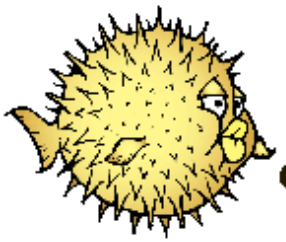


OpenBSD

Failover Firewalls

Florin Iamandi

http://todome.net https://verona.linux.it

Presentiamoci...

- Florin Iamandi - Slippery
- 19771003, Romania
- tech support, sysadmin
- OpenBSD enthusiast, Perl pilgrim
- Home page: http://todome.net

Sommario

- Introduzione
- OpenBSD
- PF
- pfsync
- CARP
- Configurazione
- LIVE ACTION!

Introduzione - Finalita'

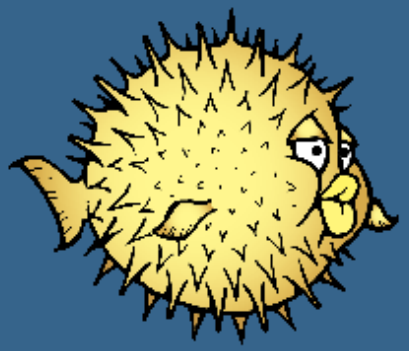
- Capire che la ridondanza e' importante
- Presentare un metodo per mettere in produzione firewall ridondanti
- Utilizzare tecnologia High-End applicabile anche negli ambienti medio-piccoli
- Usare strumenti e sistemi Open Source!!

Introduzione - Vocabolario

- High Availability
- Single Point of Failure
- Redundancy
- Failover
- Firewall

OpenBSD - http://openbsd.org

- UNIX-like, BSD 4.4, Open Source
- Multi-piattaforma, multi-uso
- Sicurezza proattiva, crittografia integrata
- Standard compliant, tecnologie innovative
- Fortezza del movimento Free Software contro le licenze restrittive



OpenBSD - Multi-piattaforma

alpha
amd64
aviion
cats
hp300
hppa
hppa64
i386
luna88k
mac68k
macppc
mvme68k
mvme88k
sgi
solbourne
sparc
sparc64
vax
zaurus

VIA Eden embedded i386

OpenBSD - http://openbsd.org

OpenBSD - OpenSSH

- Vi ricordate SSH?
- 90% dei server usano OpenSSH - standard "de facto"
- http://openssh.org

PF - Packet Filter

- PF e' lo strumento nativo di OpenBSD per il filtraggio dei pacchetti TCP/IP
- IPF e' stato rimosso dal source tree il 2001/05/29 a seguito di un cambio di licenza
- Creato da Daniel Hartmeier
- Introdotto nel source tree il 2001/06/24
- Rilasciato con la versione 3.0 il 2001/12/01

PF - Packet Filter

- Filtra il traffico TCP/IP
- NAT, reindirizzamento e nomalizzazione del traffico
- Traffic shaping, prioritizzazione dei pacchetti
- Load Balancing
- Passive OS Fingerprinting - filtra in base al sistema operativo

pfsync

- Riasciato il 2003/05/01 con OpenBSD 3.3
- Pseudo-device usato per la sincronizzazione delle tabelle di stato dei firewall
- Mette le basi per un failover "grazioso" senza perdere la connettivita' - ridondanza "stateful"

pfsync

- La sincronizzazione dei firewall e' fatta via rete
- Gli aggiornamenti sono mandati in multicast e senza autenticazione (crossover, IPsec)
- Non abbiamo i requisiti per un failover dinamico nativo. Non ancora... Pero'...

Entra il CARP!

- Common Address Redundancy Protocol
- Alternativa Open Source sicura ai protocolli proprietari di Cisco e Juniper
  - VRRP - Virtual Router Redundancy Protocol
  - HSRP - Hot Standby Router Protocol
- Rilasciato il 2004/05/01 con OpenBSD 3.5
- E' la prima implementazione per il failover stateful dei firewall che supporta il protocollo IPv6

CARP

- Consente ad un gruppo di host appartenenti ad un segmento di rete di condividere un indirizzo IP virtuale - gruppo di "ridondanza"
- Con l'IP virtuale e' creato anche un MAC address virtuale
- Aiuta a creare servizi ridondanti (DNS, FTP, HTTP etc.)
- Puo' fare anche load-balancing e preemption

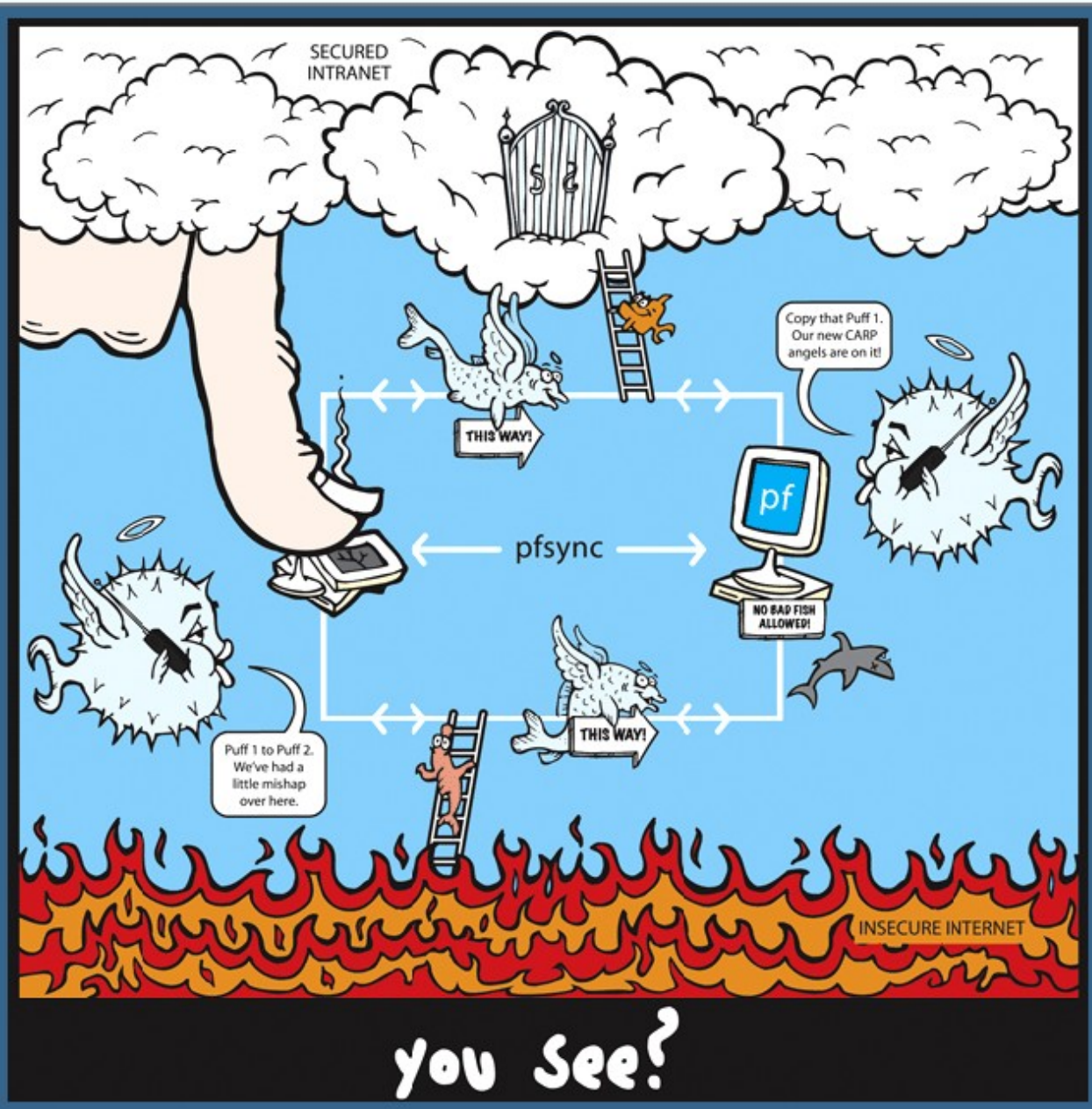
CARP

- Il guppo di ridondanza e' composto da un host MASTER e uno o piu' host di BACKUP
- Il MASTER manda constantemente avvisi per far sapere agli altri host del gruppo che e' online
- Ogni gruppo di ridondanza puo' essere cofigurato con una password per proteggere gli avvisi con l'algoritmo di cifratura SHA-1

CARP

- Se gli host di BACKUP non ricevono avvisi uno di questi host prende il ruolo di MASTER
- Il ruolo di MASTER viene preso dall'host che manda avvisi con la frequenza piu' di alta (advbase, advskew)
- F = advbase + (advskew / 256)
- Default: advbase = 1, advskew = 0

Finalmente failover dinamico!



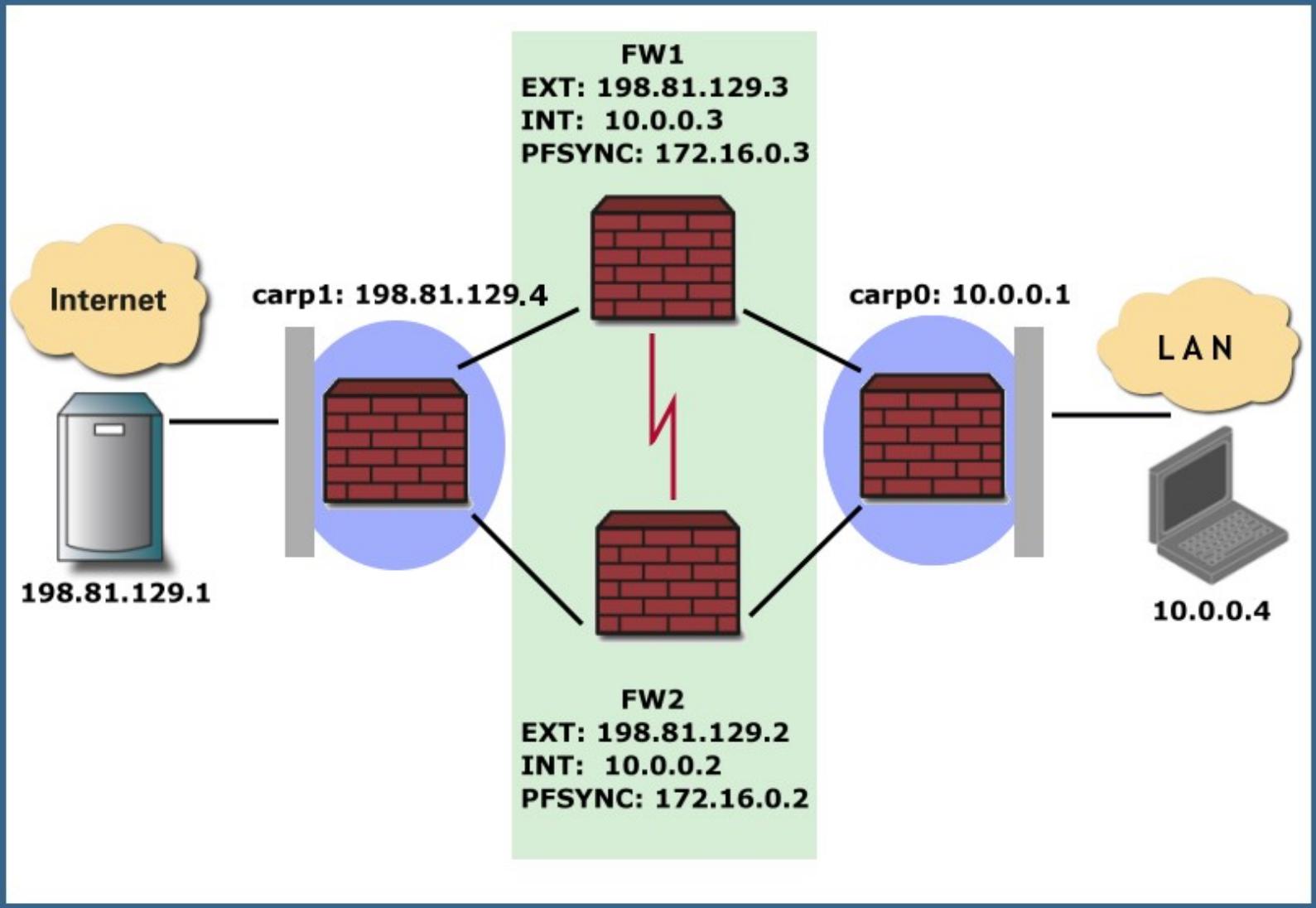
Live - Introduzione

- NFS mount over OpenVPN simulando una connessione site-to-site criptata e sicura
- Ascolteremo una canzone "over network"
- Abuseremo il sistema di firewall piu' volte ed in diversi modi
- Funzionera' - "It just works"

Live - Elementi extra

- Canzone:
  - Greg Tuby, RedHeat
  - http://www.sonicsoundscapes.com
  - The Escape from Marwinia
- Player:
  - http://mpg321.sourceforge.net
  - Il buffering non e' supportato, niente trucchi, quello che vi mostrero' sara' per davvero
- OpenVPN:
  - http://openvpn.net
  - Open Source SSL/TLS VPN

Network Layout



Configurazione - MASTER

```
# cat /etc/hostname.carp0
inet 10.0.0.1 255.255.255.0 NONE vhid 2 pass ciccio

# cat /etc/hostname.carp1
inet 198.81.129.4 255.255.255.0 NONE vhid 1 pass pippo

# cat /etc/hostname.em0
inet 172.16.0.3 255.255.255.248 NONE

# cat /etc/hostname.fxp0
inet 198.81.129.3 255.255.255.0 NONE

# cat /etc/hostname.fxp1
inet 10.0.0.3 255.255.255.0 NONE

# cat hostname.pfsync0
up syncif em0
```

Configurazione - BACKUP

```
# cat /etc/hostname.carp0
inet 10.0.0.1 255.255.255.0 NONE vhid 2 \
        advskew 100 pass ciccio

# cat /etc/hostname.carp1
inet 198.81.129.4 255.255.255.0 NONE vhid 1 \
        advskew 100 pass pippo

# cat /etc/hostname.em0
inet 172.16.0.2 255.255.255.248 NONE

# cat /etc/hostname.fxp0
inet 198.81.129.2 255.255.255.0 NONE

# cat /etc/hostname.fxp1
inet 10.0.0.2 255.255.255.0 NONE

# cat hostname.pfsync0
up syncif em0
```

Configurazione - /etc/pf.conf

```
ext_if="fxp0"
int_if="fxp1"
pfsync_if="em0"
carp1="198.81.129.4"

set block-policy return

scrub in all

nat on $ext_if from $int_if:network to any -> $carp1

block in log on $ext_if
pass quick on { lo $int_if }
pass quick on $pfsync_if proto pfsync
pass quick on { $ext_if $int_if } proto carp keep state
pass out on $ext_if keep state
```

Configurazione - Generale

Viariabili di sistema

```
# tail -2 /etc/sysctl.conf
net.inet.ip.forwarding=1
net.inet.carp.preempt=1
```

Abbilitiamo PF

```
# cat /etc/rc.conf.local
pf=YES
pf_rules=/etc/pf.conf
pflogd_flags="-f /var/log/pflog"
```

Stato iniziale

- master (FW1)

```
# ifconfig carp0; ifconfig carp1
carp0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        carp: MASTER carpdev fxp1 vhid 2 advbase 1 advskew 0
        groups: carp
        inet 10.0.0.1 netmask 0xffffff00 broadcast 10.0.0.255
carp1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        carp: MASTER carpdev fxp0 vhid 1 advbase 1 advskew 0
        groups: carp
        inet 198.81.129.4 netmask 0xffffff00 broadcast 198.81.129.255
#
```

- backup (FW2)

```
# ifconfig carp0; ifconfig carp1
carp0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        carp: BACKUP carpdev fxp1 vhid 2 advbase 1 advskew 100
        groups: carp
        inet 10.0.0.1 netmask 0xffffff00 broadcast 10.0.0.255
carp1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        carp: BACKUP carpdev fxp0 vhid 1 advbase 1 advskew 100
        groups: carp
        inet 198.81.129.4 netmask 0xffffff00 broadcast 198.81.129.255
#
```

Abusare ed usare il sistema

- 3, 2, 1, musica!

```
# mpg321 /mnt/The_Escape_from_Marwinia.mp3
High Performance MPEG 1.0/2.0/2.5 Audio Player for Layer 1, 2, and 3.
Version 0.59q (2002/03/23). Written and copyrights by Joe Drew.
Uses code from various people. See 'README' for more!
THIS SOFTWARE COMES WITH ABSOLUTELY NO WARRANTY! USE AT YOUR OWN RISK!
Title  : The Escape from Marwinia        Artist: RedHeat (m0d)
Album  : www.sonicsoundscapes.com        Year  : 2006
Comment:                                 Genre : InstrumentalInstrumental

Directory: /mnt/
Playing MPEG stream from The_Escape_from_Marwinia.mp3 ...
MPEG 1.0 layer III, 192 kbit/s, 44100 Hz joint-stereo
```

- master diservizio/upgrade/manutenzione

```
# sleep 10; reboot
Connection to kuro closed by remote host.
Connection to kuro closed.
#
```

I love music!

```
# cat monitor.sh
while :; do sleep 1; clear; ifconfig carp0; ifconfig carp1; \
        echo "\n let the music play...\n"; done
# ./monitor.sh
```

- dopo 10 secondi il BACKUP diventa MASTER

```
carp0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        carp: BACKUP carpdev fxp1 vhid 2 advbase 1 advskew 100
        groups: carp
        inet 10.0.0.1 netmask 0xffffff00 broadcast 10.0.0.255
carp1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        carp: BACKUP carpdev fxp0 vhid 1 advbase 1 advskew 100
        groups: carp
        inet 198.81.129.4 netmask 0xffffff00 broadcast 198.81.129.255

 let the music play...
```

```
carp0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        carp: MASTER carpdev fxp1 vhid 2 advbase 1 advskew 100
        groups: carp
        inet 10.0.0.1 netmask 0xffffff00 broadcast 10.0.0.255
carp1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        carp: MASTER carpdev fxp0 vhid 1 advbase 1 advskew 100
        groups: carp
        inet 198.81.129.4 netmask 0xffffff00 broadcast 198.81.129.255

 let the music play...
```

I LOVE music!

- dopo qualche minuto il MASTER ritorna...

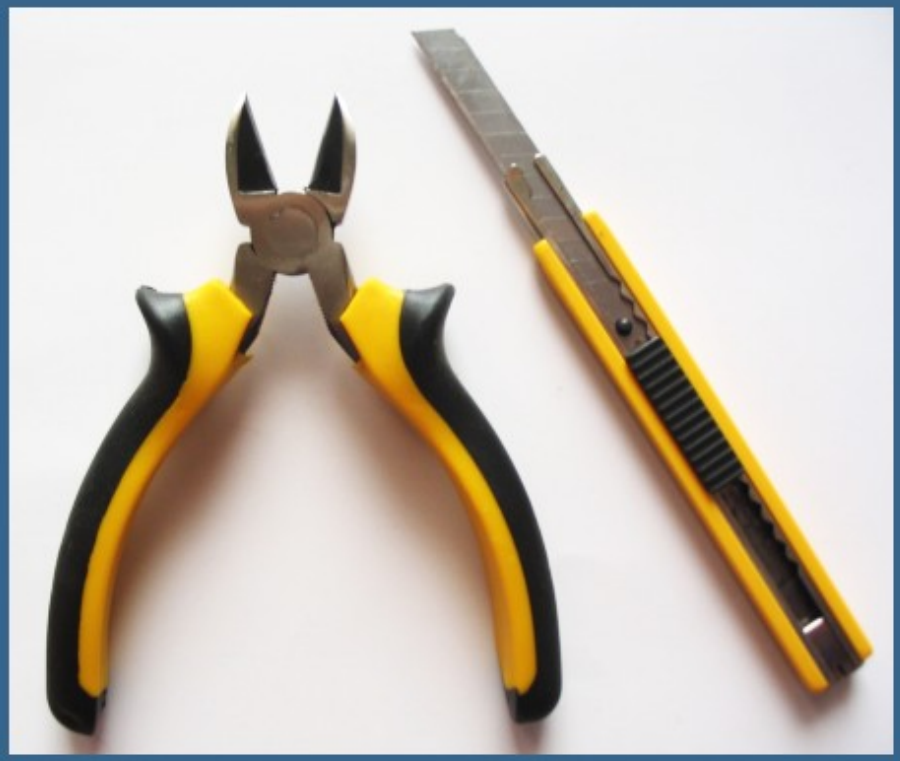
```
carp0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        carp: BACKUP carpdev fxp1 vhid 2 advbase 1 advskew 100
        groups: carp
        inet 10.0.0.1 netmask 0xffffff00 broadcast 10.0.0.255
carp1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        carp: BACKUP carpdev fxp0 vhid 1 advbase 1 advskew 100
        groups: carp
        inet 198.81.129.4 netmask 0xffffff00 broadcast 198.81.129.255

 let the music play...
```

- ... e non abbiamo perso nessuna nota!

```
[8:39] Decoding of The_Escape_from_Marwinia.mp3 finished.
#
```

Abusare dei cavi!



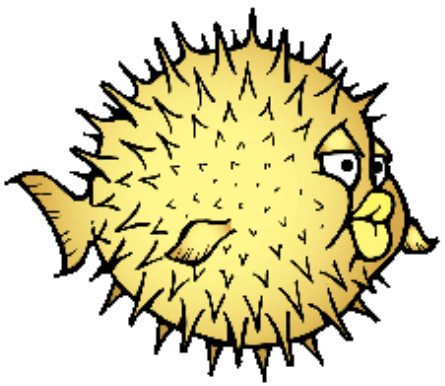
Qualcuno ha voglia? Avrei bisogno di un volontario per favore.

GRAZIE!

Aaron Campbell, Aleksander Piotrowski, Alex Feldman, Alexander Guy, Alexander von Gernler, Alexander Yurchenko, Alexandre Anriot, Andreas Gunnarsson, Angelos D. Keromytis, Anil Madhavapeddy, Artur Grabowski, Ben Lindstrom, Bernd Ahlers, Bjorn Sandell, Bob Beck, Brad Smith, Brandon Creighton, Brian Caswell, Brian Somers, Bruno Rohee, Camiel Dobbelaar, Can Erkin Acar, Cedric Berger, Chad Loder, Chris Cappuccio, Christian Weisgerber, Christopher Pascoe, Claudio Jeker, Constantine Sapuntzakis, Dale Rahn, Damien Bergamini, Damien Couderc, Damien Miller, Dan Harnett, Daniel Hartmeier, Darren Tucker, David B Terrell, David Gwynne, David Krause, David Lebel, David Leonard, Don Stewart, Dug Song, Eric Jackson, Esben Norby, Federico G. Schwindt, Fernando Gont, Greg Taleck, Grigoriy Orlov, Hakan Olsson, Hans Insulander, Hans-Joerg Hoexer, Heikki Korpela, Henning Brauer, Henric Jungheim, Hiroaki Etoh, Horacio Menezo Ganau, Hugh Graham, Ian Darwin, Jacob Meuser, Jakob Schlyter, Jan-Uwe Finck, Jared J. Yanovich, Jason Ish, Jason McIntyre, Jason Peel, Jason Wright, Jean-Baptiste Marchand, Jean-Francois Brousseau, Jean-Jacques Bernard-Gundol, Jim Rees, Joel Knight, Jolan Luff, Jonathan Gray, Jordan Hargrave, Joris Vink, Jose Nazario, Joshua Stein, Jun-ichiro itojun Hagino, Kenji Aoyama, Kenjiro Cho, Kenneth R Westerback, Kevin Lo, Kevin Steves, Kjell Wooding, Kurt Miller, Louis Bertrand, Magnus Holmberg, Marc Balmer, Marc Espie, Marc Matteo, Marco Peereboom, Marco Pfatschbacher, Marco S Hyman, Marcus Watts, Margarida Sequeira, Marius Eriksen, Mark Grimes, Mark Kettenis, Markus Friedl, Martin Reindl, Mathieu Sauve-Frankel, Mats O Jansson, Matt Behrens, Matt Smart, Matthew Jacob, Matthieu Herrb, Michael Coulter, Michael Shalayeff, Michael T. Stolarchuk, Mike Frantzen, Mike Pechkin, Miod Vallat, Moritz Jodeit, Nathan Binkert, Niall O'Higgins, Nick Holland, Niels Provos, Niklas Hallqvist, Nikolay Sturm, Nils Nordman, Oleg Safiullin, Otto Moerbeek, Patrick Latifi, Paul Janzen, Pedro Martelletto, Peter Galbavy, Peter Stromberg, Peter Valchev, Philipp Buehler, Reinhard J. Sammer, Ray Lai, Reyk Floeter, Rich Cannings, Robert Nagy, Ryan Thomas McBride, Saad Kadhi, Shell Hin-lik Hung, Stephen Kirkham, Steve Murphree, Ted Unangst, Theo de Raadt, Thierry Deval, Thomas Nordin, Thorsten Lockert, Tobias Weingartner, Todd C. Miller, Todd T. Fries, Tom Cosgrove, Uwe Stuehler, Vincent Labrecque, Wilbern Cobb, Wim Vandeputte, Xavier Santolaria.

Grazie!

GRAZIE!



OpenBSD

http://openbsd.org

http://openssh.org

http://openbgp.org