800000000"
e="15899999999"/></c></r>" /><item key="fee-charge-desc-url"
value="http://www.fetion.com.cn/shuoming1.aspx"/><item key="ivr-charge-desc" value="
资费咨询当地 10086"/><item key="info-redirect-url"
value="https://uid.fetion.com.cn/SSIPortal/Redirect.aspx?key="/></client-config><client
version="2.0.0.0"><compatible>2.0.0.0</compatible><date>2006-7-27
18:48:27</date><pc-live-update value="http://221.130.45.198/"></client> </config>
```

抓包看了一下，飞信是用了混合协议的：

- 1、基于 HTTP(XML Web Services 吧?) 进行获取系统配置、更新程序、注册用户
- 2、基于 HTTPS 进行登录时密码验证
- 3、应用层协议是 SIP 协议，但不是标准的，估计是自创的？所有交互过程如发消息、短信通过 SIP 协议进行。

关于 SIP，有巨多的 RFC 描述，飞信的 SIP 协议栈实现的是 TCP、HTTP 承载

1.TCP 承载方式：连接服务器(目前是 221.130.45.203)的 8080 端口，这时在客户端的“网络设置”中显示的是“TCP 直接连接”，SIP 信令直接就放在 TCP 的包中。

2.HTTP 承载方式：连接服务器(目前是 221.130.45.203)的 80 端口，采用 POST 方式，将信令包在 POST 请示中，这时在客户端的“网络设置”中显示的是“HTTP 直接连接”

因为是 TCP 和 HTTP 承载，所以其包格式是非常清楚的，那么注意力就可以直接放到 SIP 协议或 SIP 信令上，详细的内容稍后再写。

总的来说，飞信协议是比较简单的，不对，准确地说法是比较规范和清晰，但协议本身是复杂的，另外：

1. 飞信的协议是明文，这一点如同其兄弟 MSN，是不如 QQ 和 RTX 的，因此，通过飞信的交谈过程是可轻易截获的，通过很简单的工具，就可以截到同一网段上所有人的交谈，估计会有人写 Fetion Chat Sniffer 的，就跟 MSN 一样。
2. 协议效率比较低。
3. 状态有问题，presence 处理得不太好。

以下分析均基于飞信的这一版本：Fetion 2006 beta 版本 2.1.0.0。

作协议分析时，一抓包，就发现飞信工作时连的是 221.130.45.203 这个服务器。那这个 IP 地址从哪来的呢？会变吗？飞信的客户端程序中并没有配置服务器地址这一说。固定一个 IP？不会吧，一面向全国的系统，不可能用一个 IP 地址。用一个固定域名解析出来的多 IP 地址中的一个吗？抓出它访问 DNS 的包一看，它就只在开始时解析过一次域名：nav.fetion.com.cn，这个域名的 IP 是 221.130.45.201——听说开发飞信的人就是微软开发 MSN 的人，所以啥都跟 MSN

一样，你看那飞信的主界面元素，你能找一个位置和功能跟 MSN 不一样的吗？连解析域名这点都跟 MSN 一样，没意思啊，印象中 MSN 也是一开始就解析一个地址，好像是 Messenger.msn.com? 如果想在局域网内封锁 MSN，就把这个域名给指向 127.0.0.1，MSN 就傻了。

既然只解析过 nav.fetion.com.cn，那么 221.130.45.203 这个工作服务器（SIP 的 Proxy Server）地址，就应该是 nav.fetion.com.cn 返回来的了。确实是，但只是第一次登录时返回，并保存在了本地。后面再登录时，如果版本不更新，是不会再返回这些系统配置信息的。所以，除第一次外，再抓包是看不到这些配置信息的。

本地配置文件并没放在 Fetion 的程序目录中，而是放到了 %USERPROFILE%\ApplicationFetion 目录下。这个目录下有 configuration.dat 和飞信的用户目录，每个飞信用户目录下还有 configuration.dat、contacts.dat、userinfo.dat 这三个配置文件，看名字就知道是与用户相关的系统配置文件、好友列表文件、用户的个人信息文件。

这些文件全是 XML 格式的，所以可以用 Notepad 打开，不过，你打开后就会发现，这些文件的内容全被加密了，变态啊，这些文件有什么好加密的呢。

我们如何获得这里头的信息呢？

方法有两个：

一、我们让 Fetion 不要加密这些文件的内容，方法是：修改 FetionFx.EXE 文件。用 ildasm，将 FetionFX.EXE 反汇编出来，将其中的 Imps.Client.Pc.PersistentManager.EncodeMode1 和 Imps.Client.Pc.PersistentManager.DecodeMode1 这两个函数改掉，将这两个函数体改成以下内容：

```
.maxstack 1
IL_0000: ldarg.0
IL_0001: ret
```

即，立即将参数返回。然后再用 ilasm 工具重新汇编生成 FetionFX.EXE 文件，覆盖掉以前那个，然后，再运行飞信，所有配置文件就不会再加密了。

二、构造一个请求，给 nav.fetion.com.cn，让它返回。请求的内容很简单，抓一下包就会知道，取系统配置请求过程是：

```
xxx.xxx.xxx.xxx:xxxx >>>>>>> 221.130.45.201:80
POST /nav/getsystemconfig.aspx HTTP/1.1
User-Agent: IIC2.0/PC 2.1.0.0
Host: nav.fetion.com.cn
Content-Length: 233
Connection: Keep-Alive
```

-----

```
xxx.xxx.xxx.xxx:xxxx <<<<<<< 221.130.45.201:80
```

```
HTTP/1.1 100 Continue
```

```
-----
```

```
xxx.xxx.xxx.xxx:xxxx >>>>>>> 221.130.45.201:80
```

```
<config><user mobile-no="139xxxxxxx" /><client type="PC" version="2.1.0.0"  
platform="W5.1" /><servers version="12" /><service-no version="1" /><parameters  
version="4" /><hints version="4" /><http-applications version="5" /></config>
```

将以上内容中的从 `servers version` 开始的 `version` 全置为"0", 服务器就会返回配置信息。注意, 配置信息全是 UTF-8 编码的。用 `nc` 就可构造一个 `http` 请求发过去, 服务器立马就返回了。

推荐用方法一, 因为这样可以看和修改所有配置信息, 而方法二仅有系统配置信息。

与我们关注的服务器地址相关的信息在飞信用户目录下的 `configuration.dat` 中, 一看就明白是啥:

```
....
```

```
<sipc-proxy>221.130.45.203:8080</sipc-proxy> 这就是我们关心的 TCP 直接连接时的服务器地址
```

```
<http-tunnel>HTTP://221.130.45.203/ht/sd.aspx</http-tunnel> HTTP 直接连接时的入口地址
```

```
<get-pic-code>HTTP://221.130.45.201/nav/GetPicCode.aspx</get-pic-code> 注册时, 取验证代码图片的 URL
```

```
<get-system-status>HTTP://221.130.45.201/nav/GetSystemStatus.aspx</get-system-status  
> 取系统状态
```

```
....
```

这个配置信息放到飞信用户目录下是有原因的, 就象 SIP 协议支持的, 登录的服务器是可以分用户群的, 不同的用户可以登录不同的 Proxy Server, 每个飞信用户(手机)可以分别登录到本省的 Proxy Server, 就如同现在的手机和电话网络一样。

其实这些配置内容没什么啊, 为什么要加密呢? 而且随便构造一个 `http` 请求, 就可以获得这些内容的。最变态的是通过飞信的交谈内容不加密不变换, 却把无关紧要配置文件加密了。

另外, 用户的密码就保存在 `Application Data\Fetion` 目录下的 `Configuration.dat` 中, 当然这个密码进行了变换, 遗憾的是, 在程序中是还原出了用户密码的, 因此, 用户密码别人是可以轻易获得的。幸好丢了可以手机找回。但这仍然是个非常不安全的因素。

J2me 版飞信的通信协议, 与 PC 版的协议是完全不同的。

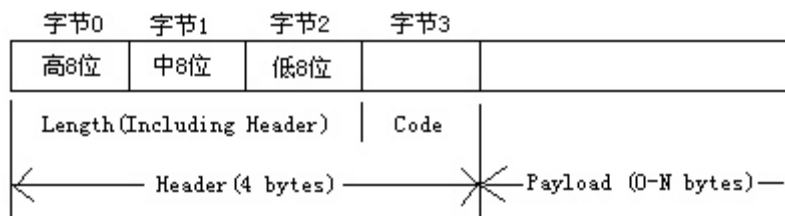
两个版本的协议, 都是以 HTTP 为基础。不同的是, PC 版的飞信, 在 HTTP 上采用了 SIP 协

议。

而 J2me 版的飞信，在 HTTP 上传输的，则是一个自定义的数据格式。

J2me 版飞信（以下简称飞信）的通信协议，基于 HTTP 协议

### 飞信数据包（请求与响应包结构相同）



1. Header长度固定为4；
2. Code(-1)表示特殊的包，该包Payload部分包含多个包，每个包结构与上面描述相同；
3. Payload的长度可以为0，表示该包只有命令码，没有数据；

可以看到，每个包都分为 Header 和 Payload 两部分。

header 是固定长度 4 个字节，其中，前三个字节(Length)表示整个数据包的程度，包括 Header 本身的长度，第 4 个字节(Code) 表示请求的命令码。表示长度的三个字节是按大端(big-endian)的格式（也就是网络字节序）来表示一个整数的。具体说就是，字节 0 表示长度的最高 8 位，字节 1 表示长度的中间 8 位，字节 2 表示长度的低 8 位。字节 3 表示请求码。

这个长度可以表示的很大，当然，暂时还用不上这么大。

Header 后的有效数据(Payload)是变长的。该部分长度可以为 0。一些简单的命令比如退出登录，只需要设置 Code 为对应的代码，Payload 部分是不需要数据的。

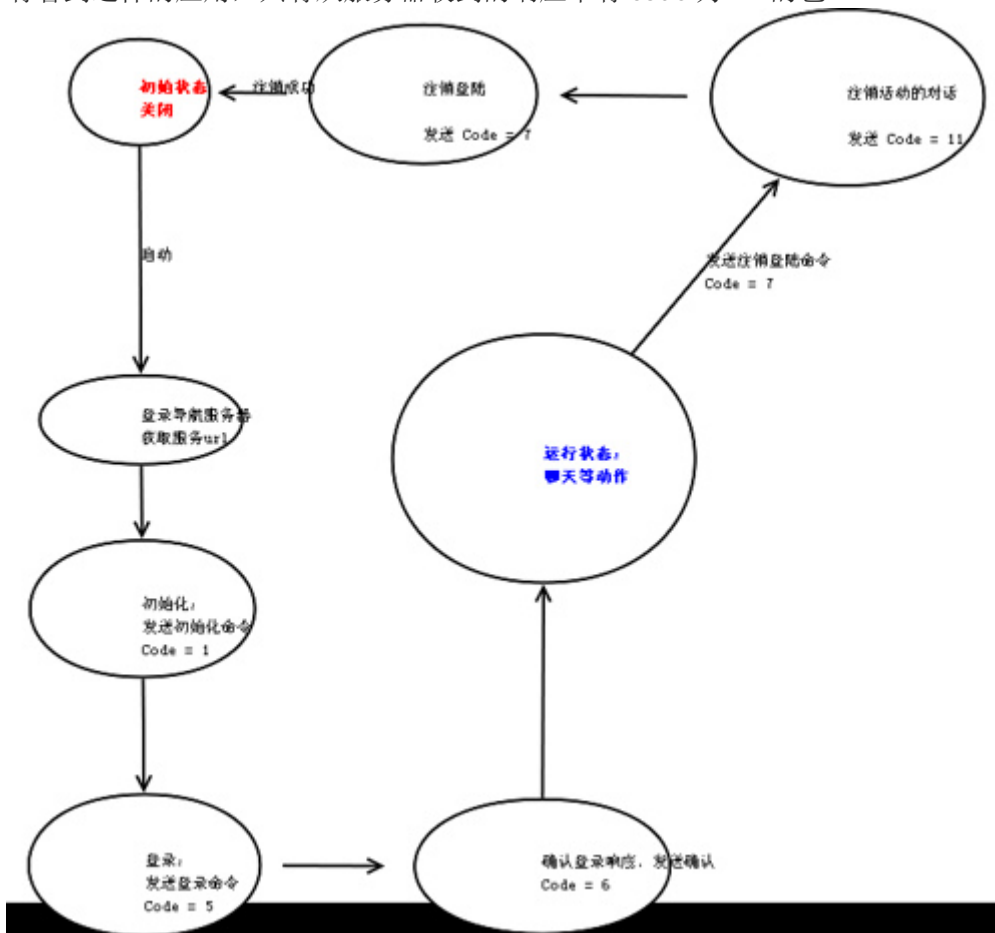
服务器返回的数据格式和客户端发出的具有相同的格式。

=== 特殊的包 ===

在服务器响应中，有一个特殊的包，Code 为 -1。Code 为-1 的包，实际上是有多个包组成的。需要把这些包全部分离出来，逐个处理它们。

\*\* 我不清楚是不是可以用 Code 为-1 的包同时发送多个包到服务器，不过在飞信的代码里，没

有看到这样的应用，只有从服务器收到的响应中有 code 为 -1 的包



=== 登录导航服务器 ===

在飞信客户端与服务器通信的过程中，登录导航服务器是第一步。目的是获得真正的服务 URL。可能是因为移动在以后会改动服务的 URL，或者按照就近服务的原则，动态的返回离使用飞信的手机最近的服务器上的服务 URL。

得到的这个服务 URL，就是后来的 登录，聊天，注销的目的地址。

从飞信的代码中可以看到缺省的导航服务器 url 是

<http://nav.m161.com.cn/getadapteruri.aspx>

该导航服务器 url，在 MANIFEST.MF 中 serverIP 也有定义，如果 MANIFEST.MF 没有定义 serverIP，就使用该默认的 url。

要获取服务 URL，需要往导航服务器 URL POST 一个字节，这个字节可以是任意数据。

如请求成功后，会返回一个 xml 文档，如下

```
<?xml version="1.0" encoding="utf-8" ?>
```

```
<Root xmlns="http://tempuri.org/DateExchange.xsd">
```

```
<Response>
```

```
<Error>0</Error>
```

```
<Memo/>
```

```
</Response>
```

```
<Uri>
```

```
http://liveja.amigo.bjmcc.net/transfer.vurl
```

```
</Uri>
```

```
</Root>
```

从 Uri 节点得到的就是飞信协议使用的服务 URL。这以后的通信，就与导航服务器无关了。

更多信息请登录 <http://www.byzoro.com>