Miranda

尽管在应用程序、操作系统和嵌入式设备中广泛使用了通用即插即用协议，但是很少有工具允许简单的发现和与启用upnp的设备进行交互。此外，在现有的工具中，大多数或所有都是闭源的Windows二进制文件。miranda是一个基于python的通用即插即用客户端应用程序，旨在发现、查询和与通用即插即用设备交互，特别是互联网网关设备(又名路由器)。

——*Craig Heffner*

1,帮助手册

交互模式下

oad
从文件中恢复以前的主机数据
头
显示/定义SSDP标题
帮助
显示程序帮助
宿主
查看和发送主机列表和主机信息
msearch
主动定位UPNP主机
pcap
被动地倾听UPNP主持人
放弃
退出这个外壳
原木
将用户提供的命令记录到日志文件中
对外星智能的探索
显示/定义应用程序设置
出口
退出这个外壳
将当前主机数据保存到文件

oad Restore previous host data from file
head Show/define SSDP headers
help Show program help
host View and send host list and host information
msearch Actively locate UPNP hosts
pcap Passively listen for UPNP hosts
quit Exit this shell
log Logs user-supplied commands to a log file
seti Show/define application settings

exit　　Exit this shell
save　　Save current host data to file

非交互模式下

用法:Miredo[选项][服务器名称]

创建一个Teredo隧道接口，用于通过UDP封装IPv6。

-c，- config指定一个配置文件
-f，-前台运行在前台
-h，-帮助显示此帮助并退出
-p，PID文件覆盖PID文件的位置
-u，-用户覆盖要将UID设置为的用户
-V，-版本显示程序版本并退出

Usage: miredo [OPTIONS] [SERVER_NAME]
Creates a Teredo tunneling interface for encapsulation of IPv6 over UDP.

-c, --config　specify an configuration file
-f, --foreground run in the foreground
-h, --help　display this help and exit
-p, --pidfile　override the location of the PID file
-u, --user　override the user to set UID to
-V, --version　display program version and exit

2.命令实例

交互式模式

> 在加任何参数的情况下，直接输入”miranda“即可进入交互式模式

help

显示“交互模式下的帮助手册”

> 加载从文件恢复以前的主机数据
> 标题显示/定义SSDP标题
> 帮助显示程序帮助
> 主机查看和发送主机列表和主机信息
> 主动定位UPNP主机
> 被动监听UPNP主机
> 退出退出此外壳
> 将用户提供的命令记录到日志文件中
> 显示/定义应用程序设置
> 退出退出这个外壳
> 将当前主机数据保存到文件

```
upnp> help

load            Restore previous host data from file
head            Show/define SSDP headers
help            Show program help
host            View and send host list and host information
msearch         Actively locate UPNP hosts
pcap            Passively listen for UPNP hosts
quit            Exit this shell
log             Logs user-supplied commands to a log file
seti            Show/define application settings
exit            Exit this shell
save            Save current host data to file
```

msearch

启用发现模式，用于发现UPNP（通用即插即用设备）主机[^可使用“Ctrl + c”进行退出扫描]

> UPNP，全称（Universal Plug and Play）中文一名为“通用即插即用”。由“通用即插即用论坛”推出的一套网络协议，该协议的主要目标是网络设备能够无缝连接。
>
> 而这项技术目前于之相似的有WIFI连接，从实验图中可以看出WIFI设备也属于即插即用技术的范围之内。
>
> 而WIFI设备刚好可以实现“无缝链接”
>
> > UPnP的概念由即插即用（Plug-and-play）一派而来，而即插即用则一种热插拔技术。
> >
> > > 而热插拔就是即插即用，比如我们熟知的机械键盘中，部分“高端”键盘也引用了这一项技术，使得机械键盘的轴体只需要插入键盘板中即可使用

```
upnp> msearch

Entering discovery mode for 'upnp:rootdevice', Ctl+C to stop...

****************************************************************
SSDP reply message from 192.168.0.1:1900
XML file is located at http://192.168.0.1:1900/igd.xml
Device is running vxWorks/5.5 UPnP/1.0 TL-WR886N/6.0
****************************************************************

^CDiscover mode halted...
```

mserach device TP-LINK

仅搜索“TP_LINK”设备

> 可通过 “msearch”查看
>
> ```
> ****************************************************************
> SSDP notification message from 192.168.0.1:1900
> XML file is located at http://192.168.0.1:1900/igd.xml
> Device is running vxWorks/5.5 UPnP/1.0 TL-WR886N/6.0
> ****************************************************************
> ```

```
upnp> msearch device TP-LINK

Entering discovery mode for 'urn:schemas-upnp-org:device:TP-LINK:1', Ctl+C to stop...

****************************************************************
SSDP notification message from 192.168.0.1:1900
XML file is located at http://192.168.0.1:1900/igd.xml
Device is running vxWorks/5.5 UPnP/1.0 TL-WR886N/6.0
****************************************************************
```

msearch service WANIPConnection

仅搜索支持WANIPConnection的UPUN设备

host

host list

获取当前内网络设备中所以UPNP设备及索引号[^索引号为0]

```
upnp> host list

        [0] 192.168.0.1:1900
```

host get 0

将索引号为0的UNUP设备进行枚举

host info 0

查看索引号为0的UNUP设备详细信息。

```
upnp> host get 0

Data for this host has already been enumerated!

upnp> host info 0

xmlFile : http://192.168.0.1:1900/igd.xml
name : 192.168.0.1:1900
proto : http://
serverType : None
upnpServer : vxWorks/5.5 UPnP/1.0 TL-WR886N/6.0
dataComplete : True
deviceList : {}
```

host details 0

显示索引号为0的UNUP设备详细信息

```
upnp> host details 0

Host name:        192.168.0.1:1900
UPNP XML File:    http://192.168.0.1:1900/igd.xml


Device information:
        Device Name: InternetGatewayDevice
                Service Name: Layer3Forwarding
                        controlURL: /l3f
                        eventSubURL: /l3f
                        serviceId: urn:upnp-org:serviceId:L3Forwarding1
                        SCPDURL: /l3f.xml
                        fullName: urn:schemas-upnp-org:service:Layer3Forwarding:1
                        ServiceActions:
                                SetDefaultConnectionService
                                        NewDefaultConnectionService
                                                DefaultConnectionService:
                                                        dataType: string
                                                        sendEvents: N/A
                                                        allowedValueList: []
                                                direction: in
                                GetDefaultConnectionService
                                        NewDefaultConnectionService
                                                DefaultConnectionService:
                                                        dataType: string
                                                        sendEvents: N/A
                                                        allowedValueList: []
                                                direction: out
        Device Name: WANDevice
                Service Name: WANCommonInterfaceConfig
                        controlURL: /ifc
                        eventSubURL: /ifc
                        serviceId: urn:upnp-org:serviceId:WANCommonInterfaceConfig
                        SCPDURL: /ifc.xml
                        fullName: urn:schemas-upnp-org:service:WANCommonInterfaceConfig:1
                        ServiceActions:
                                GetTotalPacketsSent
                                        NewTotalPacketsSent
                                                TotalPacketsSent:
                                                        dataType: ui4
                                                        sendEvents: N/A
                                                        allowedValueList: []
                                                direction: out
                                GetTotalPacketsReceived
                                        NewTotalPacketsReceived
                                                TotalPacketsReceived:
                                                        dataType: ui4
```

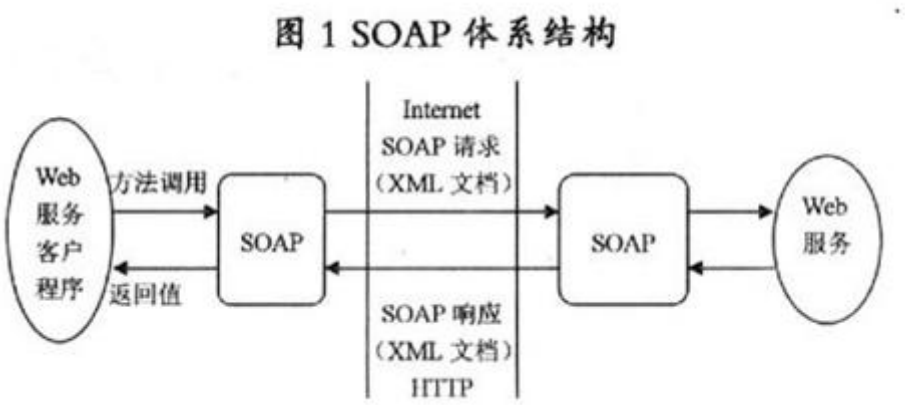
host summary 0

显示索号为0的简短摘要信息

```
upnp> host summary 0

Host: 192.168.0.1:1900
XML File: http://192.168.0.1:1900/igd.xml
InternetGatewayDevice
        manufacturerURL: http://www.tp-link.com.cn
        modelName: TL-WR886N
        UPC: 123456789001
        modelNumber: 6.0
        presentationURL: http://192.168.0.1:80
        friendlyName: Wireless N Router TL-WR886N
        fullName: urn:schemas-upnp-org:device:InternetGatewayDevice:1
        modelDescription: TL-WR886N 6.0
        UDN: uuid:8c15e41f-3d83-41c1-b35d-7557B1448207
        manufacturer: TP-LINK
WANDevice
        manufacturerURL: http://www.tp-link.com.cn
        modelName: WAN Device
        UPC: 123456789001
        modelNumber: 1.0
        friendlyName: WAN Device
        fullName: urn:schemas-upnp-org:device:WANDevice:1
        modelDescription: WAN Device
        UDN: uuid:8c15e41f-3d83-41c1-b35d-7557B1448207
        manufacturer: TP-LINK
WANConnectionDevice
        manufacturerURL: http://www.tp-link.com.cn
        modelName: WAN Connection Device
        UPC: 123456789001
        modelNumber: 1.0
        friendlyName: WAN Connection Device
        fullName: urn:schemas-upnp-org:device:WANConnectionDevice:1
        modelDescription: WAN Connection Device
        UDN: uuid:8c15e41f-3d83-41c1-b35d-7557B1448207
        manufacturer: TP-LINK
```

host send WANConnectionDevice WANIPConnection AddProtMapping

向目标设备发送SOAP请求[^简单对象访问协议]



简单对象访问协议（Simple Object Access Protocol，SOAP）是一种标准化的通讯规范，主要用于WEB服务之中。主要广泛使用HTTP协议和XML，业界称之为“没有发明任何新技术的技术”

SOAP基本结构

```
<?xml version="1.0"?>

<soap:Envelope

xmlns:soap="http://www.w3。org/2001/12/soap-envelope"

soap:encodingStyle="http://www.w3。org/2001/12/soap-encoding">

<soap:Header>

...

</soap:Header>

<soap:Body>

...

<soap:Fault>
```

```
...

</soap:Fault>

</soap:Body>

</soap:Envelope>
```

```
Required argument:
        Argument Name:  NewPortMappingDescription
        Data Type:      string
        Allowed Values: []
        Set NewPortMappingDescription value to: 10

Required argument:
        Argument Name:  NewLeaseDuration
        Data Type:      ui4
        Allowed Values: []
        Set NewLeaseDuration value to: 29

Required argument:
```

---

pcap

被动监听UPNP发送的通知信息

```
upnp> pcap

Entering passive mode, Ctl+C to stop...

```

---

head

head show

查看当前所有头信息

```
upnp> head show

MX : 2
MAN : "ssdp:discover"
```

head del MX

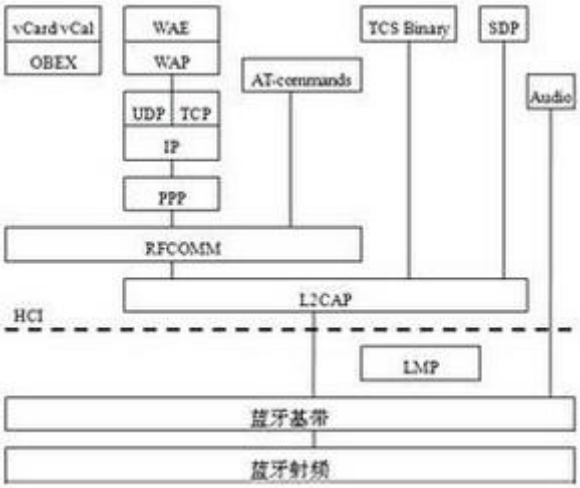
将MX头移除[^危险操作]

```
upnp> head del MX

MX removed from header list
```

```
upnp> head show

MAN : "ssdp:discover"
```

head set MX 3

添加MX 3 SSDP包头

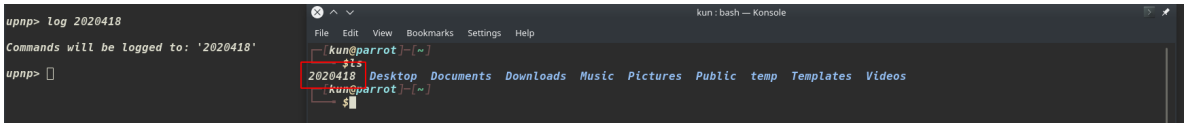


> 简单服务器发送协议（SSDP，Simple Server Discovery Protocol）是一种应用层协议，是构成即插即用（UPNP）技术的核心协议之一。在HTTP和HTTPMU的基础上实现此协议
>
> 按照协议规定，当一个客户端接入网络的时候，他可以向一个特定的多播地址上使用SSDP端口以M-SEARCH的方式发送ssdp:discover消息
>
> 放设备听到这个保留的多播地址上由控制点发送西安系的时候，设备会分析请求点的服务，如果自身带了请求点服务，设备将会通过单播的方式直接响应控制点请求。

---

log 2020418

将当前用户提供的命令保存至"2020418"文件之中

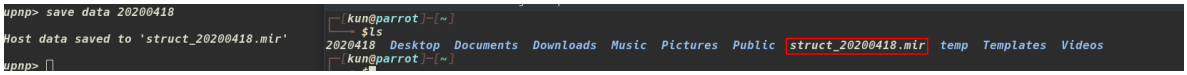


---

sava

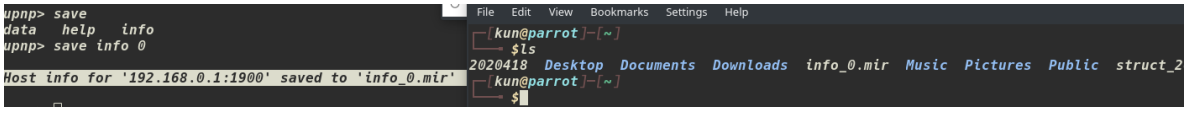
sava data 20200418

将当前主机数据保存到20200418文件之中



sava info 0

将索引号为“0”的数据以人类可读的格式输出



---

load

load struct_20200418.mir

从文件内加载以前中的文件数据

> 此处使用 “info”参数的文件你无法导入的，因为“info”参数是为了给你看的，而data 参数是为了给miranda看的

```
upnp> load struct_20200418.mir

Host data restored:

       [0] 192.168.0.1:1900
```

---

seti（高阶）

seti show

显示当前miranda配合

```
upnp> seti show

Multicast IP:           239.255.255.250
Multicast Port:         1900
Network Interface:      None
Number of known hosts:  0
UPNP Version:           1.0
Debug mode:             False
Verbose mode:           False
Show only unique hosts: True
Using log file:         False

upnp>
```

seti uniq

设置Unique模式为：False

> miranda作者北齐名约“在发现即插即用”设备时，切换“只显示uniq主机”的设置

```
upnp> seti uniq

Show unique hosts set to: False

upnp> seti show

Multicast IP:           239.255.255.250
Multicast Port:         1900
Network Interface:      None
Number of known hosts:  0
UPNP Version:           1.0
Debug mode:             False
Verbose mode:           False
Show only unique hosts: False
Using log file:         False

upnp>
```

seti debug

切换为调试模式

```
UPNP Version:           1.0
Debug mode:             True
Verbose mode:           False
```

seti verbose

切换为详细模式[^这个可以有]

```
UPNP Version:           1.0
Debug mode:             True
Verbose mode:           False
```

seti version 520

更改即插即用版本为“520‘[^也许可以在和你女朋友谈情说爱的时候使用到～]

```
upnp> seti version 520

UPNP version set to: 520

upnp> seti show

Multicast IP:           239.255.255.250
Multicast Port:         1900
Network Interface:      None
Number of known hosts:  0
UPNP Version:           520
Debug mode:             False
```

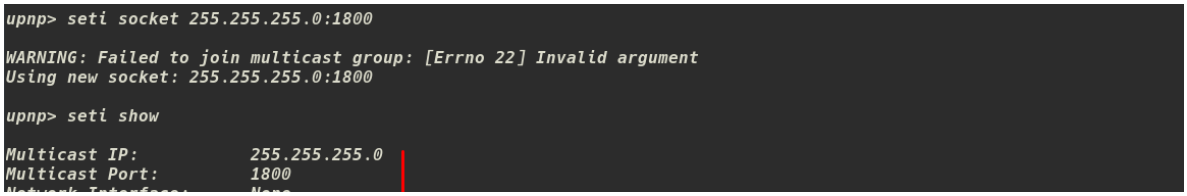
seti iface vmnet8

将网卡接口指定为vmnet8

> 这在miranda中打错了，所以miranda来提醒我是否拥有此接口（网卡）的所有权？
>
> 正确的应该为 vmnet8，vmnet8是我的VMware中的虚拟网卡，用于给Ubuntu 192.168.11.0网段所使用，
>
> 在正常情况下你可以选择miranda默认的或者是你物理机的echo0或wlan0都是可以的。

seti socket 255.255.255.0:1800""

重新设置用于发现即插即用设的广播/多播的IP地址和端口号



退出命令

quit

"Exit this shell"

> “这优美的描述让我不知如何表达”
>
> **quit**
>
> quit参数是指你在一个命令之中，比如你输入miranda，进入了upnp即插即用模式的第二级，就拿以下图为例：
>
> > 我是第一级 Upnp
> >
> > > 我是第二级upnp
>
> 此时你使用quit参数是指你在upnp模式下退出到第一级而不完全退出
>
> **exit**
>
> 但是你如果使用exit的话，不管你在那一个级，都将直接退出miranda。就如下图为例
>
> > 系统终端
> >
> > > miranda
> > >
> > > > Upnp
>
> 此时你如果在Upnp模式下，使用exit的话将会直接退出到系统终端中。

exit

"Exit this shell"

补充

"即使在非交互式模式下，也可以使用miranda，与交互模式不同的是在非交互模式中miranda的参数有一些被简化了，这也方便了安全研究人员的使用并提高了用户的体验和便捷性。

具体的使用方法与交互模型类似，只不过有了一些简化命令，比如load被简化成了"-s"参数，意思不变。

> 命令行用法：usr/bin/miranda[选项]
> -s从结构文件加载以前的主机数据
> -l将用户提供的命令记录到日志文件
> -i指定要使用的接口的名称（仅限Linux，需要根目录）
> -u禁用仅显示uniq主机选项
> -d启用调试模式
> -v启用详细模式
> -h显示帮助

参考资料：

> 简单服务器发送协议 https://baike.sogou.com/v66199633.htm?fromTitle=SSDP