

Phone Home

Use Dynamic DNS to phone home!

Paul Elliott

Tell the dynamic DNS server to attend to your domain.

The image displays two screenshots of the Namecheap.com website interface, illustrating the process of configuring dynamic DNS for a domain.

Left Screenshot: Contact Information

The left screenshot shows the 'ADMINISTRATIVE CONTACT' and 'TECHNICAL CONTACT' forms. The contact information is as follows:

| Field | Value |
|-------------------|-------------------------------|
| First Name | Paul |
| Last Name | Elliott |
| Organization Name | Elliott Family |
| Street Address | PMB 181 |
| City | Austin |
| State/Prov. | TX |
| Zip/Postal Code | 78758 |
| Country | United States |
| E-Mail Address | paul_elliott_owl@sbcglobe.com |
| Phone Number | +1 5128371096 |
| Fax Number | +1 |

Right Screenshot: Modify Domain Settings

The right screenshot shows the 'Modify Domain' page for the domain **blackpatchpanel.com**. The 'ENABLE/ DISABLE DYNAMIC DNS FOR THIS DOMAIN' section is visible, with the current status set to 'Enabled'. The 'INFORMATION REQUIRED FOR DYNAMIC DNS CLIENT' section shows the domain name and host name.

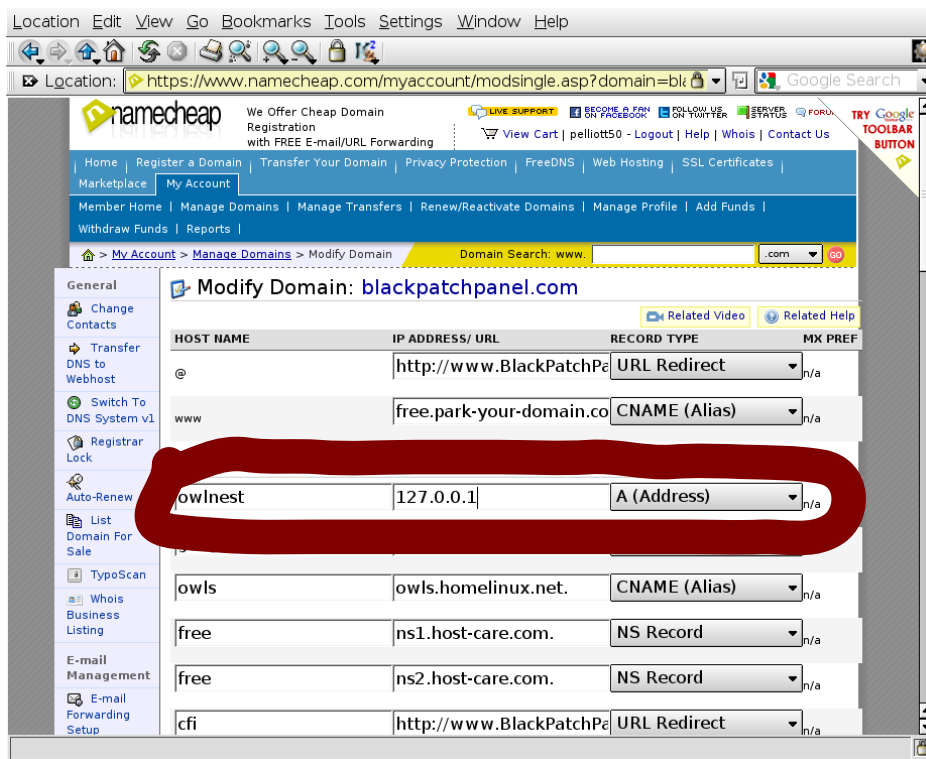
Domain Name: **blackpatchpanel.com**
Host Name: **anyhost_you_specify_in_client**

A large red arrow points from the 'Dynamic DNS' option in the left sidebar to the 'Dynamic DNS' section on the right page.

- 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!



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

Configure DDNS from LuCI Services

The screenshot shows the OpenWrt Dynamic DNS configuration page in the LuCI web interface, accessed via Mozilla Firefox. The browser's address bar shows the URL `tplink/cgi-bin/luci/stok=3bd65114bcff75f505bd6e632d199c0b/admin/services`. The page title is "OpenWrt - Dynamic DNS - LuCI". The navigation bar includes "OpenWrt", "Status", "System", "Services", "Network", and "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

Username

Password

Source of IP address network

Network wan

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

Related Help

ENABLE/ DISABLE DYNAMIC DNS FOR THIS DOMAIN

Current Dynamic DNS Status : **Enabled**

☒ Re-enable Dynamic DNS. **Password will be reset to new password.**

☐ Disable Dynamic DNS for this domain.

Save Changes

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

This is your hostname

Any "A" record can be modified.

NameCheap Hostname and Username

Modify Domain: blackpatchpanel.com

Host Records Updated Successfully
Host record information provided with valid values was updated successfully.

| HOST NAME | IP ADDRESS/ URL | RECORD TYPE | MX PRE |
|-----------|--------------------------------|---------------|--------|
| @ | http://www.BlackPatchPanel.com | URL Redirect | n/a |
| www | free.park-your-domain.com | CNAME (Alias) | n/a |

SUB-DOMAIN SETTINGS

| Sub-domain | Host Name | Record Type | MX PRE |
|--------------|---------------------|---------------|--------|
| owlnest | blackpatchpanel.com | A (Address) | n/a |
| google | google.com. | CNAME (Alias) | n/a |
| peless | home.gna.org. | CNAME (Alias) | n/a |
| swissephauto | home.gna.org. | CNAME (Alias) | n/a |
| free | ns1.host-care.com. | NS Record | n/a |
| free | ns2.host-care.com. | NS Record | n/a |
| | | | n/a |
| | | | n/a |
| | | | n/a |
| | | | n/a |

OpenWrt - Dynamic DNS - LuCI - Mozilla Firefox

OpenWrt - Dynamic DNS - LuCI

Dynamic DNS

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

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

NameCheap
ownest.blackpatchpanel.com

The diagram illustrates the ownership and DNS configuration of the domain ownest.blackpatchpanel.com. The domain name is shown at the top, with 'NameCheap' above it. The domain is circled in red. Two red arrows point from the domain to the text below: one from 'ownest' pointing to 'Subdomain with "A" record' and one from 'blackpatchpanel.com' pointing to 'My domain'.

- Subdomain with “A” record
- My domain

NameCheap
ownI nest.blackpatchpanel.com

The diagram consists of two red ovals at the top. The first oval contains the text 'ownI nest' and a red arrow points from it to the first bullet point below. The second oval contains the text 'blackpatchpanel.com' and a red arrow points from it to the second bullet point below.

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

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

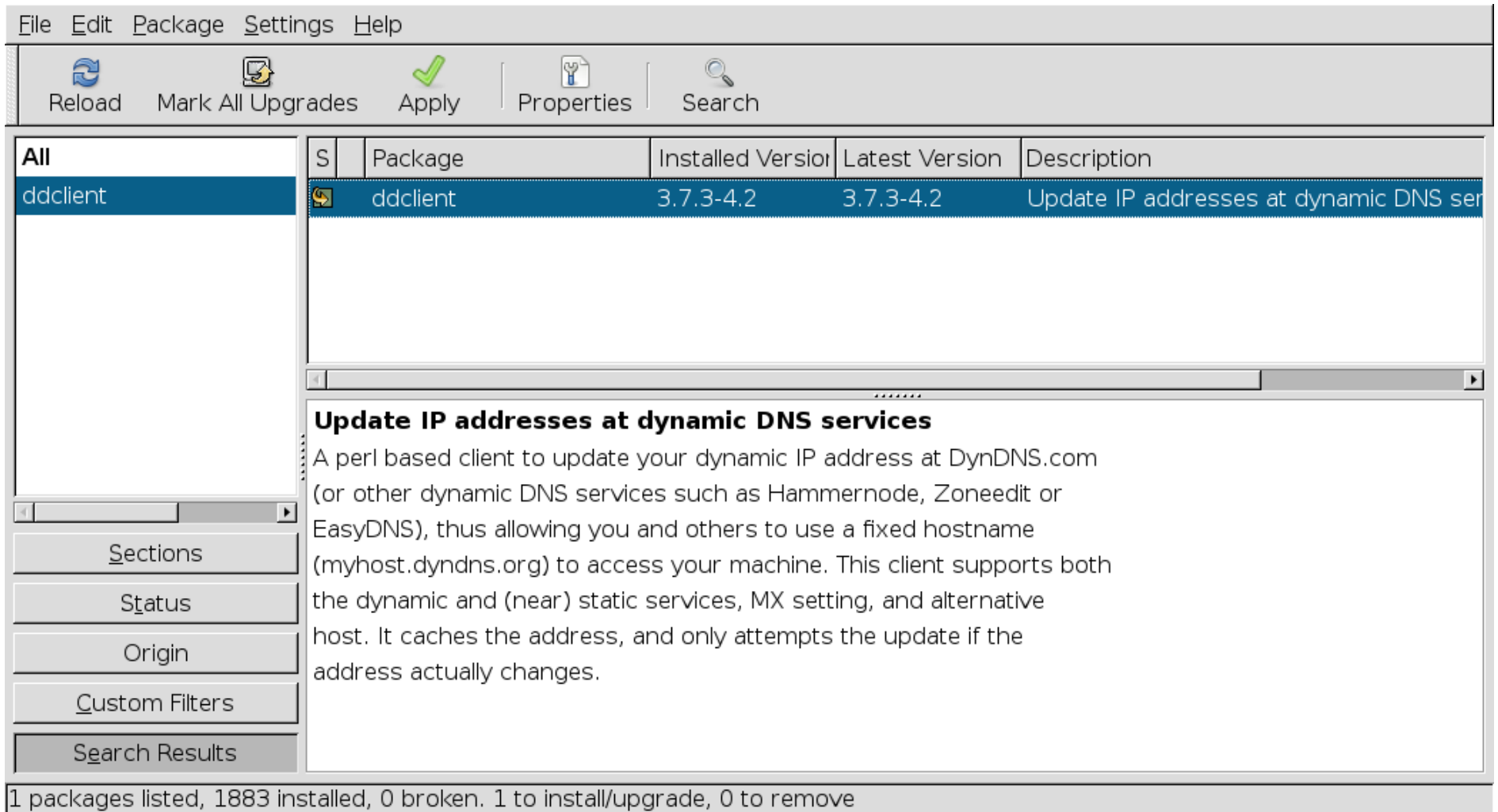
Network

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



The screenshot shows the Synaptic Package Manager interface. The top menu bar includes File, Edit, Package, Settings, and Help. Below the menu is a toolbar with icons for Reload, Mark All Upgrades, Apply, Properties, and Search. The main window is divided into two panes. The left pane shows a list of packages, with 'ddclient' selected under the 'All' category. The right pane displays the details for the 'ddclient' package, including its name, icon, installed version (3.7.3-4.2), latest version (3.7.3-4.2), and description. The description states: 'Update IP addresses at dynamic DNS services'. Below the description, there are buttons for Sections, Status, Origin, Custom Filters, and Search Results. At the bottom of the window, a status bar indicates: '1 packages listed, 1883 installed, 0 broken. 1 to install/upgrade, 0 to remove'.

File Edit Package Settings Help

Reload Mark All Upgrades Apply Properties Search

| S | Package | Installed Version | Latest Version | Description |
|---|----------|-------------------|----------------|--|
|  | ddclient | 3.7.3-4.2 | 3.7.3-4.2 | Update IP addresses at dynamic DNS ser |

Update IP addresses at dynamic DNS services

A perl based client to update your dynamic IP address at DynDNS.com (or other dynamic DNS services such as Hammernode, Zoneedit or EasyDNS), thus allowing you and others to use a fixed hostname (myhost.dyndns.org) to access your machine. This client supports both the dynamic and (near) static services, MX setting, and alternative host. It caches the address, and only attempts the update if the address actually changes.

Sections
Status
Origin
Custom Filters
Search Results

1 packages listed, 1883 installed, 0 broken. 1 to install/upgrade, 0 to remove

Are you running dhclient or dhcpcd?

```
$ ps -A|grep -i dh
```

```
3222 ?          00:00:00 dhcddbd
```

```
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  
#password=test  
#mx=mx.for.your.host  
#backupmx=yes|no  
#wildcard=yes|no
```

- Your complete dns hostname goes here.

- Login

- password

default login

default password

default MX

host is primary MX?

add wildcard CNAME?

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=XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX \
owlneast
```

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=XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX \
owlneast
```

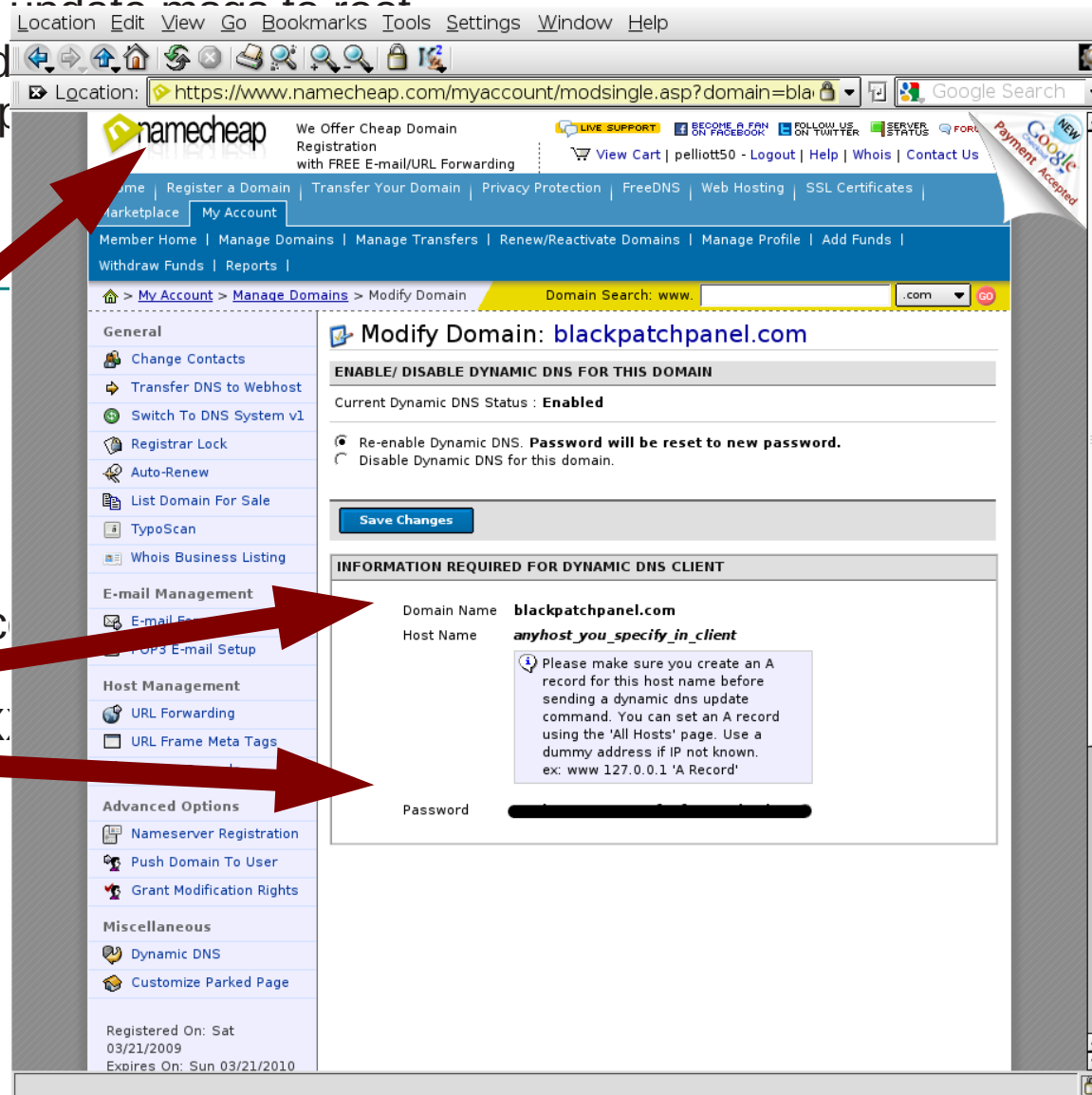
- Needed only if you need to run as a daemon
- i.e. not running dhclient or dhcpcd

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 pid
ssl=yes              # use ssl-sup
```

```
use=fw, fw=192.168.86.198/mymodem
```

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



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
ssl=yes              # use ssl
```

use=fw, fw=192.168.86.198/mymod

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

The screenshot shows the 'Modify Domain' page for 'blackpatchpanel.com' on the NameCheap website. The page displays a table of DNS records. A red arrow points from the 'owlnest' entry in the configuration text to the 'owlnest' entry in the DNS records table.

| HOST NAME | IP ADDRESS/ URL | RECORD TYPE | MX PREF |
|-----------------------|--------------------------|---------------|---------|
| @ | http://www.BlackPatchPa | URL Redirect | n/a |
| www | free.park-your-domain.co | CNAME (Alias) | n/a |
| SUB-DOMAIN SETTINGS ▼ | | | |
| owlnest | 127.0.0.1 | A (Address) | n/a |
| google2a45a90e0d339fd | google.com. | CNAME (Alias) | n/a |
| owls | owls.homelinux.net. | CNAME (Alias) | n/a |
| free | ns1.host-care.com. | NS Record | n/a |
| free | ns2.host-care.com. | NS Record | n/a |
| cfi | http://www.BlackPatchPa | URL Redirect | n/a |

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
```

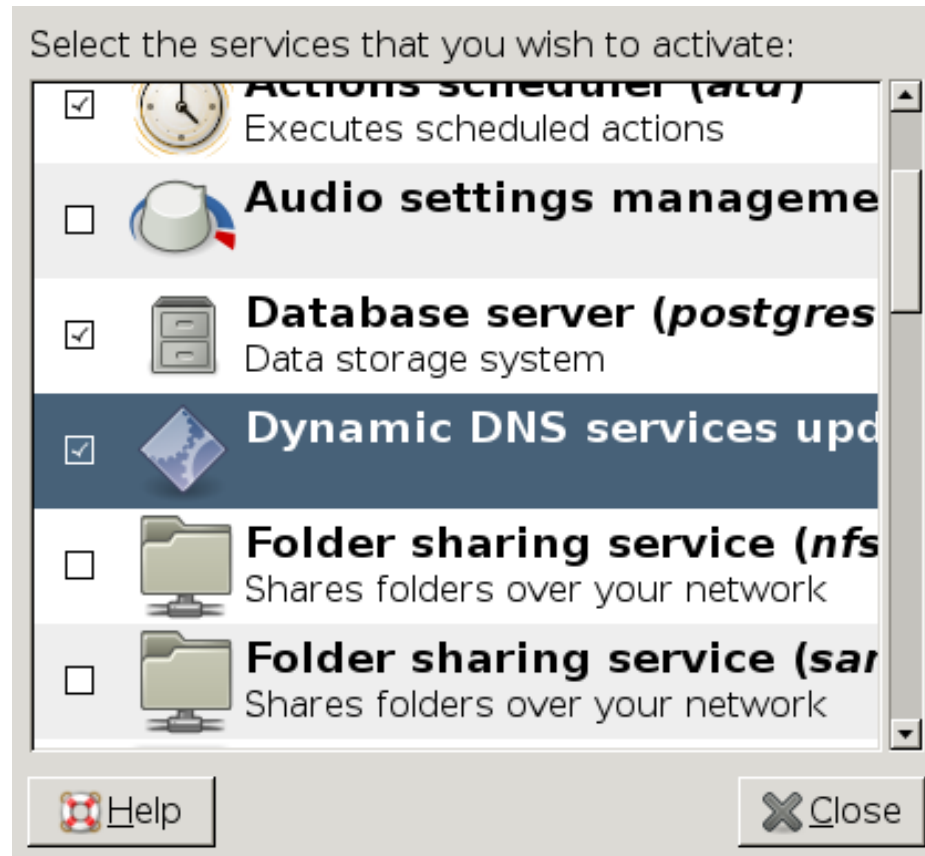
```
TIME CMD
```

```
2833 ?
```

```
00:00:00 dhclient
```

- `cp /usr/share/doc/dhclient/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
```

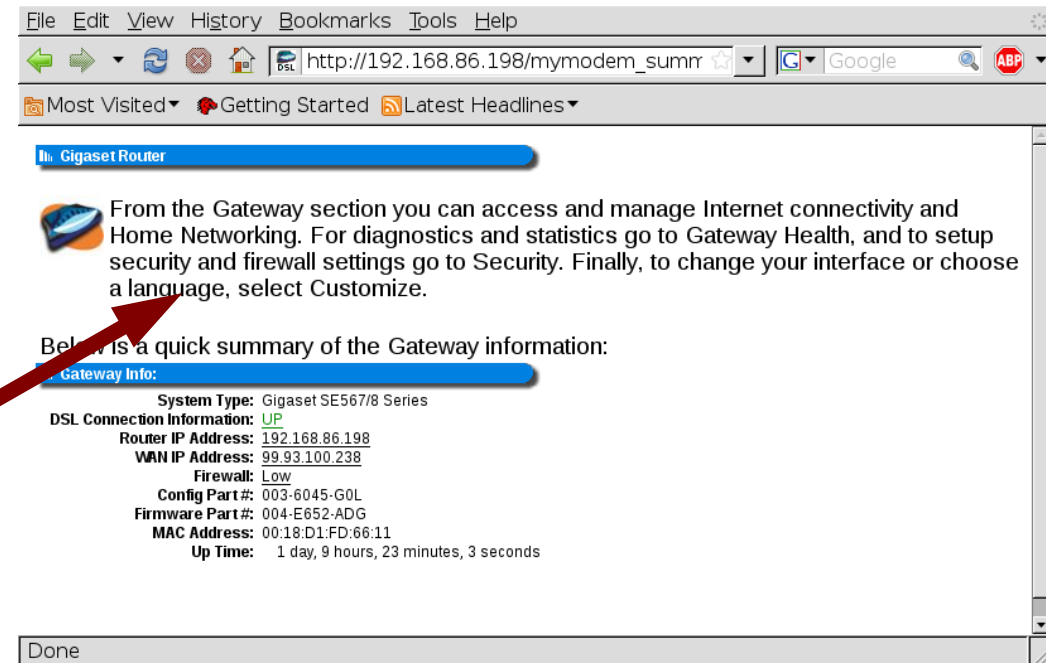
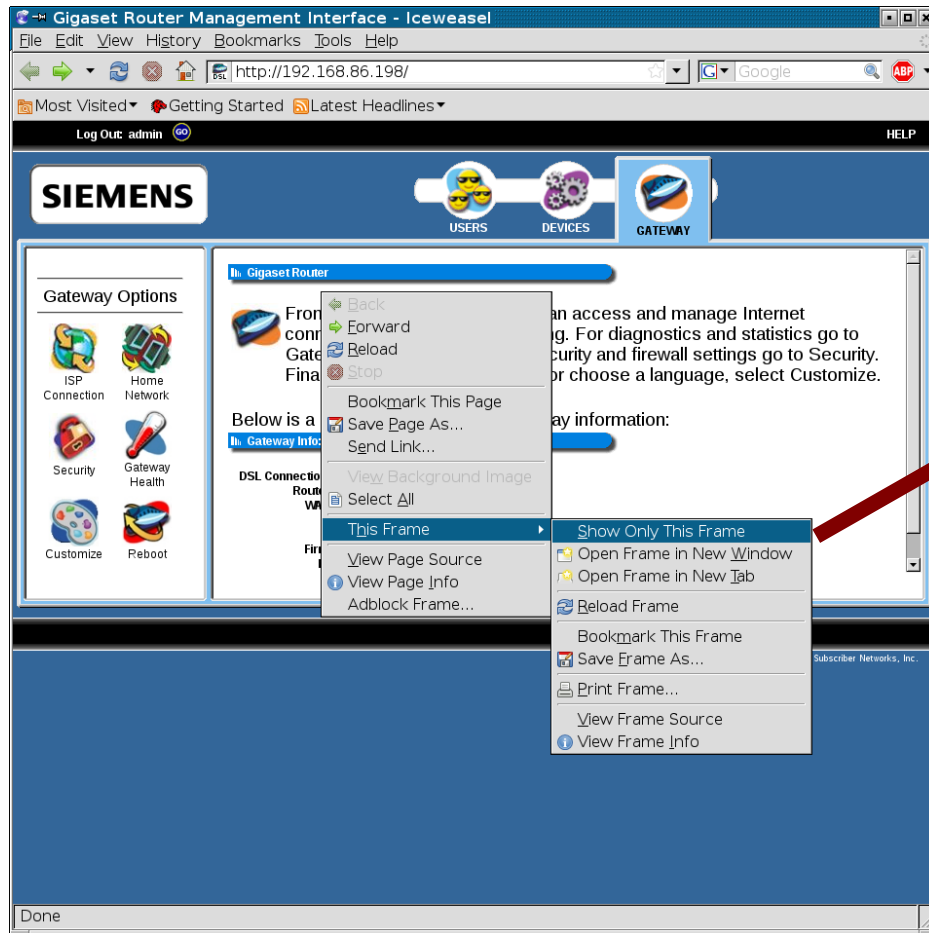
- Common routers have built in support.
- Just uncomment correct “use” line in the sample ddclient.conf file.

If your router is unsupported Web Scrape



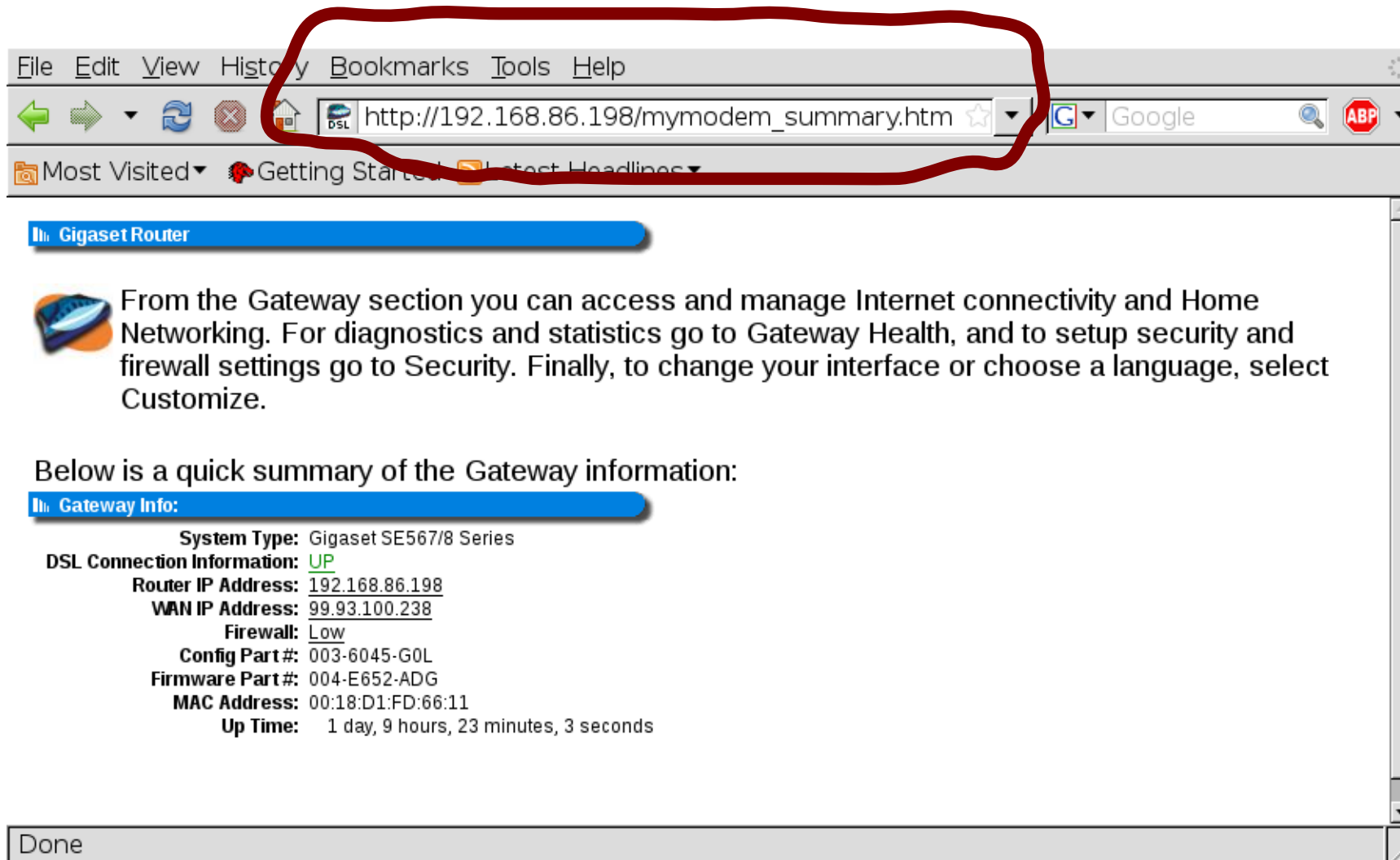
- Find the page in your router's web pages that displays the external IP address.

Isolate the frame containing the external IP address.



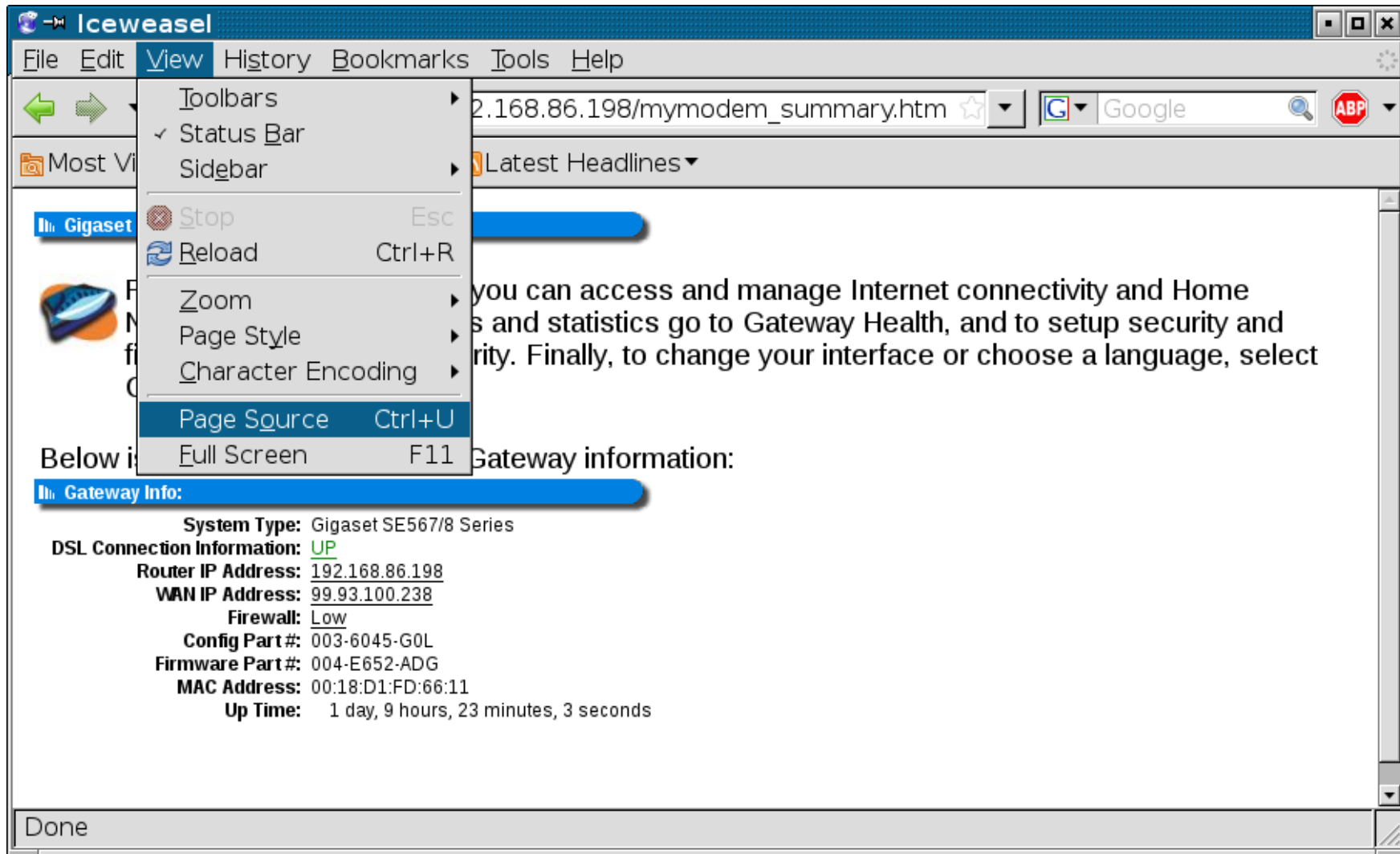
- Right click on the frame; Show only this Frame

Note the URL.

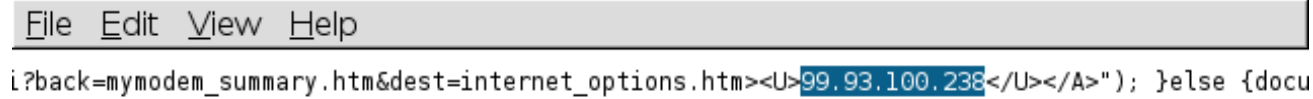


- We will use the url to create a “use” line.

View the source for the page

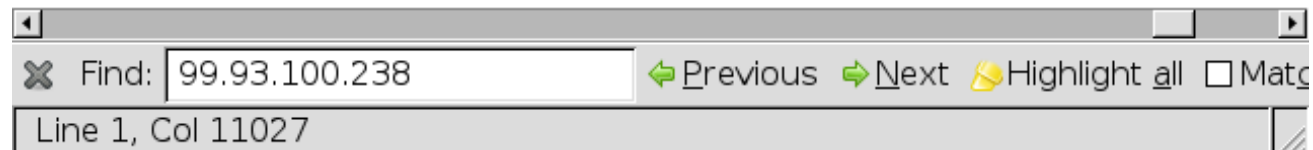


Search of external IP address in the source!



The screenshot shows a text editor window with a menu bar (File, Edit, View, Help) and a single line of code. The code is a JavaScript conditional statement. The IP address '99.93.100.238' is highlighted in blue. Below the editor, a search bar is visible with the same IP address entered, and navigation buttons for finding the next or previous occurrence.

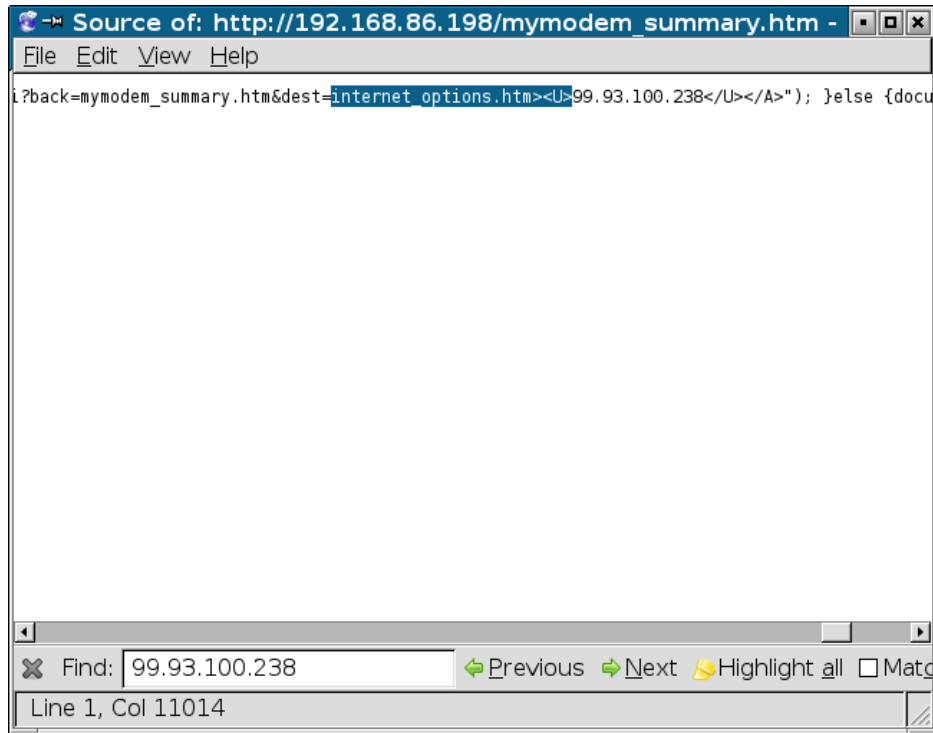
```
File Edit View Help  
i?back=mymodem_summary.htm&dest=internet_options.htm><U>99.93.100.238</U></A>"); }else {docu
```



This section shows the search interface of the text editor. The search bar contains the text '99.93.100.238'. To the right of the search bar are buttons for 'Previous', 'Next', 'Highlight all', and a checkbox for 'Match case'. Below the search bar, the status bar indicates the current position in the document: 'Line 1, Col 11027'.

Find: 99.93.100.238 Previous Next Highlight all ☐ Match case
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

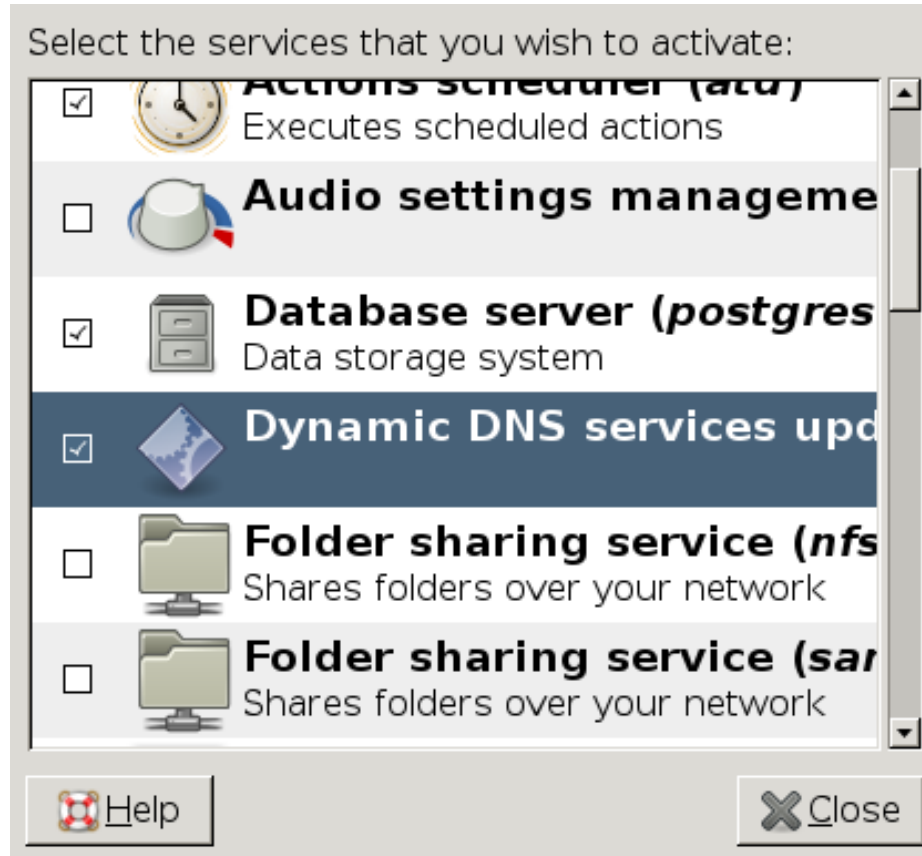
Edit /etc/ddclient.conf

```
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=XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX \
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

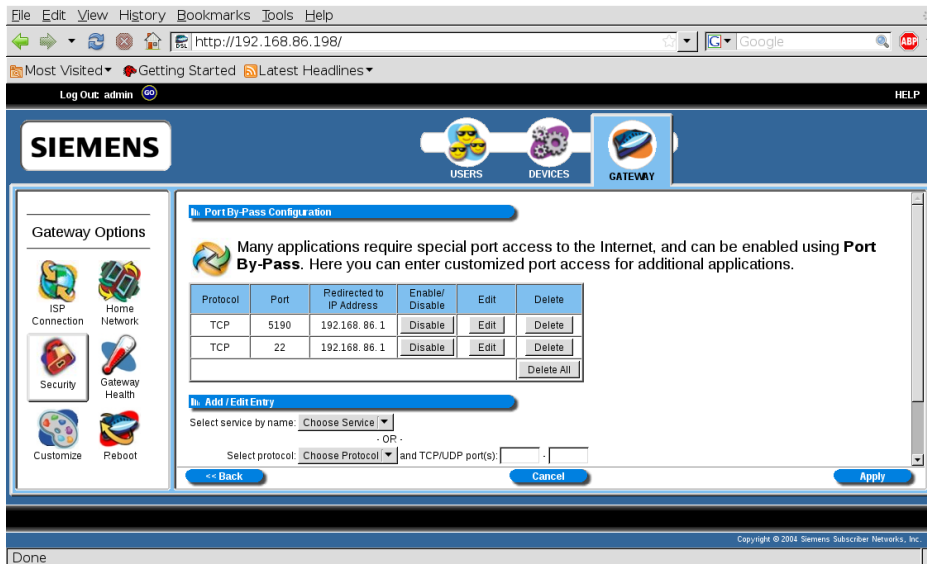
;; ANSWER SECTION:
owlnest.blackpatchpanel.com. 1800 IN A 99.93.100.238

;; 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



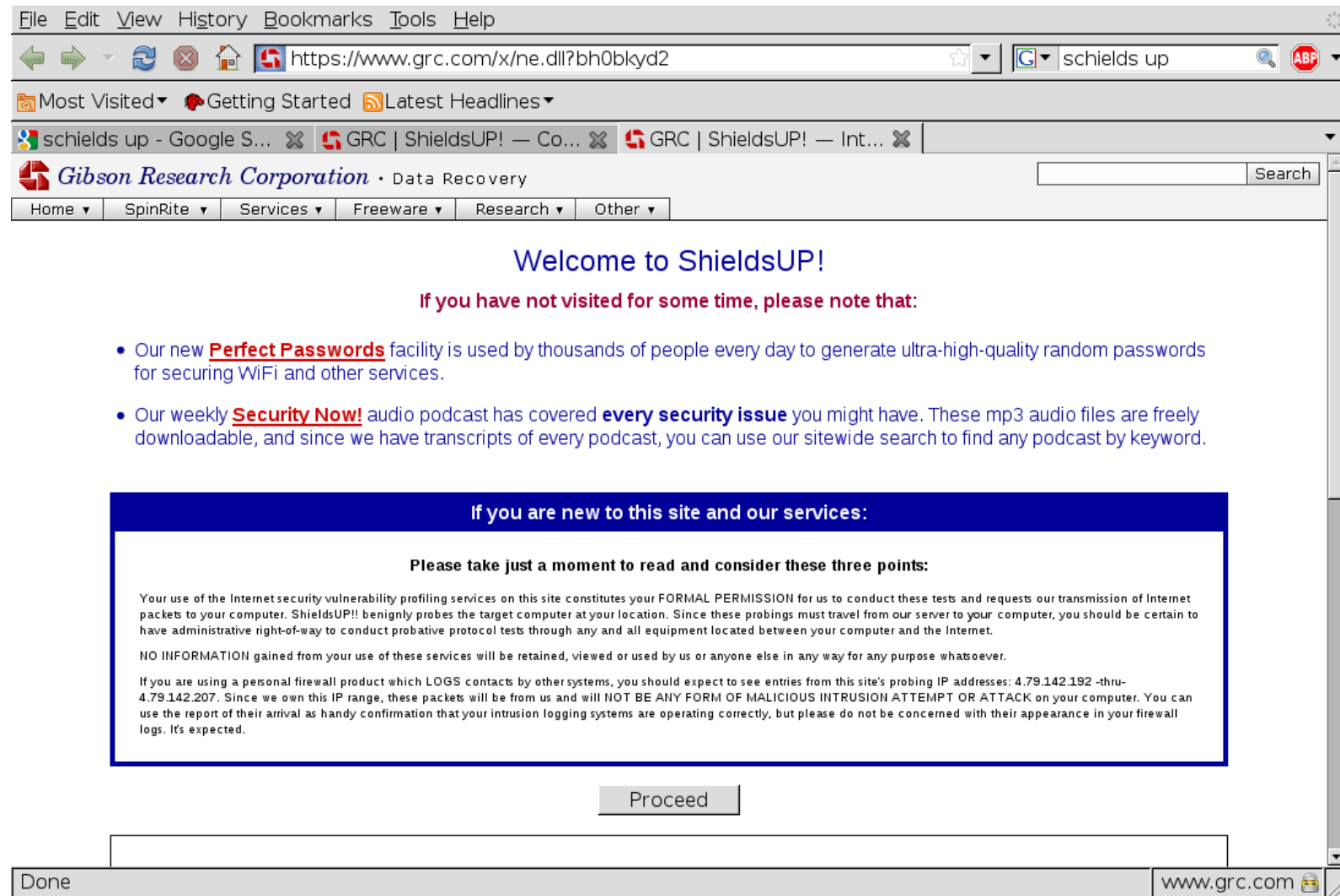
- How you do this depends on your firewall management software.
- I use “firestarter”

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!

The screenshot shows the ShieldsUP website interface. At the top, the browser address bar shows the URL `https://www.grc.com/x/ne.dll?rh1dkyd2`. The ShieldsUP logo is prominently displayed, followed by the text "Port Authority Edition - Internet Vulnerability Profiling by Steve Gibson, Gibson Research Corporation".

The main heading reads "Checking the Most Common and Troublesome Internet Ports". Below this, a message states: "This Internet Common Ports Probe attempts to establish standard TCP Internet connections with a collection of standard, well-known, and often vulnerable or troublesome Internet ports on YOUR computer. Since this is being done from our server, successful connections demonstrate which of your ports are 'open' or visible and soliciting connections from passing Internet port scanners."

The user's IP address is shown as **99.76.4.57**, with the status "Is being profiled. Please stand by...". A progress bar indicates the testing time: "Total elapsed testing time: 5.007 seconds".

The results section is titled "TruStealth Analysis" and is flanked by two large red "FAILED" stamps. The text explains: "Solicited TCP Packets: RECEIVED (FAILED) — As detailed in the port report below, one or more of your system's ports actively responded to our deliberate attempts to establish a connection. It is generally possible to increase your system's security by hiding it from the probes of potentially hostile hackers. Please see the details presented by the specific port links below, as well as the various resources on this site, and in our extremely helpful and active [user community](#)."

Below this, it states: "Unsolicited Packets: PASSED — No Internet packets of any sort were received from your system as a side-effect of our attempts to elicit some response from any of the ports listed above. Some questionable personal security systems expose their users by attempting to 'count-probe the probe', thus revealing themselves. But your system remained wisely silent. (Except for the fact that not all of its ports are completely stealthed as shown below.)"

The "Ping Echo: PASSED" message indicates: "Your system ignored and refused to reply to repeated Pings (ICMP Echo Requests) from our server."

A table summarizes the scan results:

| Port | Service | Status | Security Implications |
|--------------------|---------|---------|---|
| 0 | <nil> | Stealth | There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address! |
| 21 | FTP | Stealth | There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address! |
| 22 | SSH | OPEN! | Secure Shell provides a secure-connection version of the Telnet remote console service with additional features. Unfortunately, the SSH services and their security add-on packages have a long history of many widely exploited buffer overflow vulnerabilities. If your system has this port exposed to the outside world you should be vigilant in keeping your SSH service updated. |
| 23 | Telnet | Stealth | There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address! |

The browser status bar at the bottom shows "Done" and the address `www.grc.com`.

- 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

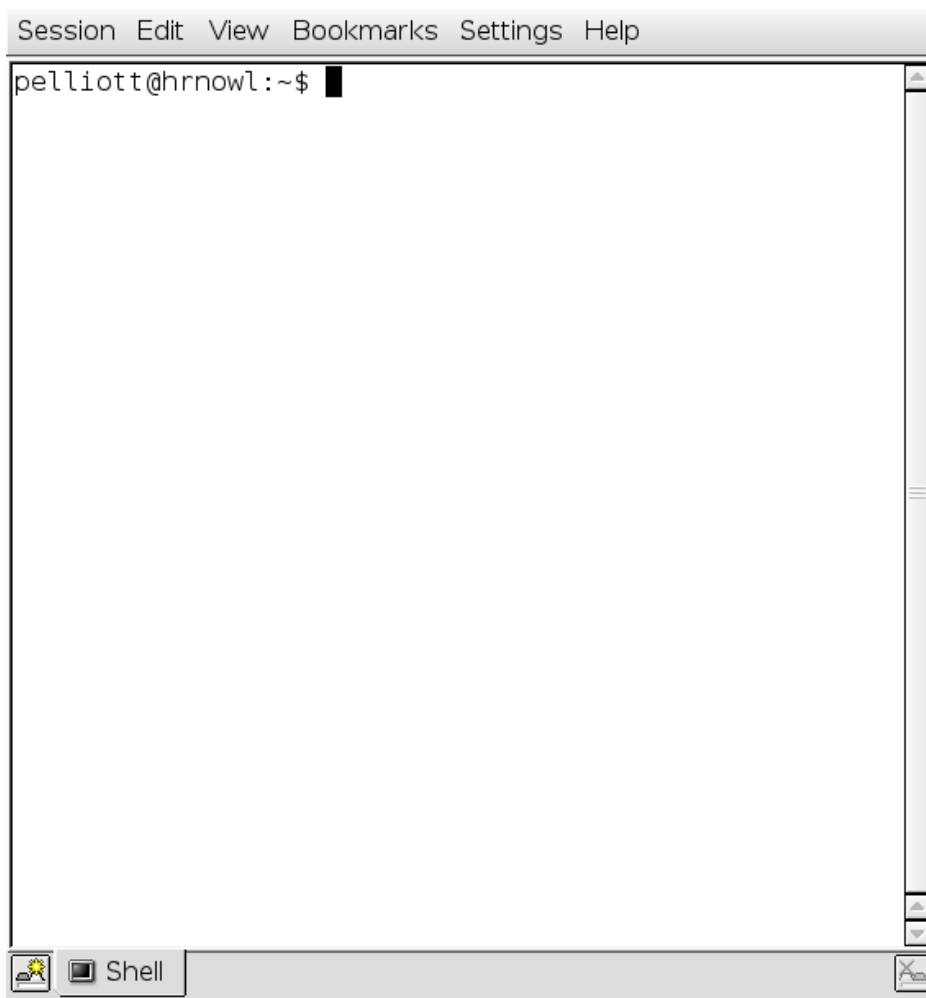
- `ssh-copy-id -i ~/.ssh/yourkey.pub user@remote.host`
 - If you have disabled password access this will not work!
 - Copy the file via sneaker net and a usb stick
 - On your mobile computer
 - `Cp mykey.pub /media/usbstick/mykey.pub`
 - On your home computer
 - `cat /media/usbstick/mykey.pub \>>~/.ssh/authorized_keys`

You are now ready to phone home.

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

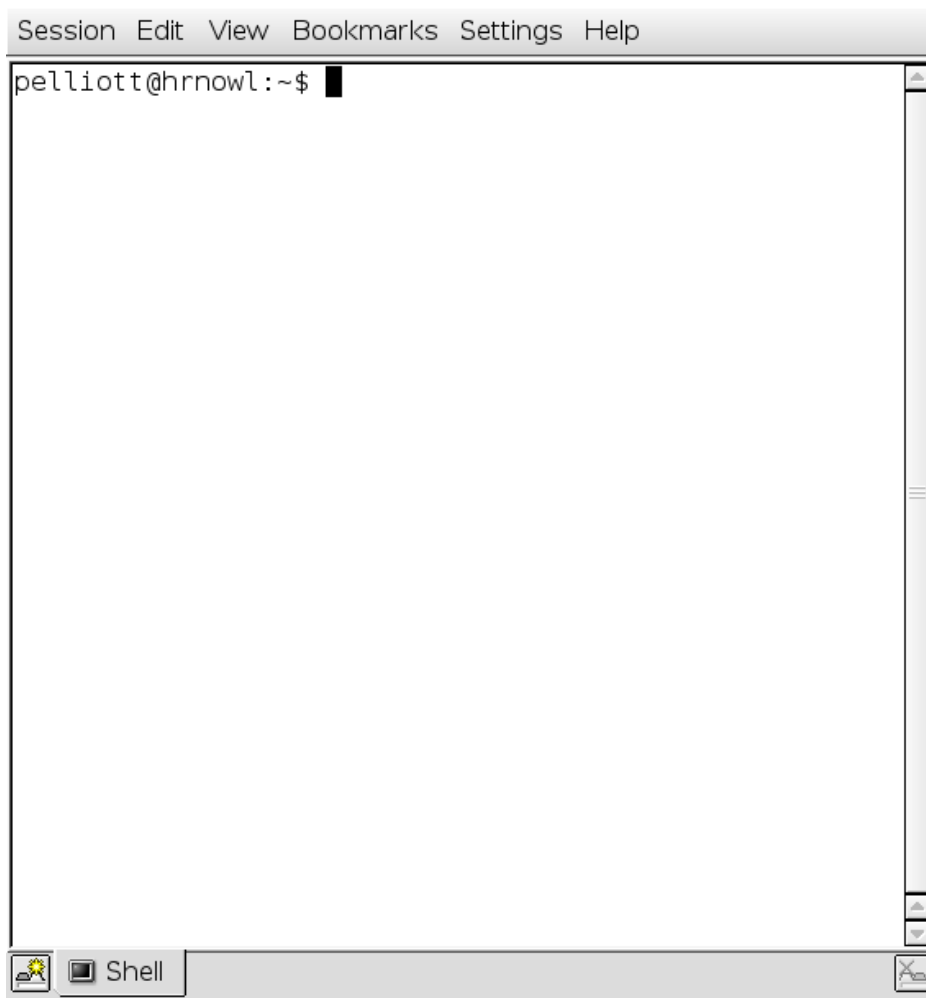
- Run a X11 terminal program on your home computer from your remote laptop.
- From this window you can run any X11 programs.
- You can even su to root, (if you know the password), for remote system administration, using X11 point and clicky programs.

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.