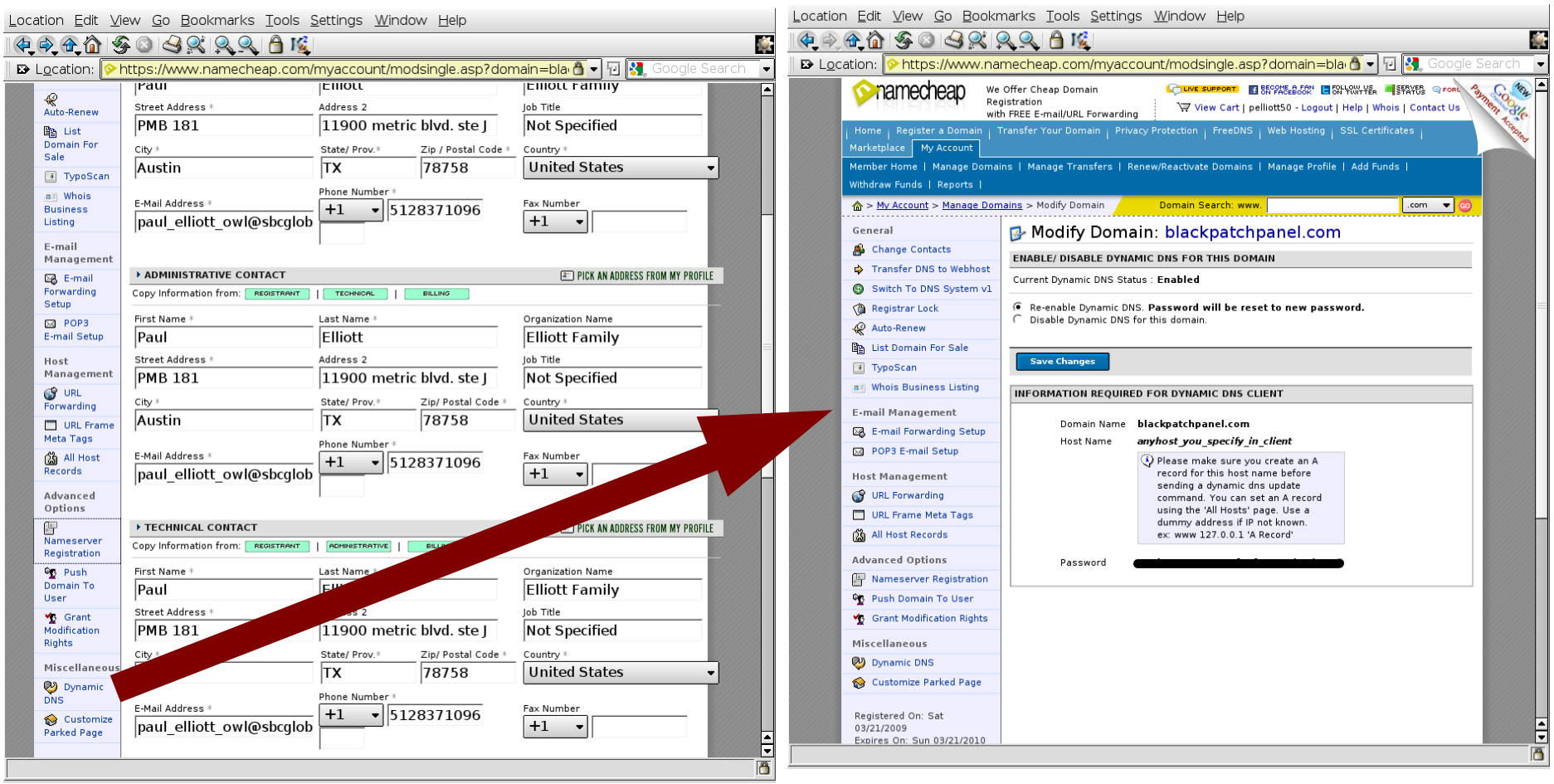
Phone Home

Use Dynamic DNS to phone home!

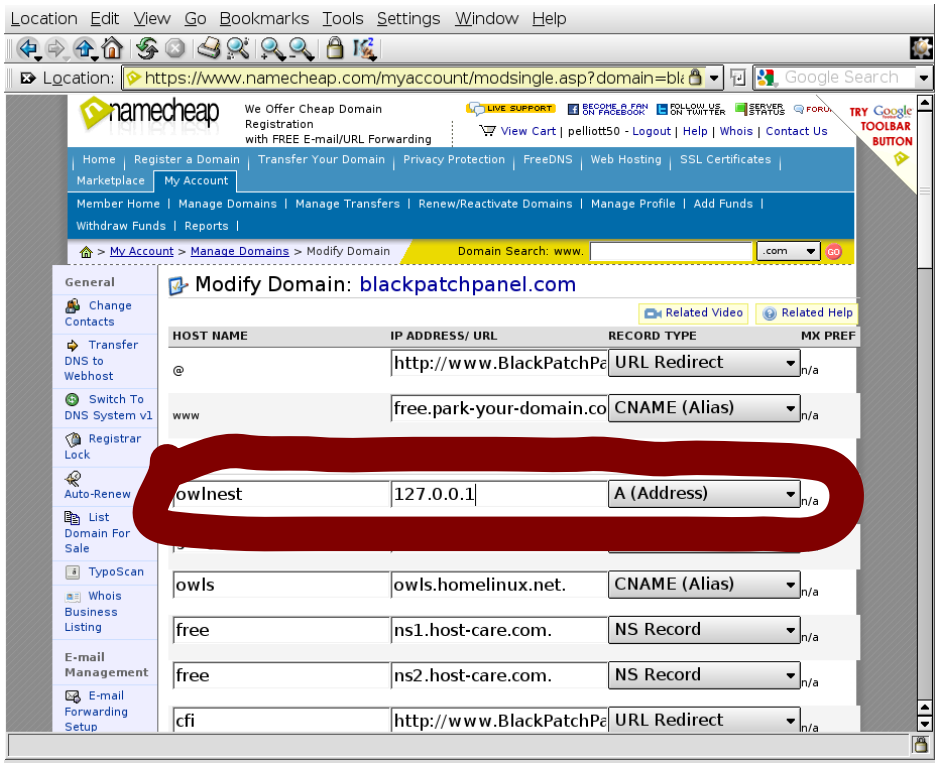
Paul Elliott

Tell the dynamic DNS server to attend to your domain.



- The dynamic DNS server will modify A records.

Create an A record for dynamic DNS to point to your Home computer.

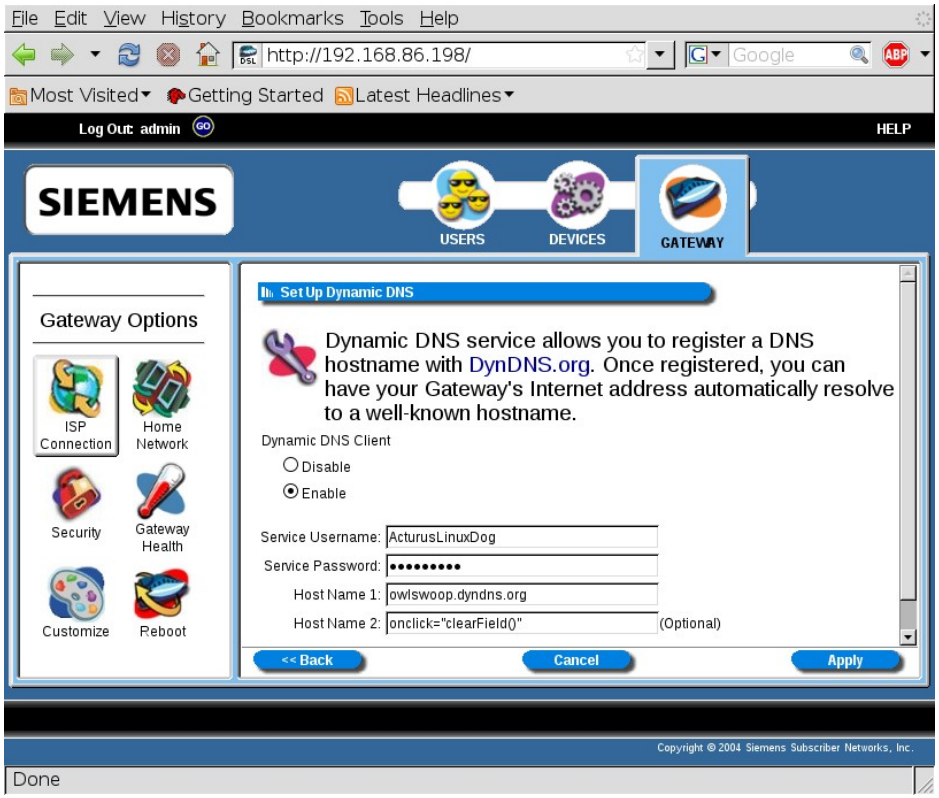


- 127.0.0.1 (local host) is a good initial value.

You do not have to have your own domain to phone home.

- If you get a free account with dyndns.org they will create an host within one of their domains that you can cause to always point to your home computer.
- You can ssh to this host
  - ssh you@yourcomputer.dyndns.org

Tell your router to phone home to your dynamic DNS server.



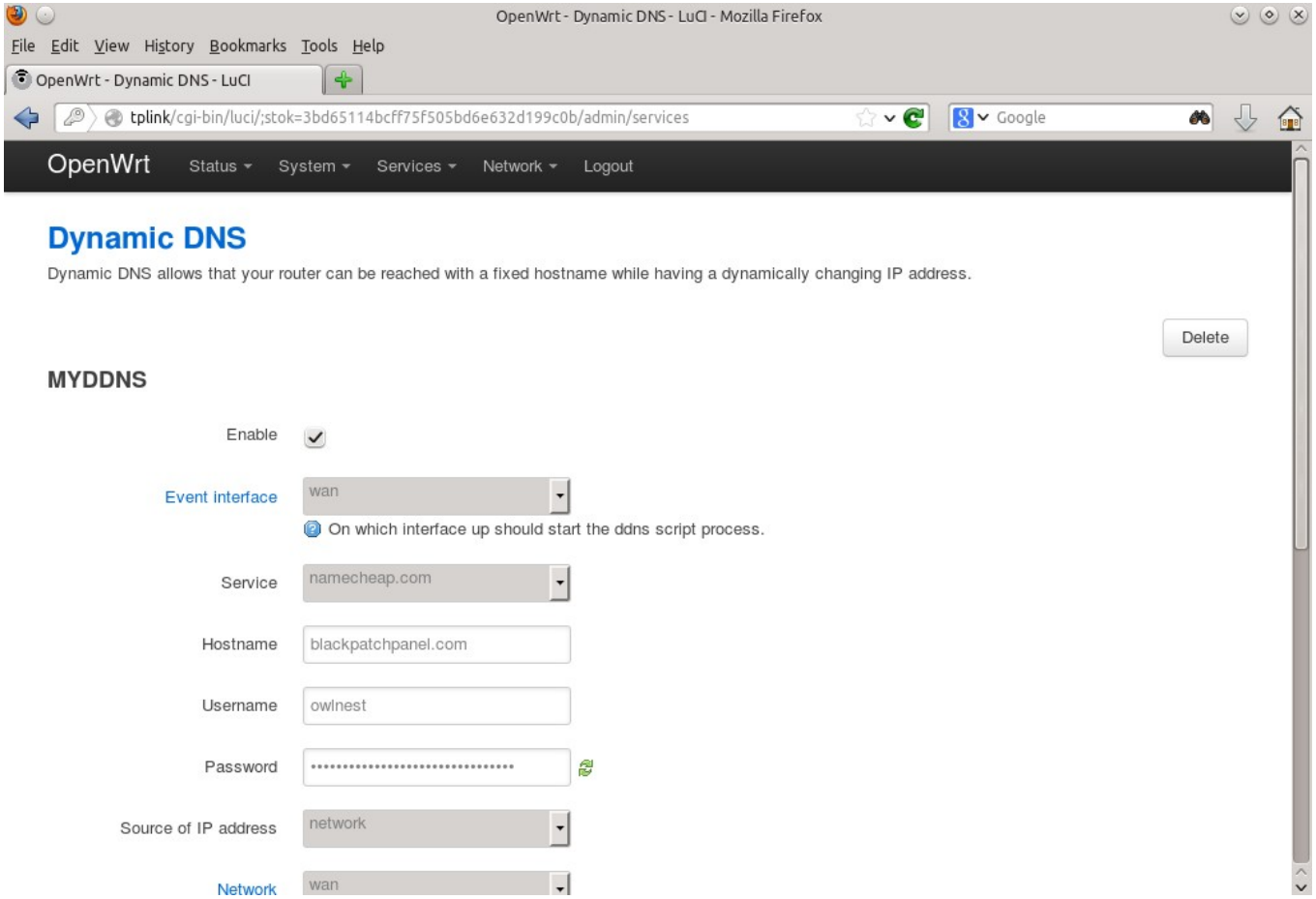
- How you do this depends on your router.
- This is the best way, if it works.
- However some routers don't know how.
- So you need plan B
- a dynamic DNS client.

If you have openwrt you can have your router handle dynamic dns!

OpenWrt
Wireless Freedom

- If you have openwrt have your router do dynamic dns!
- Install luci-app-ddns from “System/Software”

Configure DDNS from LuCI Services



Namecheap.com - Modify Domain (blackpatchpanel.com) – rekonq

https://manage.www.namecheap.com/myaccount/modsingle.asp?domain=blackpatchpanel.com&type=ddns&rkey=NC

Programming | Linux | News politics | personal | Search | Religion | peless | newrng810 | RTC | Comedy | MIDI | Comercial

openwrt luci-app-ddns d... | Working NameCheap DD... | DDNS Client - OpenWrt ... | [ddns] update issue help ... | Namecheap.com - Modif...

Get a personal .ME domain+private email for just $0.98
For a limited time you can get a personal .ME domain name and private email at a deeply discounted rate.Let .ME get you online!

General
- Change Contacts
- Transfer DNS to Webhost
- Switch To DNS System v1
- Registrar Lock
- Auto-Renew
- List Domain For Sale
- TypoScan

Websites
- Onepager Website

E-mail Management
- E-mail Forwarding Setup
- OX Email Hosting

Host Management
- URL Forwarding
- URL Frame Meta Tags
- All Host Records

Advanced Options

Modify Domain: blackpatchpanel.com

Related Help | Rela

ENABLE/ DISABLE DYNAMIC DNS FOR THIS DOMAIN

Current Dynamic DNS Status : **Enabled**

This is your hostname

- (•) Re-enable Dynamic DNS. **Password will be reset to new password.**
- ( ) Disable Dynamic DNS for this domain.

Save Changes

Any “A” record can be modified.

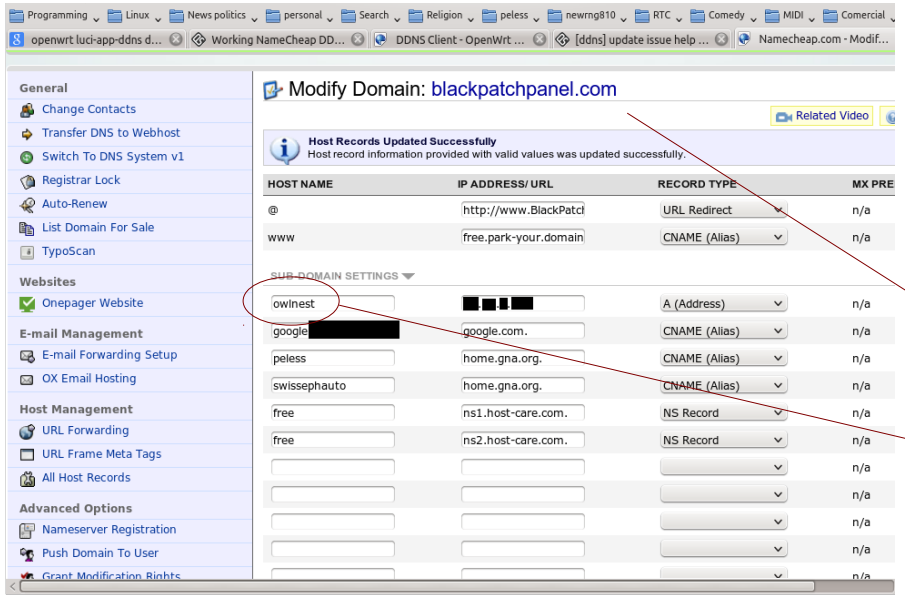
INFORMATION REQUIRED FOR DYNAMIC DNS CLIENT

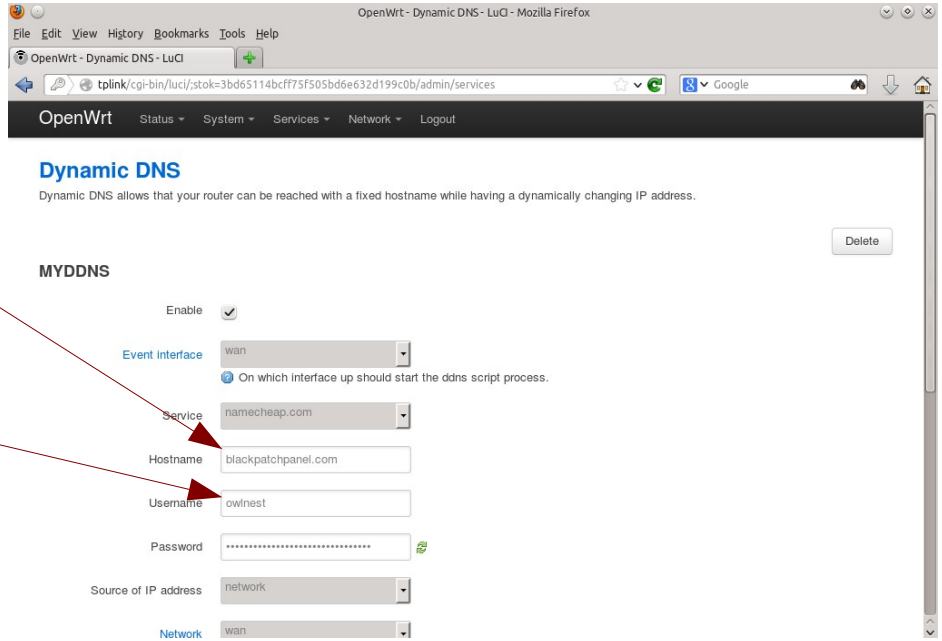
Domain Name	**blackpatchpanel.com**
Host Name	***anyhost_you_specify_in_client***

Please make sure you create an A record for this host name before sending a dynamic dns update command. You can set an A record using the 'All Hosts' page. Use a dummy address if IP not known.
ex: www 127.0.0.1 'A Record'

Password	[redacted]

NameCheap
Hostname and Username





NameCheap
owlnest.blackpatchpanel.com

- Subdomain with “A” record
- My domain

NameCheap
owlnest.blackpatchpanel.com

- Goes in openwrt “Username” field.
- Goes in openwrt “Domain” field.

OpenWrt - Dynamic DNS - LuCI - Mozilla Firefox

File Edit View History Bookmarks Tools Help

OpenWrt - Dynamic DNS - LuCI

tplink/cgi-bin/luci/;stok=3bd65114bcff75f505bd6e632d199c0b/admin/services

Google

OpenWrt Status System Services Network Logout

Dynamic DNS

Dynamic DNS allows that your router can be reached with a fixed hostname while having a dynamically changing IP address.

Delete

MYDDNS

Enable ☑

Event interface: wan

On which interface up should start the ddns script process.

Service: namecheap.com

Hostname: blackpatchpanel.com

Username: owlnest

Password: ••••••••••••••••••••••••••••••

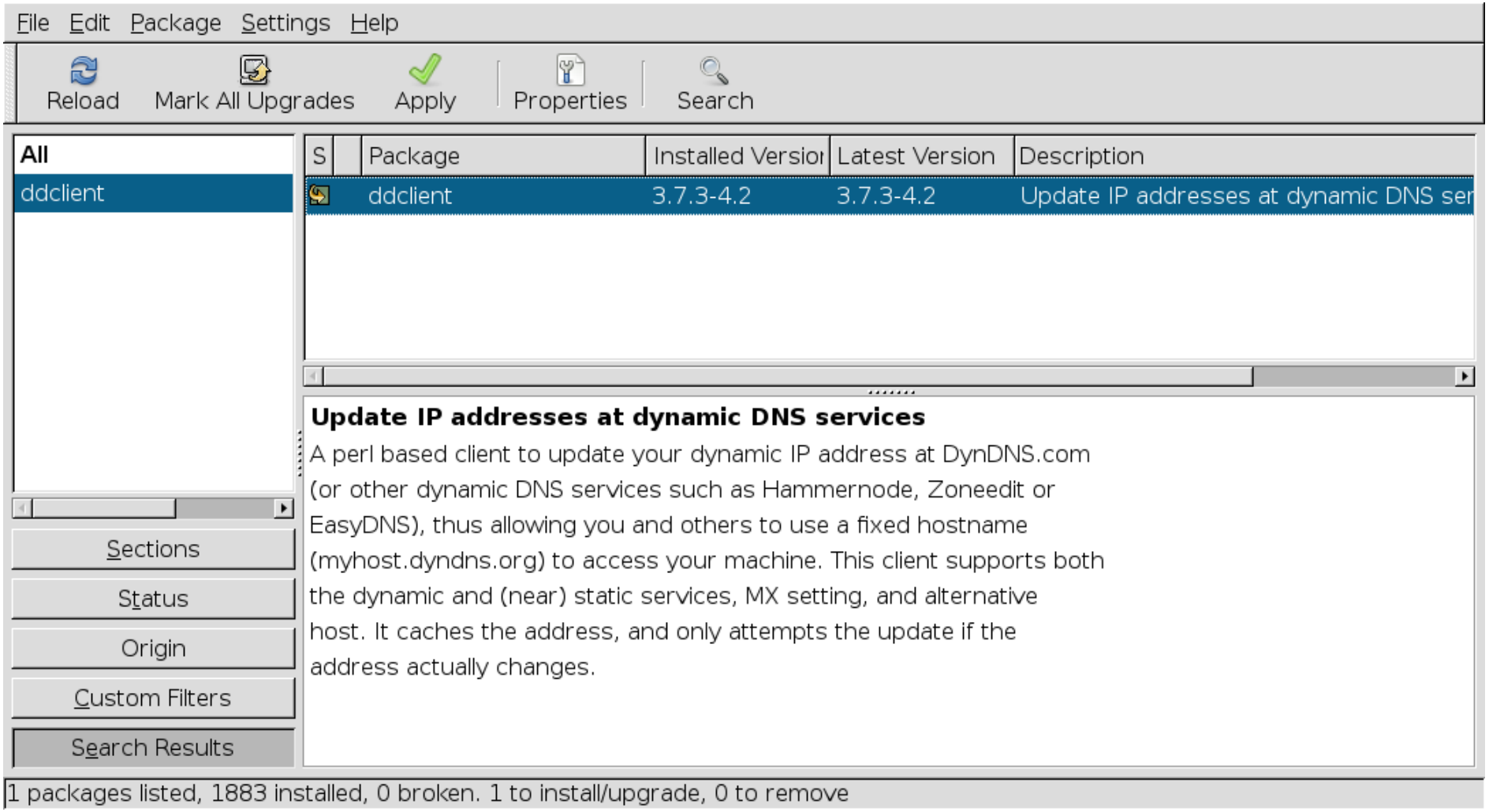
Source of IP address: network

Network: wan

If your router will not cooperate

- Then you must get your linux computer to update dynamic dns.
- Read on.

Install ddclient on your linux machine



Are you running dhclient or dhcpcd?

```
$ ps -A|grep -i dh
 3222 ?        00:00:00 dhcdbd
 3426 ?        00:00:00 dhclient
```

Edit /etc/ddclient.conf

- Start with
  - /usr/share/doc/ddclient/examples/sample-etc_ddclient.conf
- Includes most common ddclient options

```
daemon=300                    # check every 300 seconds
syslog=yes                    # log update msgs to syslog
mail=root                     # mail all msgs to root
mail-failure=root             # mail failed update msgs to root
pid=/var/run/ddclient.pid     # record PID in file.
ssl=yes                       # use ssl-support.  Works with
```

Edit /etc/ddclient.conf

- Start with
  - /usr/share/doc/ddclient/examples/sample-etc_ddclient.conf
- Includes “use” line for getting external IP address from most common routers. Simply uncomment router you have!

```
#use=watchguard-soho,        fw=192.168.111.1:80        # via Watchguard's SOHO FW
#use=netopia-r910,           fw=192.168.111.1:80        # via Netopia R910 FW
#use=smc-barricade,          fw=192.168.123.254:80      # via SMC's Barricade FW
#use=netgear-rt3xx,          fw=192.168.0.1:80          # via Netgear's internet FW
#use=linksys,                fw=192.168.1.1:80          # via Linksys's internet FW
#use=maxgate-ugate3x00,      fw=192.168.0.1:80          # via MaxGate's UGATE-3x00  FW
#use=elsa-lancom-dsl10,      fw=10.0.0.254:80           # via ELSA LanCom DSL/10 DSL Router
#use=elsa-lancom-dsl10-ch01, fw=10.0.0.254:80           # via ELSA LanCom DSL/10 DSL Router
#use=elsa-lancom-dsl10-ch02, fw=10.0.0.254:80           # via ELSA LanCom DSL/10 DSL Router
#use=alcatel-stp,            fw=10.0.0.138:80           # via Alcatel Speed Touch Pro
#use=xsense-aero,            fw=192.168.1.1:80          # via Xsense Aero Router
#use=allnet-1298,            fw=192.168.1.1:80          # via AllNet 1298 DSL Router
#use=3com-oc-remote812,      fw=192.168.0.254:80        # via 3com OfficeConnect Remote 812
#use=e-tech,                 fw=192.168.1.1:80          # via E-tech Router
#use=cayman-3220h,           fw=192.168.0.1:1080        # via Cayman 3220-H DSL Router
```

Edit /etc/ddclient.conf

- Start with
  - /usr/share/doc/ddclient/examples/sample-etc_ddclient.conf
- Includes server options for most dynamic dns hosts. Simply uncomment lines add your host name and password!

```
##
## dyndns.org dynamic addresses
##
## (supports variables: wildcard,mx,backupmx)
##
# server=members.dyndns.org,
# protocol=dyndns2
# your-dynamic-host.dyndns.org
#login=your-login                # default login
#password=test                   # default password
#mx=mx.for.your.host             # default MX
#backupmx=yes|no                 # host is primary MX?
#wildcard=yes|no                 # add wildcard CNAME?
```

- Your complete dns hostname goes here.
- Login
- password

Edit /etc/ddclient.conf

```
daemon=300                  # check every 300 seconds
syslog=yes                  # log update msgs to syslog
mail-failure=root           # mail failed update msgs to root
pid=/var/run/ddclient.pid         # record PID in file.
ssl=yes                     # use ssl-support.  Works with


use=fw, fw=192.168.86.198/mymodem_summary.htm, fw-skip='internet_options.htm><U>'


#
# NameCheap (namecheap.com)
#
protocol=namecheap,                     \
server=dynamicdns.park-your-domain.com,   \
login=blackpatchpanel.com,                  \
password=XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX             \
owlnest
```

Edit /etc/ddclient.conf

```
daemon=300                  # check every 300 seconds
syslog=yes                  # log update msgs to syslog
mail-failure=root           # mail failed update msgs to root
pid=/var/run/ddclient.pid         # record PID in file.
ssl=yes                     # use ssl-support.  Works with


use=fw, fw=192.168.86.198/mymodem_summary.htm, fw-skip='internet_options.htm><U>'


#
# NameCheap (namecheap.com)
#
protocol=namecheap,                     \
server=dynamicdns.park-your-domain.com,   \
login=blackpatchpanel.com,                  \
password=XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX            \
owlnest
```

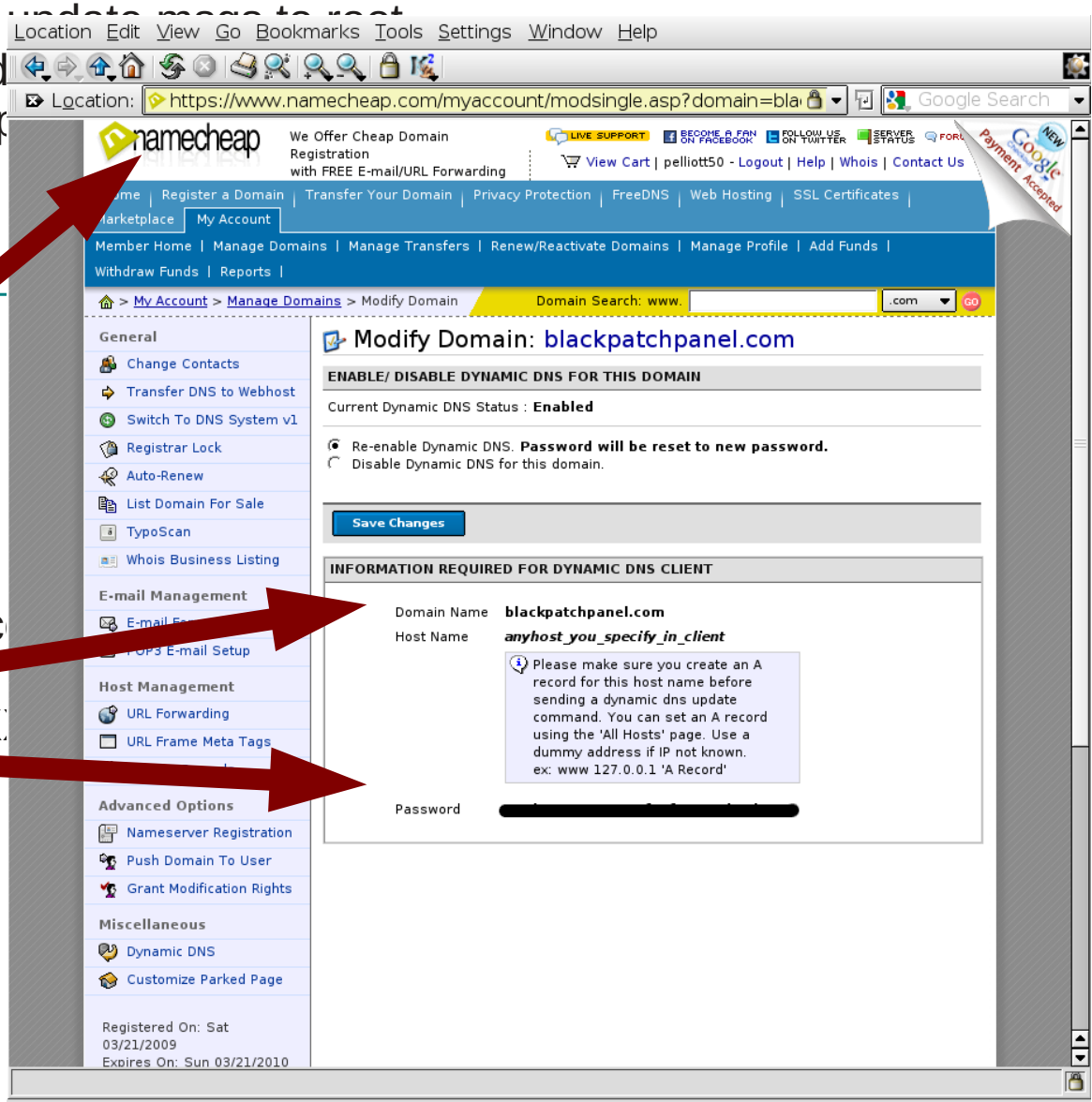
- Needed only if you need to run as a daemon
- i.e. not running dhclient or dhcpcd

Edit /etc/ddclient.conf

```
daemon=300                  # check every 300 seconds
syslog=yes                  # log update msgs to syslog
mail-failure=root           # mail failed update msgs to root
pid=/var/run/ddclient.pid       # record
ssl=yes                     # use ssl-sup
```

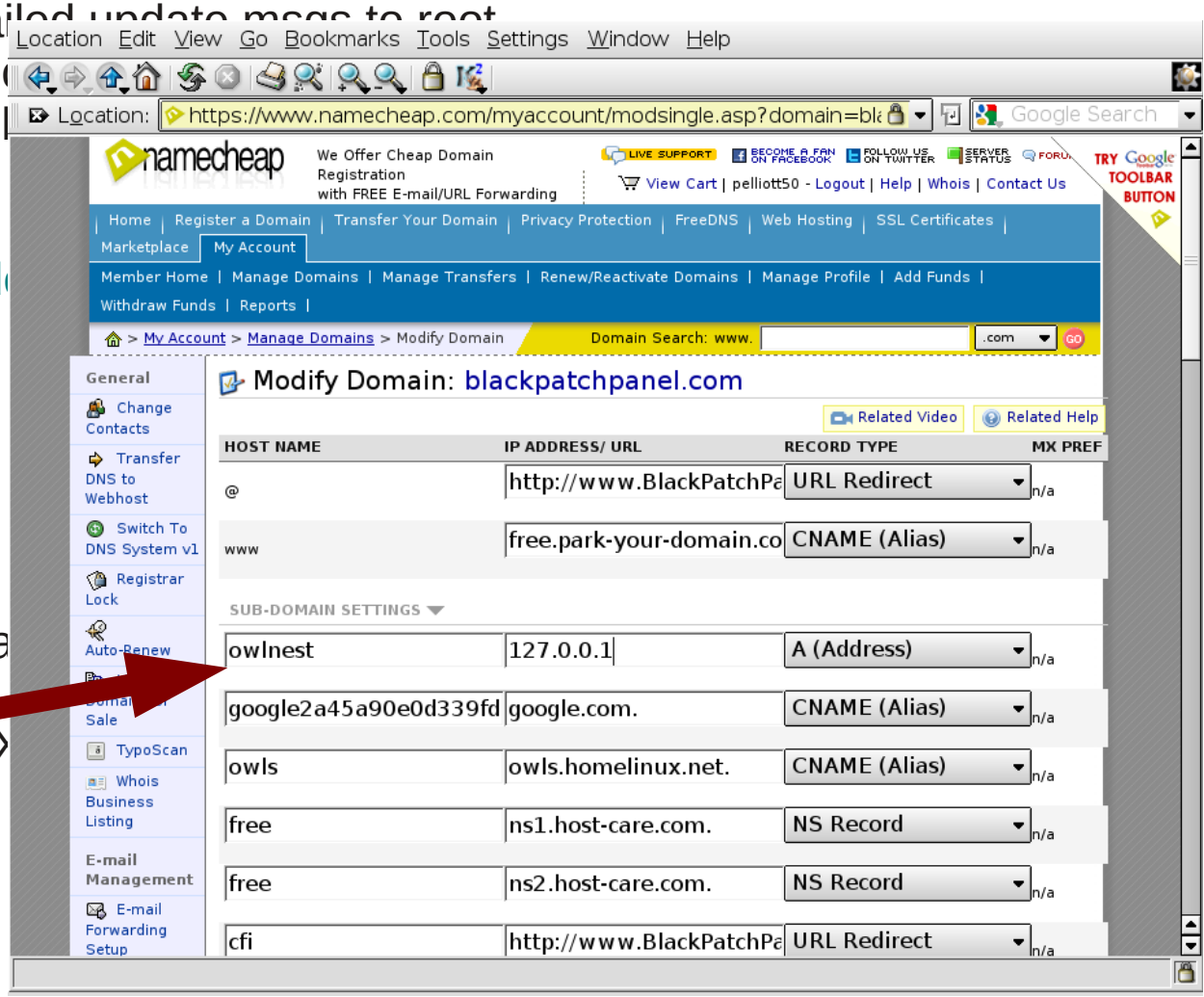
use=fw, fw=192.168.86.198/mymodem_

```
#
# NameCheap (namecheap.com)
#
protocol=namecheap,                 \
server=dynamicdns.park-your-domain.c
login=blackpatchpanel.com,
password=XXXXXXXXXXXXXXXXXXX
owlnest
```



Edit /etc/ddclient.conf

```
daemon=300                  # check every 300 seconds
syslog=yes                  # log update msgs to syslog
mail-failure=root           # mail failed update msgs to root
pid=/var/run/ddclient.pid       # re
ssl=yes                     # use ssl

use=fw, fw=192.168.86.198/mymod

#
# NameCheap (namecheap.com)
#
protocol=namecheap,
server=dynamicdns.park-your-doma
login=blackpatchpanel.com,
password=XXXXXXXXXXXXXXXX
owlnest
```



Running dhcpcd?

```
cp /usr/share/doc/ddclient/examples/sample-etc_dhcpc_dhcpcd-eth0.exe   \
    /etc/dhcpc/dhcpcd-{your ethernet interface}.exe
```

- See ddclient documentation.

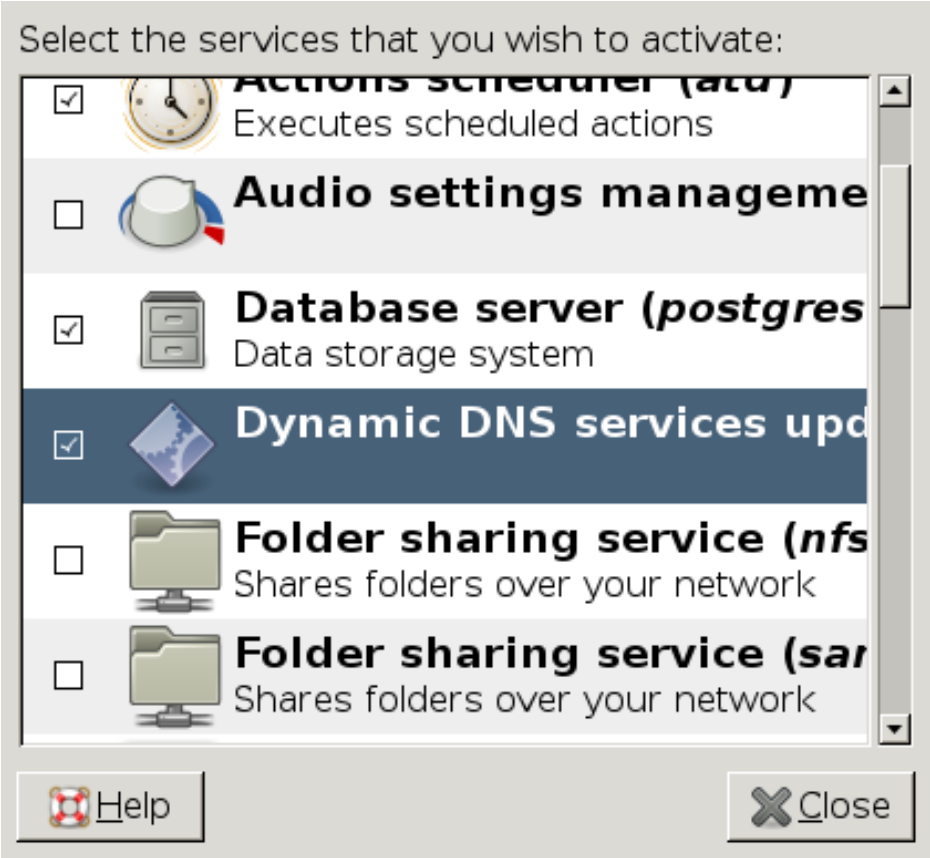
```
#!/bin/sh
##############################################################################
## $Id: sample-etc_dhcpc_dhcpcd-eth0.exe 8 2006-06-14 19:51:39Z wimpunk $
##############################################################################
PATH=/usr/sbin:${PATH}

## update the DNS server unless the IP address is a private address
## that may be used as an internal LAN address. This may be true if
## other interfaces are assigned private addresses from internal
## DHCP server.

case "$1" in
10.*)           ;;
172.1[6-9].* | 172.2[0-9].* | 172.3[0-1].*)     ;;
192.168.*)      ;;
*)
        logger -t dhcpcd IP address changed to $1
        ddclient -daemon=0 -syslog -use=ip -ip=$1 >/dev/null 2>&1
        ;;
esac
```

If you are running dhclient?

```
$ ps -C dhclient
  PID TTY          TIME CMD
 2833 ?        00:00:00 dhclient
```

- cp /usr/share/doc/ddclient/examples/sample-etc_dhclient-exit-hooks /etc/dhclient-exit-hooks

Otherwise... Run ddclient as a daemon

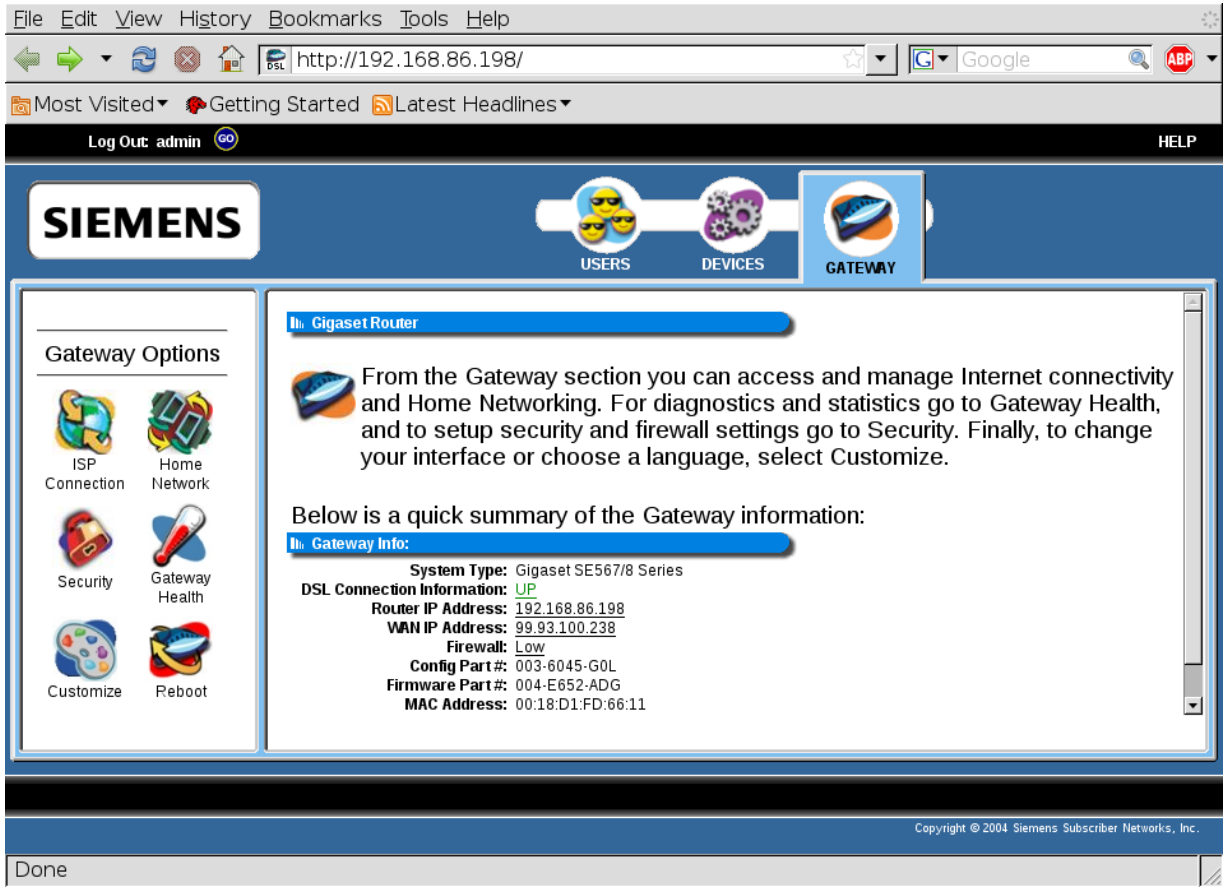


Daemon talks to router to get external IP address.

```
#use=watchguard-soho,        fw=192.168.111.1:80        # via Watchguard's SOHO FW
#use=netopia-r910,           fw=192.168.111.1:80        # via Netopia R910 FW
#use=smc-barricade,          fw=192.168.123.254:80      # via SMC's Barricade FW
#use=netgear-rt3xx,          fw=192.168.0.1:80          # via Netgear's internet FW
#use=linksys,                fw=192.168.1.1:80          # via Linksys's internet FW
#use=maxgate-ugate3x00,      fw=192.168.0.1:80          # via MaxGate's UGATE-3x00  FW
#use=elsa-lancom-dsl10,      fw=10.0.0.254:80           # via ELSA LanCom DSL/10 DSL Router
#use=elsa-lancom-dsl10-ch01, fw=10.0.0.254:80           # via ELSA LanCom DSL/10 DSL Router
#use=elsa-lancom-dsl10-ch02, fw=10.0.0.254:80           # via ELSA LanCom DSL/10 DSL Router
#use=alcatel-stp,            fw=10.0.0.138:80           # via Alcatel Speed Touch Pro
#use=xsense-aero,            fw=192.168.1.1:80          # via Xsense Aero Router
#use=allnet-1298,            fw=192.168.1.1:80          # via AllNet 1298 DSL Router
#use=3com-oc-remote812,      fw=192.168.0.254:80        # via 3com OfficeConnect Remote 812
#use=e-tech,                 fw=192.168.1.1:80          # via E-tech Router
#use=cayman-3220h,           fw=192.168.0.1:1080        # via Cayman 3220-H DSL Router
```

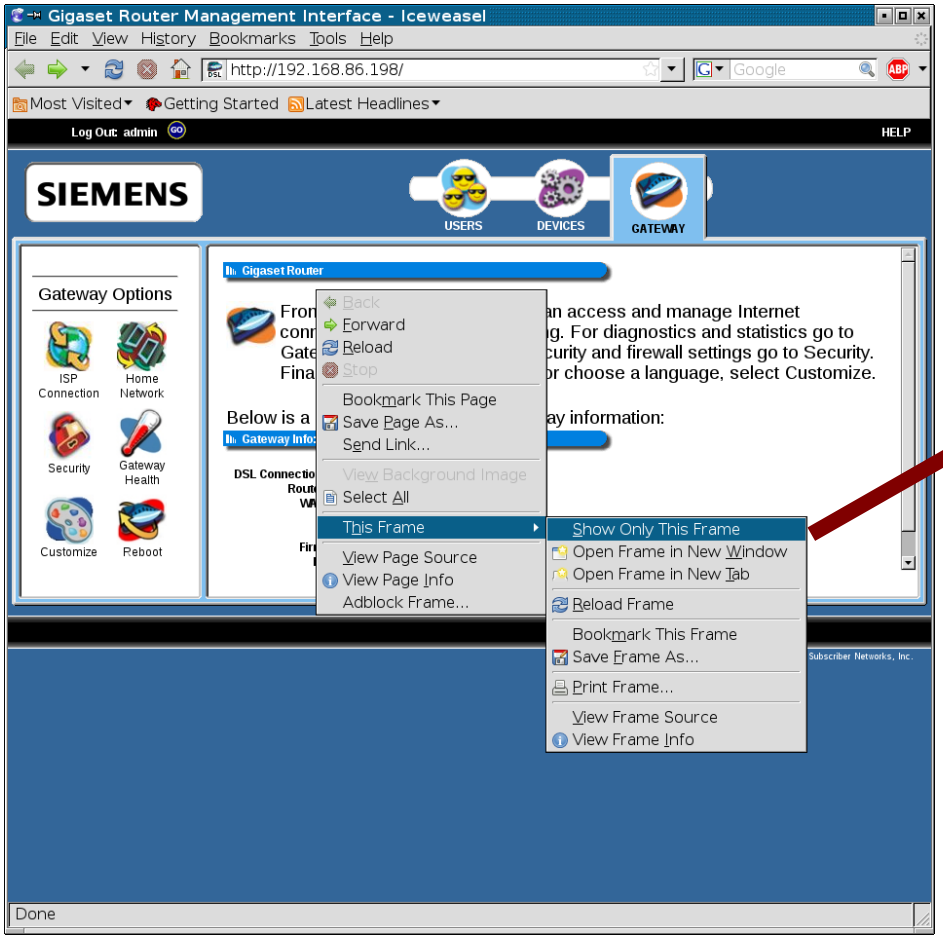
- Common routers have built in support.
- Just uncomment correct “use” line in the sample ddclient.conf file.

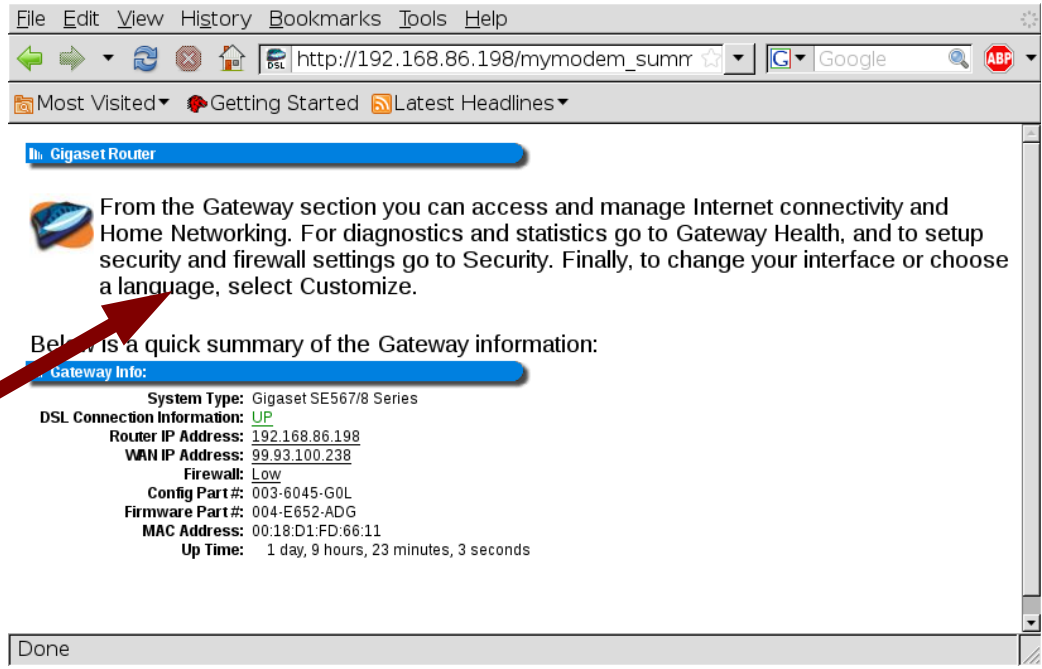
If your router is unsupported Web Scrape



- Find the page in your router's web pages that displays the external IP address.

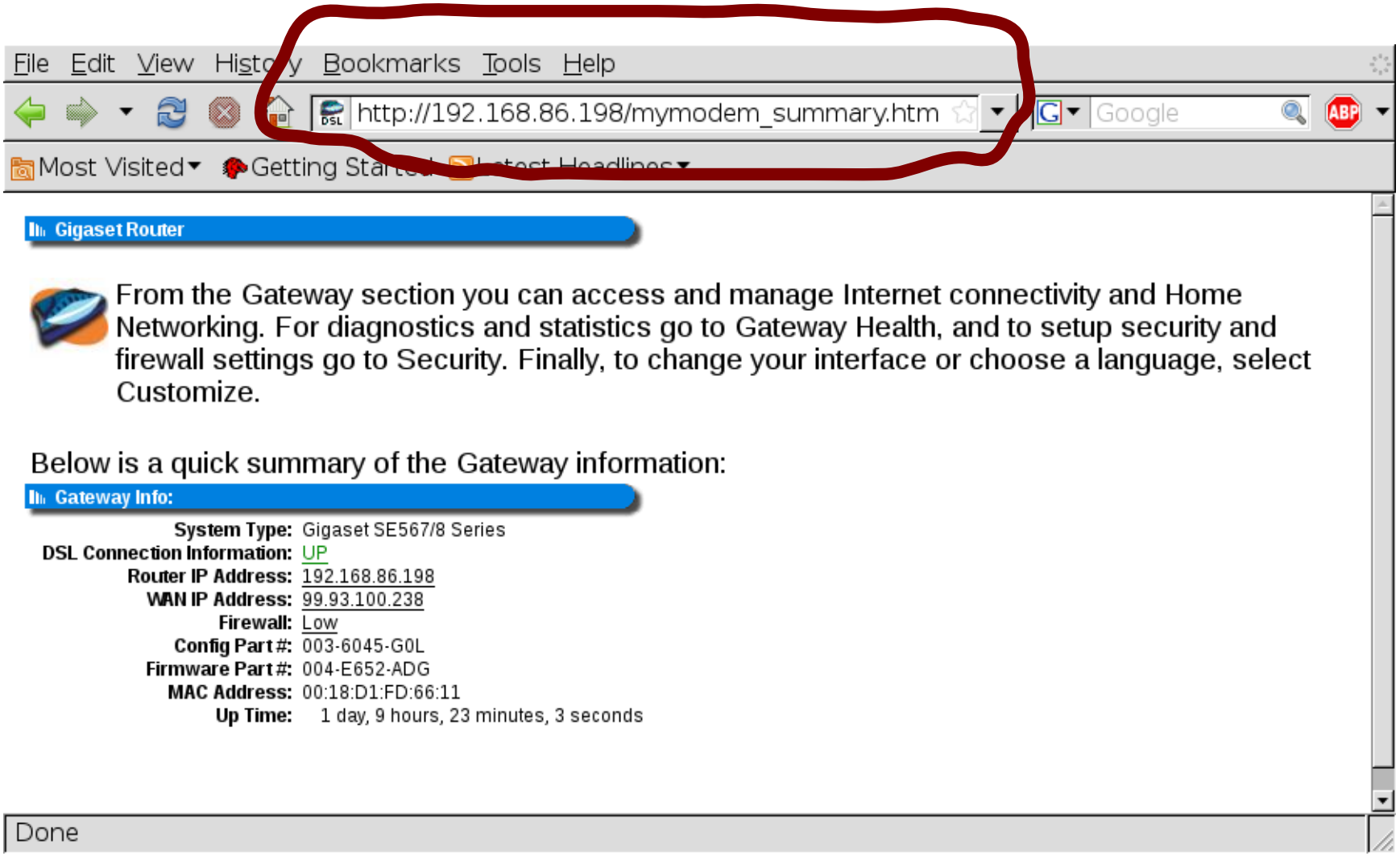
Isolate the frame containing the external IP address.





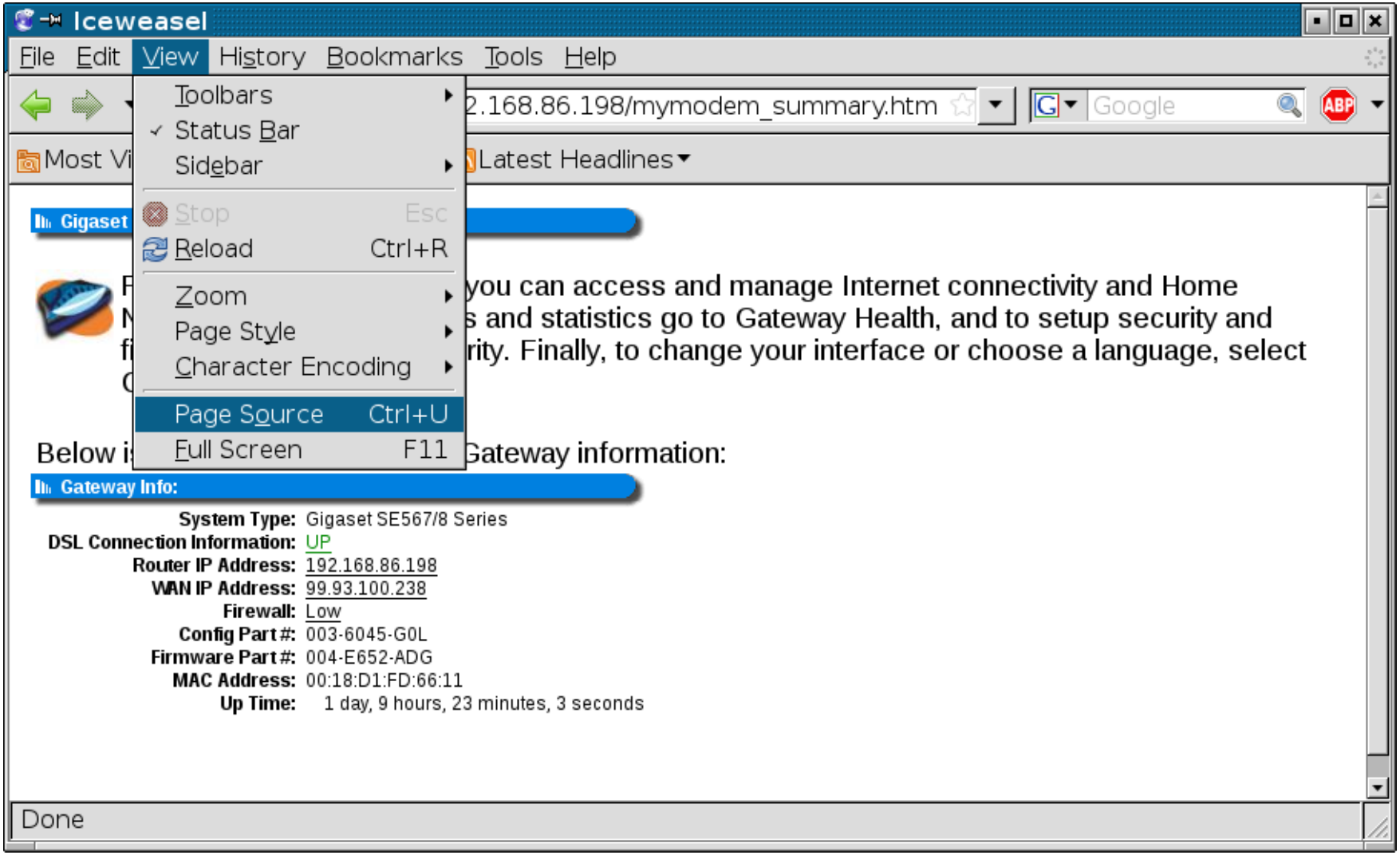
- Right click on the frame; Show only this Frame

Note the URL.



- We will use the url to create a “use” line.

View the source for the page



Search of external IP address in the source!

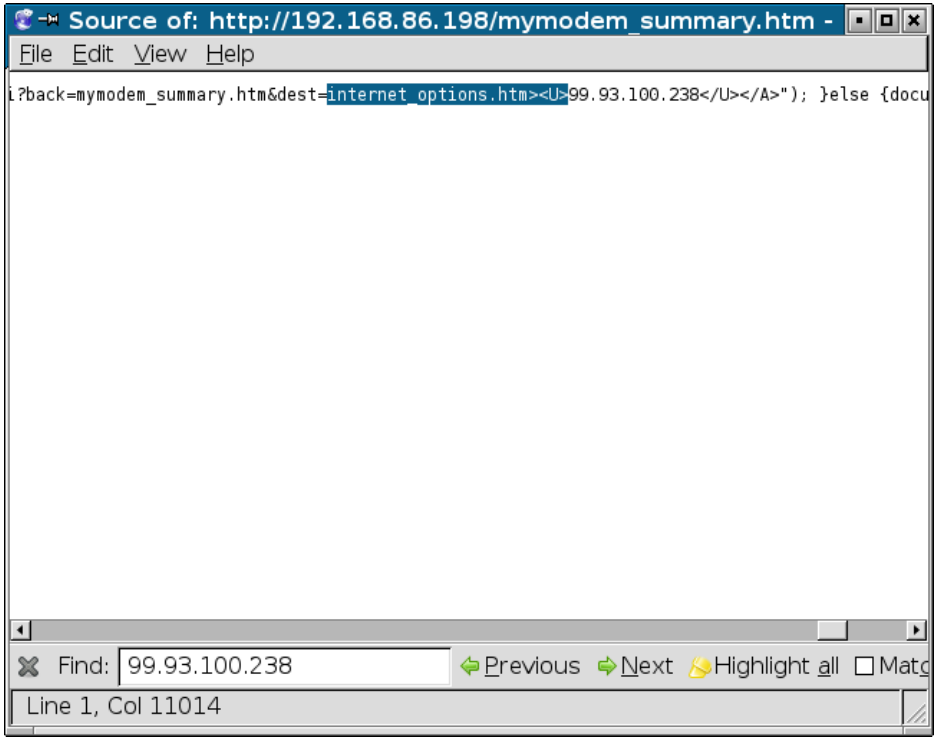
File Edit View Help

```
i?back=mymodem_summary.htm&dest=internet_options.htm><U>99.93.100.238</U></A>"); }else {docu
```

Find: 99.93.100.238 Previous Next Highlight all Matc

Line 1, Col 11027

Locate unique prefix



- Locate a prefix that uniquely precedes the external IP address in the source html.
- If necessary, use regular expressions.

Construct a “use” line.

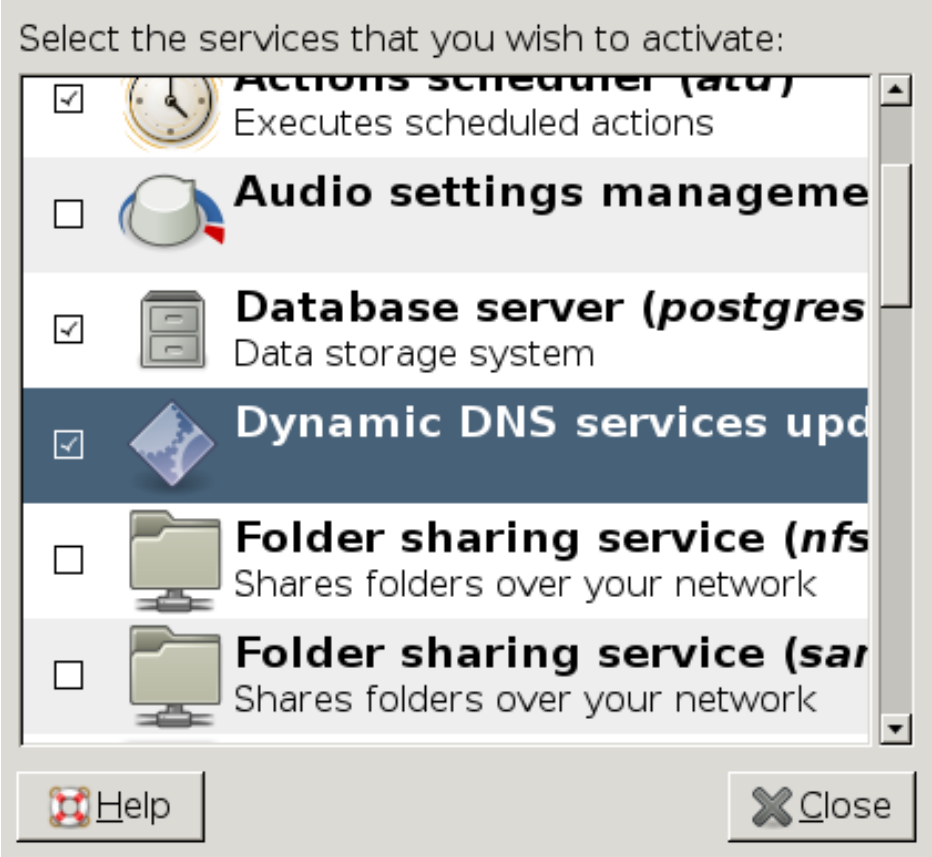
use=fw, fw=192.168.86.198/mymodem_summary.htm, fw-skip='internet_options.htm><U>'

- Construct a use line from the two pieces of data we have gathered.
  - The URL.
  - The Prefix string
- Put use line in /etc/ddclient.conf

Edit /etc/ddclient.conf

```
daemon=300                  # check every 300 seconds
syslog=yes                  # log update msgs to syslog
mail-failure=root           # mail failed update msgs to root
pid=/var/run/ddclient.pid         # record PID in file.
ssl=yes                     # use ssl-support.  Works with


use=fw, fw=192.168.86.198/mymodem_summary.htm, fw-skip='internet_options.htm><U>'


#
# NameCheap (namecheap.com)
#
protocol=namecheap,                     \
server=dynamicdns.park-your-domain.com,   \
login=blackpatchpanel.com,                  \
password=XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX             \
owlnest
```

Run ddclient as a daemon



- Done configuring ddclient

Remember how I told you if you had dhclient or dhcpcd you did not have to run ddclient?

- You could read the ddclient doc and find out a file you could copy to run ddclient when you received a new dhcp lease?
- On my debian lenny distro it, (the method specified in the ddclient docs,) which I told you about earlier in this presentation, did not work!

What worked.

```
#!/bin/sh

/usr/sbin/ddclient -daemon=0 -syslog  -use=fw -fw "192.168.86.198/mymodem_summary.htm" -fw-skip 'internet_options.htm><U>' >/dev/null 2>&1
```

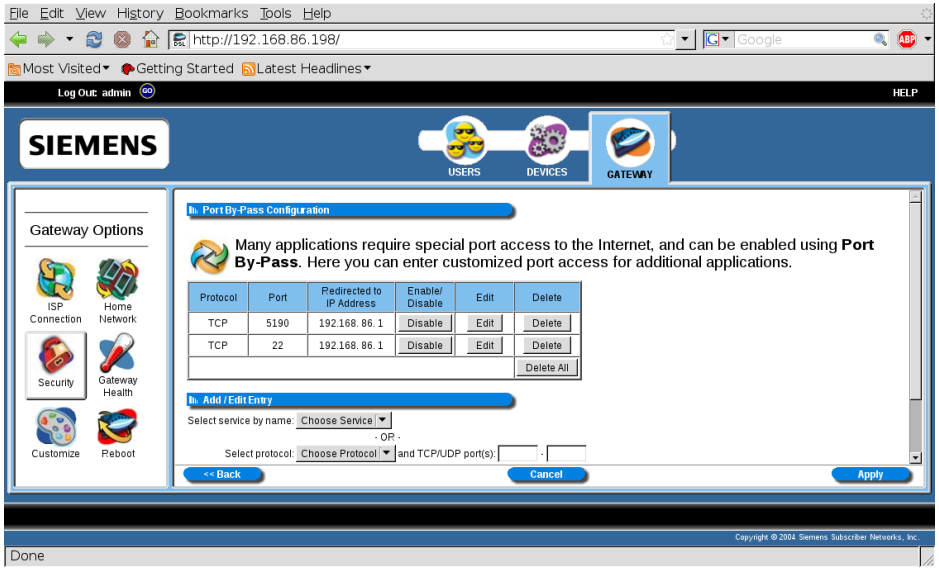
- Added the following file to
  - /etc/dhcp3/dhclient-exit-hooks.d/ddclient-hook
- Highlighted portions are from my use line. You will need to find them by web scraping your router as previously described.

Test that host record points to correct place.

```
$ dig owlnest.blackpatchpanel.com

; <<>> DiG 9.5.1-P3 <<>> owlnest.blackpatchpanel.com
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49840
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;owlnest.blackpatchpanel.com.   IN      A

;; ANSWER SECTION:
owlnest.blackpatchpanel.com. 1800 IN    A       99.93.100.238

;; Query time: 106 msec
;; SERVER: 192.168.86.198#53(192.168.86.198)
;; WHEN: Sun Jan 24 13:15:47 2010
;; MSG SIZE  rcvd: 61

$
```

- Repeat that test still works after you get a new DHCP lease!

Tell your router how to route incoming connection requests.



- How to do this depend on your router.
- Port 22 is used by ssh
- what should your router do with an incoming connection request on port 22?

Configure the ssh daemon's security.

- Under root, edit
  - /etc/ssh/sshd_config
-

Limit sshd access to users with known strong security.

AllowUsers pelliott

- Your “distro” will often add accounts that you don't even know about.
- Just because you let someone have an account on your computer, does not mean you want to let them have remote access.
- Most people's security practices are horrible.
- It is nice to limit remote access to a known finite list.

Consider disabling password access altogether!

PasswordAuthentication no

- Berlios developer web site was attacked recently using man-in-the-middle attack using passwords.

Disable protocol 1

Protocol 2

- Protocol 1 is old.

If you want to run remote X11 programs, you will have to enable X11Forwarding

X11Forwarding yes

- Most security concerns concerning X11 Forwarding are for the X server i.e. where the mouse and the display is.

TCP wrappers may prevent sshd from accepting incoming connections!

/etc/hosts.deny
ALL : ALL EXCEPT LOCAL,localhost

- Most distro's versions of ssh link to tcp wrappers.
- This means they will not allow incoming connections if tcp wrappers is not configured properly.
- It is a good idea to tell tcp wrappers to disallow everything not explicitly permitted.

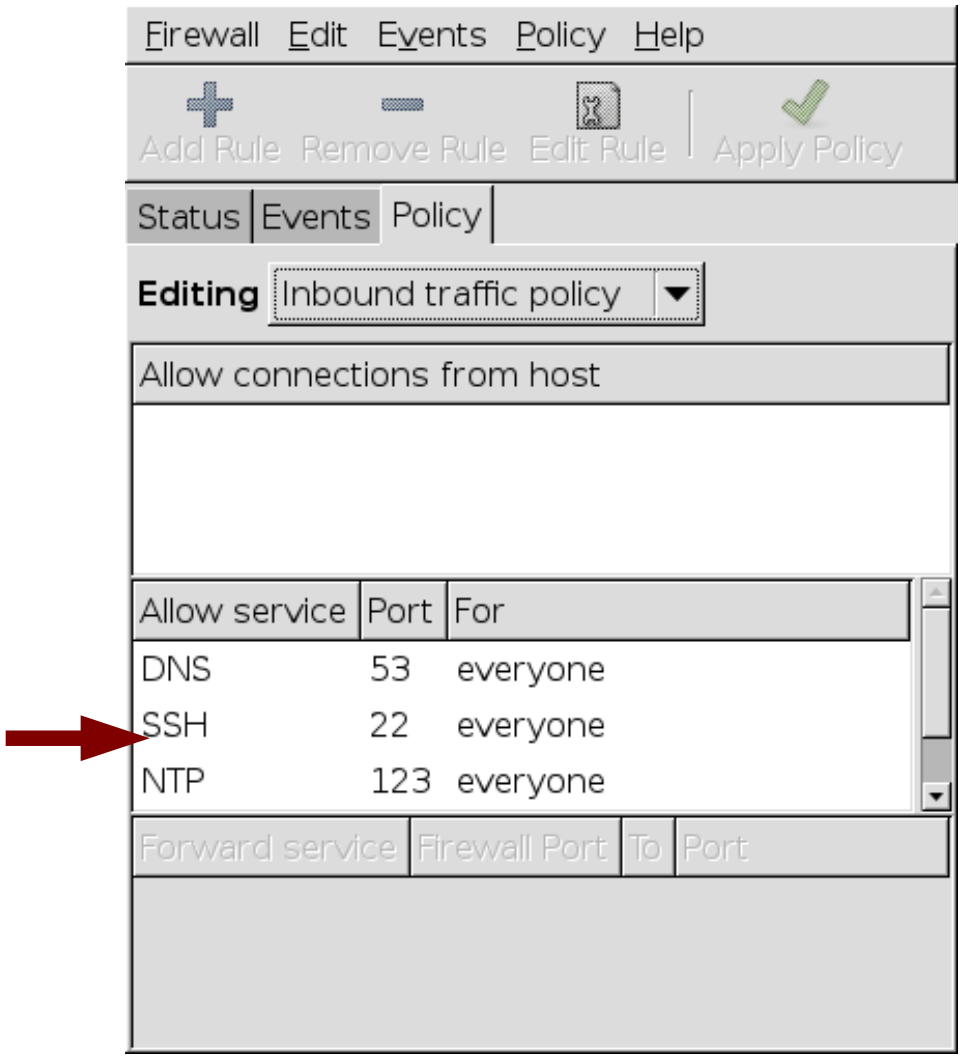
Explicitly allow sshd to connect.

/etc/hosts.allow

```
portmap: 192.168.86.0/255.255.255.0
statd:  192.168.86.0/255.255.255.0
sshd: ALL : ALLOW
```

- Modify /etc/hosts.allow to allow sshd to talk to the outside world.

Pierce your firewall to allow incoming connections



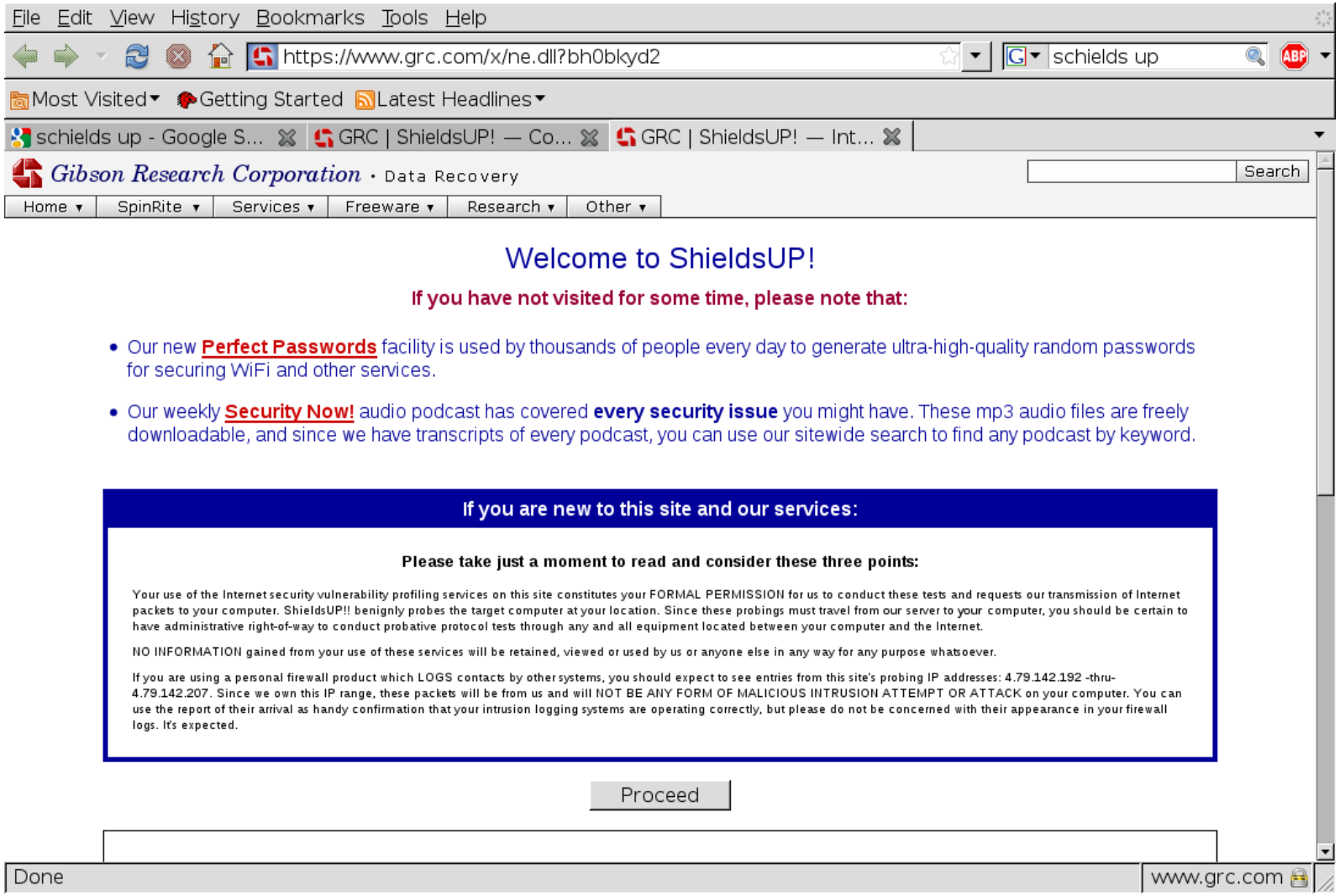
- How you do this depends on your firewall management software.
- I use “firestarter”

Restart the ssh daemon

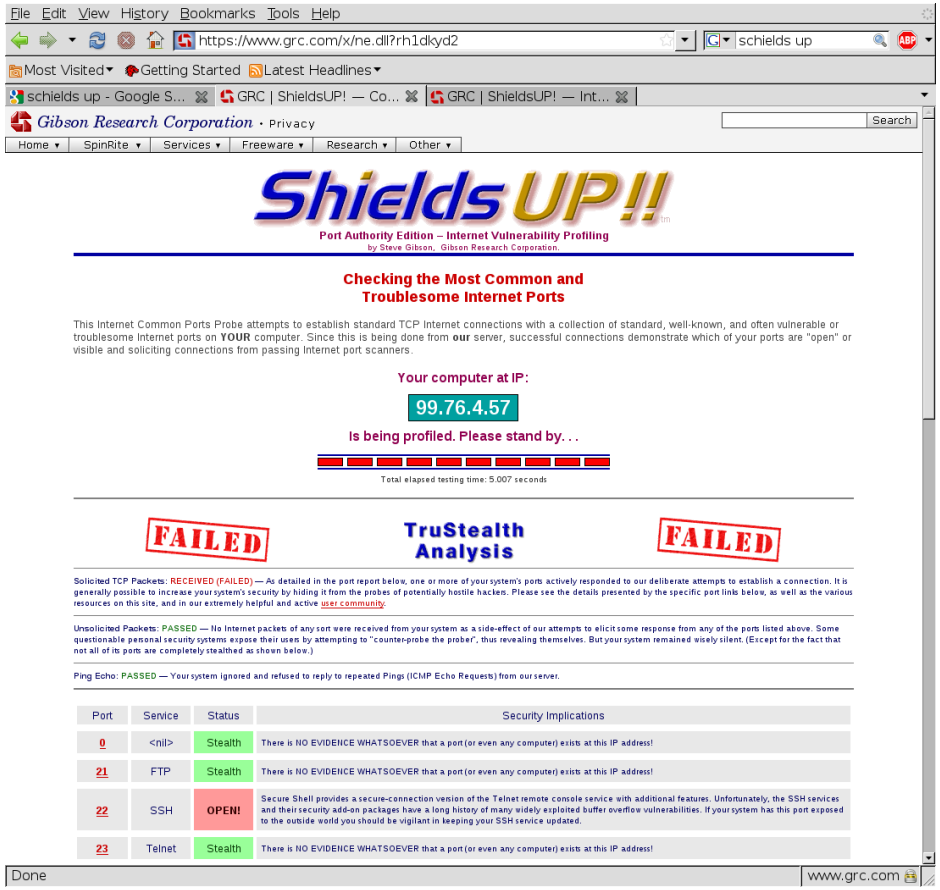
```
# /etc/init.d/ssh restart
```

- After changing security parameters, you will need to restart the daemon.

Go to ShieldsUP to verify we have and open port!



Go to ShieldsUP to verify we have and open port!



- No Open port, no possibility of remote access!

Make sure your passwords are strong because they will try to get in!

```
hrnowl:/var/log# grep ssh auth.log |grep root
Feb  2 15:31:40 hrnowl sshd[5205]: User root from 211.92.149.147 not allowed because not listed in AllowUsers
Feb  2 15:31:42 hrnowl sshd[5207]: User root from 211.92.149.147 not allowed because not listed in AllowUsers
Feb  2 15:31:44 hrnowl sshd[5209]: User root from 211.92.149.147 not allowed because not listed in AllowUsers
Feb  2 15:31:46 hrnowl sshd[5211]: User root from 211.92.149.147 not allowed because not listed in AllowUsers
Feb  2 15:31:48 hrnowl sshd[5213]: User root from 211.92.149.147 not allowed because not listed in AllowUsers
Feb  2 15:31:50 hrnowl sshd[5215]: User root from 211.92.149.147 not allowed because not listed in AllowUsers
Feb  2 15:31:52 hrnowl sshd[5217]: User root from 211.92.149.147 not allowed because not listed in AllowUsers
Feb  2 15:31:54 hrnowl sshd[5219]: User root from 211.92.149.147 not allowed because not listed in AllowUsers
Feb  2 15:31:56 hrnowl sshd[5221]: User root from 211.92.149.147 not allowed because not listed in AllowUsers
Feb  2 15:31:59 hrnowl sshd[5223]: User root from 211.92.149.147 not allowed because not listed in AllowUsers
Feb  2 15:32:01 hrnowl sshd[5225]: User root from 211.92.149.147 not allowed because not listed in AllowUsers
Feb  2 16:29:29 hrnowl sshd[5658]: User root from 219.93.76.50 not allowed because not listed in AllowUsers
hrnowl:/var/log#
```

- Excerpt from my system log show hackers trying to get in!

Generate a ssh public private key pair (if you have not already)

- Use ssh-keygen to generate the keys. On your mobile computer
- Distribute the public key to the remote computer. That is your home computer.
  - To the ~/.ssh directories of the accounts that will phone home.
- If you have disabled password access, you won't be able to use ssh itself to do this.
- Append the public key to ~/.ssh/authorized_keys of the account that will be used at home.
- ssh-copy-id -i ~/.ssh/yourkey.pub user@remote.host

If you have disabled passwords you will have to use sneakernet for distribution

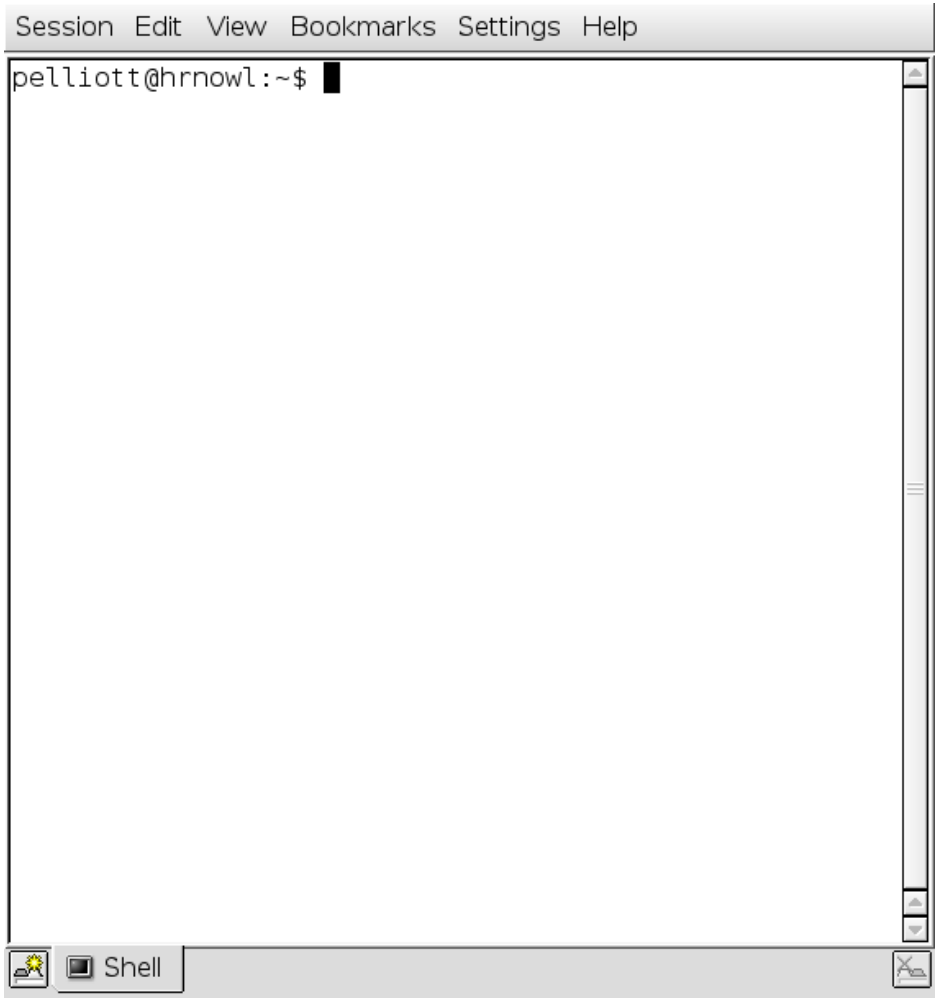
- ssh-copy-id -i ~/.ssh/yourkey.pub user@remote.host
  - If you have disabled password access this will not work!
  - Copy the file via sneaker net and a usb stick
  - On your mobile computer
    - Cp mykey.pub /media/usbstick/mykey.pub
  - On your home computer
    - cat /media/usbstick/mykey.pub \ >>~/.ssh/authorized_keys

You are now ready to phone home.

```
ssh -X pelliott@owlnest.blackpatchpanel.com /usr/bin/konsole
```

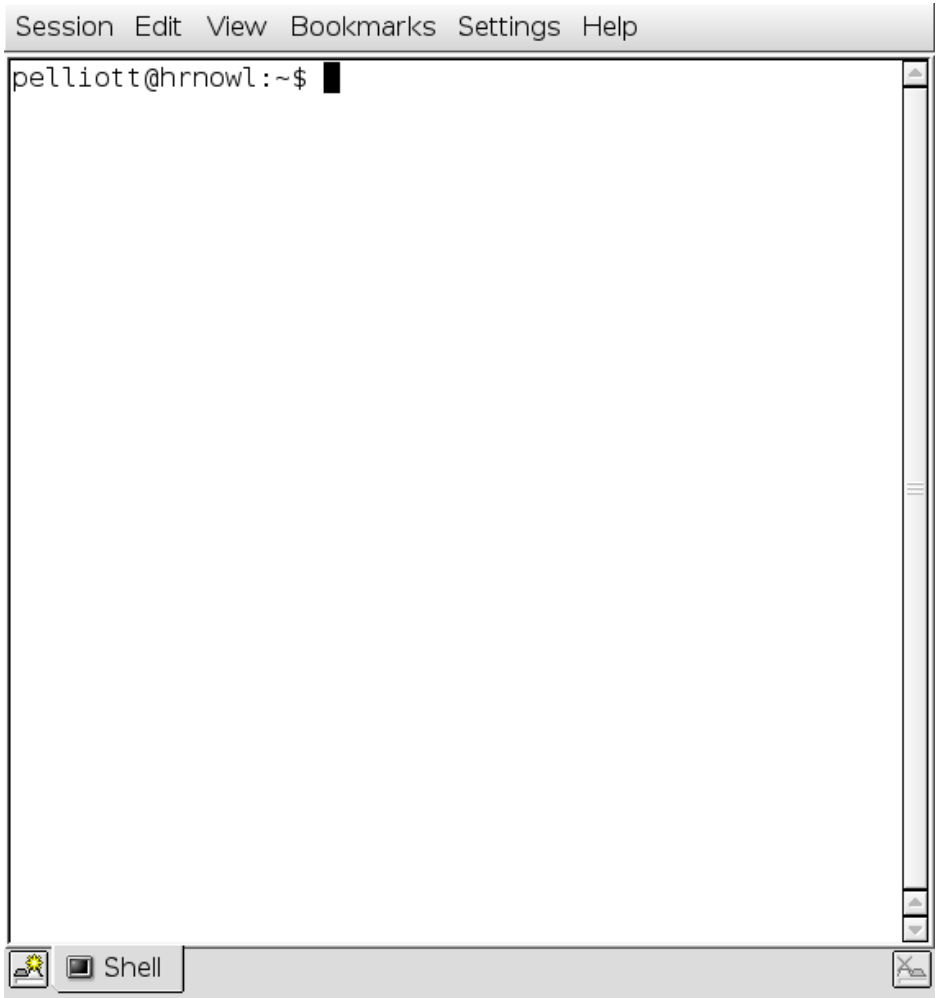
- Run a X11 terminal program on your home computer from your remote laptop.
- From this window you can run any X11 programs.
- You can even su to root, (if you know the password), for remote system administration, using X11 point and clicky programs.

Run program on remote “client”



- From this console window, you can run any X11 program.
- Output display will be seen on local X server. Program will run on remote computer.

X11 terminology



- In X11 terminology, the “X server” is where the screen, the keyboard and the mouse is, and the “client” is where the “program” is.
- This is backward from most other usage of client/server.