

AirNet (PPTP) on linux

- Overview
- Requirements
- MPPE
- Security
- Installation
- Configuration
- Getting it going
- Examples
- Resources (links)

VPN, PPTP & AirNet

- What is VPN?
- What is PPTP?
- How does AirNet work
 - Signing up for AirNet
 - Is AirNet the right solution?

PPTP

- Requirements:
 - PPP (>2.4.2)
 - MPPE
 - linux kernel(>2.6.15*)
 - pptp-linux
 - Routing scripts

MPPE

- Microsoft Point-to-Point Encryption (RFC 3078)
- Encrypts using RC4
 - 128bit, but there is less entropy in reality
- Data compression (patented MPPC algorithm)
- Linux issues
 - Support is finally here
 - Supported with kernel 2.6.15 or greater
 - Old kernels can be patched

Security

- Authentication
 - PPTP uses MS-CHAPv2
 - susceptible to brute force attack if data stream is captured
 - Use strong passwords (although school assigns them)
- MPPE
 - uses RC4 stream encryption
 - key can be derived from MS-CHAPv2 credentials
- All in all AirNet might still be more secure than ResNet

Installing

- pptp-linux
 - Debian/ubuntu
 - apt-get install pptp-linux
 - FC1-5, gentoo, madrake, netbsd, redhat, suse
 - RTFM (:
 - <http://pptpclient.sourceforge.net/documentation.phtml>
- pptpconfig
 - GUI configuration tool
 - Not needed

Configuration

- pptpconfig vs config by hand
- Download my config files and Edit:
 - /etc/ppp/chap-secrets
 - Line 3
 - /etc/ppp/ip-up.local (overrides routing scripts)
 - Line 5
 - /etc/ppp/ip-down.local (overrides routing scripts)
 - Line 5
 - /etc/ppp/pap-secrets
 - Line 43
 - /etc/ppp/peers/sunysb
 - Line 2

Getting it going

```
~# iwconfig $INTERFACE essid $ESSID
```

```
~# ifup $INTERFACE
```

```
~# pon $TUNNEL # or
```

OR

```
~#pon $TUNNEL debug dump logfd 2 nodetach # for debugging
```

```
~# poff $TUNNEL
```

```
~# ifdown $INTERFACE
```

```
ilya-lap:~# pon sunysb debug dump logfd 2 nodetach
```

```
pppd options in effect:
```

```
debug          # (from command line)
nodetach       # (from command line)
logfd 2       # (from command line)
dump          # (from command line)
noauth        # (from /etc/ppp/options.pptp)
name $USERNAME # (from /etc/ppp/peers/sunysb)
remotename PPTP # (from /etc/ppp/peers/sunysb)
              # (from /etc/ppp/options.pptp)
pty pptp vpn.sunysb.edu --nolaunchpppd # (from /etc/ppp/peers/sunysb)
crtscts       # (from /etc/ppp/options)
              # (from /etc/ppp/options)
asyncmap 0    # (from /etc/ppp/options)
lcp-echo-failure 4 # (from /etc/ppp/options)
lcp-echo-interval 30 # (from /etc/ppp/options)
hide-password # (from /etc/ppp/options)
ipparam tunnel # (from /etc/ppp/peers/sunysb)
proxyarp     # (from /etc/ppp/options)
nobsdcomp    # (from /etc/ppp/options.pptp)
nodeflate    # (from /etc/ppp/options.pptp)
require-mppe-128 # (from /etc/ppp/peers/sunysb)
noipx       # (from /etc/ppp/options)
```

```
using channel 7
```

```
Using interface ppp0
```

```
Connect: ppp0 <--> /dev/pts/23
```

```
sent [LCP ConfReq id=0x1 <asyncmap 0x0> <magic 0x3d1500ea> <pcomp> <accomp>]
```

```
rcvd [LCP ConfReq id=0x0 <auth chap MS-v2>]
```

```
sent [LCP ConfAck id=0x0 <auth chap MS-v2>]
```

```
rcvd [LCP ConfAck id=0x1 <asyncmap 0x0> <magic 0x3d1500ea> <pcomp> <accomp>]
```

```
sent [LCP EchoReq id=0x0 magic=0x3d1500ea]
```

```
rcvd [CHAP Challenge id=0x1 <STUFF>, name = ""]
```

```
sent [CHAP Response id=0x1 <STUFF>, name = "$USERNAME"]
```

```
rcvd [LCP EchoRep id=0x0 magic=0x0]
rcvd [CHAP Challenge id=0x2 <STUFF>, name = ""]
sent [CHAP Response id=0x2 <STUFF>, name = "$USERNAME"]
rcvd [CHAP Success id=0x2 "S=STUFF"]
CHAP authentication succeeded
sent [CCP ConfReq id=0x1 <mppe +H -M +S -L -D -C>]
rcvd [IPCP ConfReq id=0x0 <addr 10.255.252.2>]
sent [IPCP TermAck id=0x0]
rcvd [CCP ConfReq id=0x0 <mppe +H -M +S +L -D +C>]
sent [CCP ConfNak id=0x0 <mppe +H -M +S -L -D -C>]
rcvd [CCP ConfNak id=0x1 <mppe +H -M +S -L -D -C>]
sent [CCP ConfReq id=0x2 <mppe +H -M +S -L -D -C>]
rcvd [CCP ConfReq id=0x1 <mppe +H -M +S -L -D -C>]
sent [CCP ConfAck id=0x1 <mppe +H -M +S -L -D -C>]
rcvd [CCP ConfAck id=0x2 <mppe +H -M +S -L -D -C>]
MPPE 128-bit stateless compression enabled
sent [IPCP ConfReq id=0x1 <compress VJ 0f 01> <addr 0.0.0.0>]
rcvd [IPCP ConfReq id=0x1 <addr 10.255.252.2>]
sent [IPCP ConfAck id=0x1 <addr 10.255.252.2>]
sent [IPCP ConfReq id=0x1 <compress VJ 0f 01> <addr 0.0.0.0>]
rcvd [IPCP ConfRej id=0x1 <compress VJ 0f 01>]
sent [IPCP ConfReq id=0x2 <addr 0.0.0.0>]
rcvd [IPCP ConfNak id=0x2 <addr 129.49.5.179>]
sent [IPCP ConfReq id=0x3 <addr 129.49.5.179>]
rcvd [IPCP ConfAck id=0x3 <addr 129.49.5.179>]
found interface wlan0 for proxy arp
local IP address 129.49.5.179
remote IP address 10.255.252.2
Script /etc/ppp/ip-up started (pid 580)
Script /etc/ppp/ip-up finished (pid 580), status = 0x0
Terminating on signal 2
Script pptp vpn.sunysb.edu --nolaunchpppd finished (pid 570), status = 0x0
Modem hangup
```

Connect time 50.1 minutes.
Sent 194410 bytes, received 736101 bytes.
Script /etc/ppp/ip-down started (pid 1110)
MPPE disabled
sent [LCP TermReq id=0x2 "MPPE disabled"]
Connection terminated.
Script /etc/ppp/ip-down finished (pid 1110), status = 0x0

Example

```
ilya-lap:~# iwconfig wlan0 mode managed && iwconfig wlan0 essid AirNet
```

```
ilya-lap:~# ifup wlan0
```

```
ilya-lap:~# pon sunysb
```

```
ilya-lap:~# route
```

```
Kernel IP routing table
```

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
prv.no-wire.sto	*	255.255.255.255	UH	0	0	0	wlan0
10.255.252.0	*	255.255.252.0	U	0	0	0	wlan0
default	*	0.0.0.0	U	0	0	0	wlan0

```
ilya-lap:~# route
```

```
Kernel IP routing table
```

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
prv.no-wire.sto	*	255.255.255.255	UH	0	0	0	wlan0
prv.no-wire.sto	*	255.255.255.255	UH	0	0	0	ppp0
10.255.252.0	*	255.255.252.0	U	0	0	0	wlan0
default	*	0.0.0.0	U	0	0	0	ppp0

Resources

- <http://pptpclient.sourceforge.net/>
 - Step by step guides
 - trouble shooting tips
- <http://pptpclient.sourceforge.net/routing.phtml#all-to-tunnel>
 - Configure routing scripts
- <http://dotcommie.net/lugsb/>
 - my config files

Presentation by

- Ilya Sukhanov (dotCOMmie)
- contact:
 - mailing list:
<http://www.fsl.cs.sunysb.edu/mailman/listinfo/lugsb>