

OpenSSH config tricks

Secure network connections to
remote hosts, plus some tricks

Malcolm Herbert
mjch@mjch.net
2015-05-25

Assumptions

- know about ssh key-based logins
- know about ssh agents

Project goals

- hosts know their peers by name
- don't expose host IPs in config
- single command to furthest remote
- ssh key agent control at each hop

~/.ssh/config globbing

Host config details collected in file order, where the supplied name matches the stanza glob

Config added until file is exhausted, if hostname parameter changes, config is reread (not sure how recent this feature is, tbh)

~/.ssh/config globbing (ctd)

```
host eeny
  user joeb
  identityfile ssh/keys/joeb

host meeny
  user root

host *
  user jbloggs
  identityfile ssh/keys/jbloggs
```

ssh proxycommand

- tunnel ssh over another protocol
- usually corkscrew for http tunnels
- netcat or socat preferred, 8bit clean
- some versions of telnet might work

ssh proxycommand (ctd)

general use with netcat:

```
proxycommand nc %h %p
```

- uses netcat to open TCP tunnel
- %h replaced with remote hostname
- %p replaced with remote port
- other substitutions available too

config stanza breakdown

- 'host' shortcuts call 'host-via-host'
- 'host-via-*' give access details
- '*-via-host' give forwarding details
- '*' stanza gives general defaults

config stanza breakdown (ctd)

```
host meeny  
    hostname meeny-via-eeny
```

```
host meeny-via-  
    forwardagent yes
```

```
host *-via-meeny  
    proxycommand ...
```

ssh-in-ssh tunnels

- (ab)use the proxycommand
- combine ssh+nc to advance tunnel
- pro: single local config for all hops
- con: local end multiply encrypted

ssh-in-ssh tunnels (ctd)

```
host jump
```

```
...
```

```
host remote
```

```
proxycommand ssh jump nc %h %p
```

ssh agents and keys

- pre-load agent with all tunnel keys
- tag '*-via-host' with required key
- use identitiesonly in general config

ssh agents and keys (ctd)

```
host *  
  user jbloggs  
  identitiesonly true  
  identityfile ssh/keys/jbloggs
```

ssh agent forwarding

- pro: useful to pass keys
- con: dangerous to pass keys
- use forwardagent config
- be selective about exposure

ssh agent forwarding (ctd)

```
host meeny  
    forwardagent yes
```

```
host *  
    forwardagent no
```

controlmaster shenanigans

- post-authenticated sub-channel
- used to spawn remote commands
- can't modify established connection
- accessed via local sockets
- sockets can be shared
- may be set to persist
- con: post-auth, needs securing!

controlmaster shenanigans (ctd)

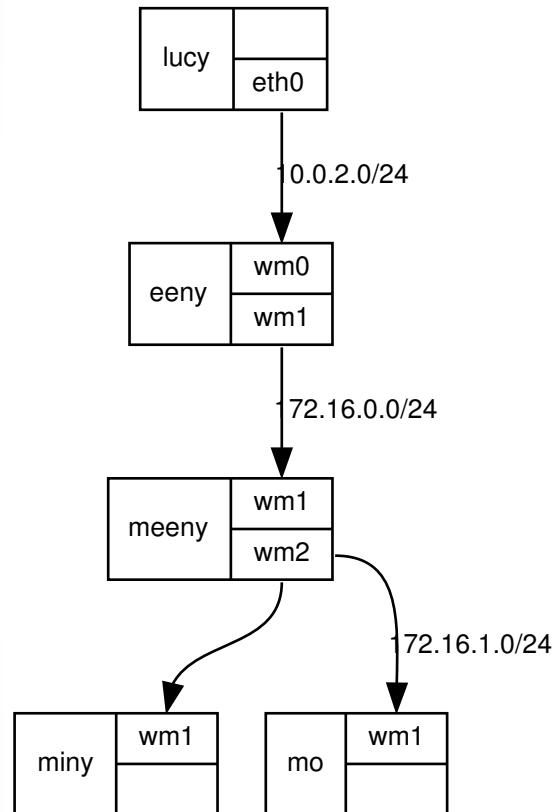
```
host *  
  controlmaster auto  
  controlpersist no  
  controlpath run/%u@%L-%u@%n:%p
```

putting it all together

Our lab network:

- four VMs: eeny, meeny, miny and mo
- access to meeny only via eeny
- access to miny and mo only via meeny

putting it all together (ctd)



ssh/config

```
# eeny config
```

```
host eeny
```

```
    identityfile ssh/keys/joeb
```

```
    hostname localhost
```

```
    port 14710
```

```
    user joeb
```

```
host *-via-eeny
```

```
    identityfile ssh/keys/joeb
```

```
    proxycommand ssh -F ssh/config eeny /usr/pkg/sbin/nc \
```

```
        `echo %h | sed -e 's/-via.*//'\` %p
```

ssh/config (ctd)

```
# meeny config
```

```
host meeny
```

```
    hostname meeny-via-eeny
```

```
host meeny-via-*
```

```
    forwardagent yes
```

```
host *-via-meeny
```

```
    proxycommand ssh -F ssh/config meeny /usr/pkg/sbin/nc \  
    `echo %h | sed -e 's/-via.*//'\` %p
```

ssh/config (ctd)

```
# miny config
```

```
host miny
```

```
    hostname miny-via-meeny
```

```
host miny-via-*
```

```
    forwardagent yes
```

```
host *-via-miny
```

```
# nop
```

ssh/config (ctd)

```
# mo config
```

```
host mo
```

```
    hostname mo-via-meeny
```

```
host mo-via-*
```

```
    identityfile ssh/keys/sekret
```

```
host *-via-mo
```

```
# nop
```

ssh/config (ctd)

```
# general config
```

```
host *
```

```
    user jbloggs
```

```
    identitiesonly true
```

```
    identityfile ssh/keys/jbloggs
```

```
    controlmaster auto
```

```
    controlpersist no
```

```
    controlpath run/%u@%L-%u@%n:%p
```


connection breakdown

lucy	
	eth0

eeny	wm0
	wm1

meeny	wm1
	wm2

miny	wm1

mo	wm1

connection breakdown

lucy	
	eth0



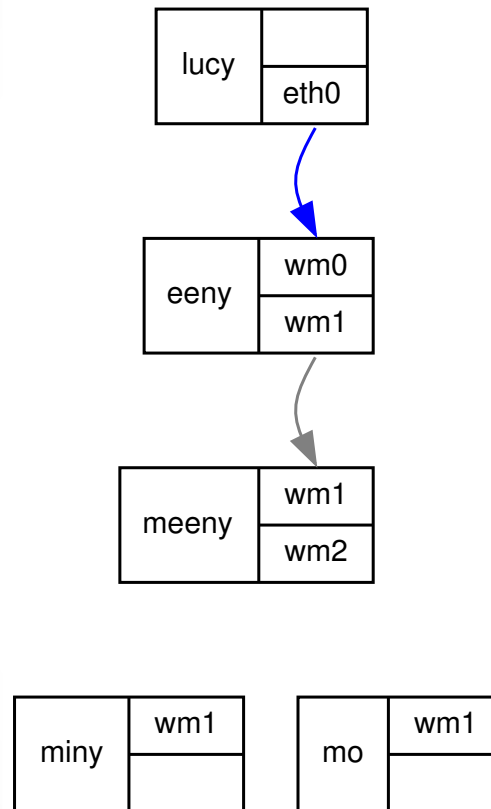
eeny	wm0
	wm1

meeny	wm1
	wm2

miny	wm1

mo	wm1

connection breakdown (ctd)



connection breakdown (ctd)

lucy	
	eth0



eeny	wm0
	wm1

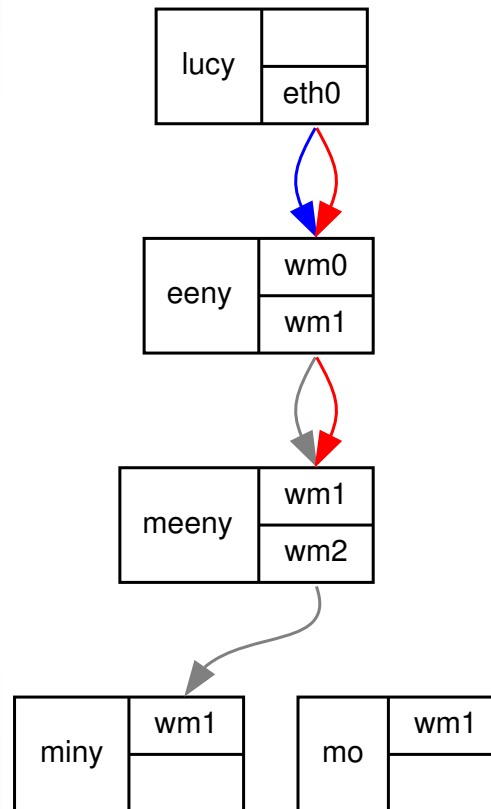


meeny	wm1
	wm2

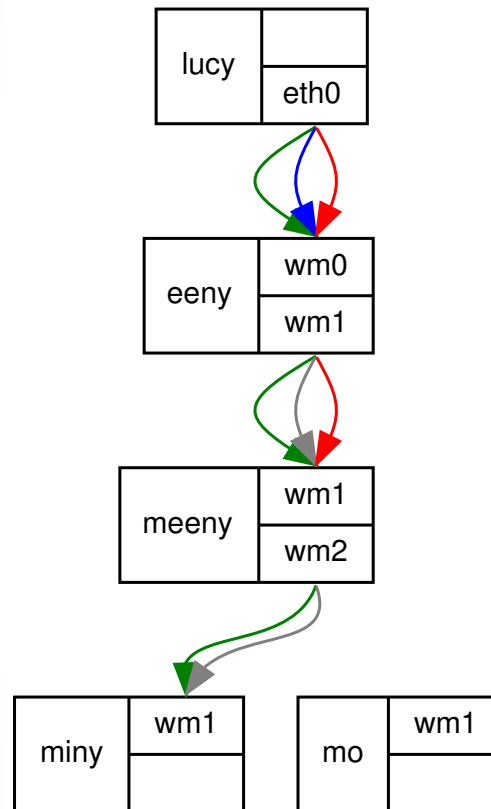
miny	wm1

mo	wm1

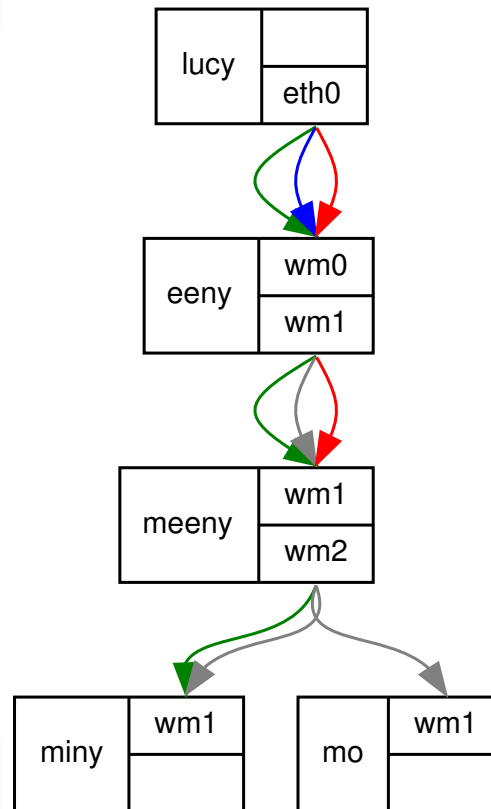
connection breakdown (ctd)



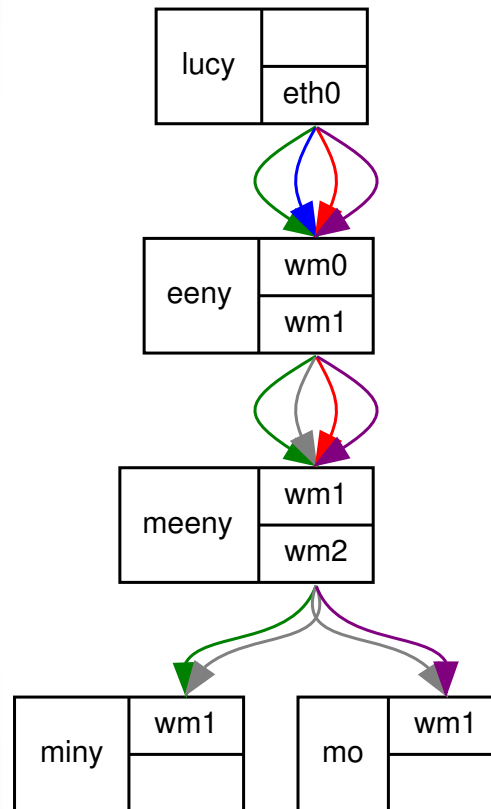
connection breakdown (ctd)



connection breakdown (ctd)



connection breakdown (ctd)



Live demo

`*crosses fingers*`

Comments, questions?

OpenSSH config tricks

Secure network connections to
remote hosts, plus some tricks

Malcolm Herbert
mjch@mjch.net
2015-05-25

License

Copyright (c) 2015, Malcolm Herbert. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS MATERIAL IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.