

# Netinfo

## Network System Locator and Policy Enforcement Tool

---

*version 3.0.0*

*distributed under GPLv2*

<http://www.it.teithe.gr/~v13/>

by Stefanos Harhalakis  
<v13@priest.com>

# 1 Introduction

In a switch based campus it is not easy to restrict users from changing the IP address of their computers. It is also common for people to change the network location of their computers by using any plug near them.

There are also times when you know the IP address of a computer that causes problems but you don't know the exact location of it inside the switched network.

Netinfo locates each and every known MAC address inside a campus and the IP address(es) it is using. It can spot IP address changes, NIC changes or switchport changes.

Netinfo was original developed to locate machines around the network. Since then it was extended to hold much more network information and can also prevent users from changing IPs or Location to their computers.

# 2 How it works

Netinfo uses SNMP to collect information from predefined routers and switches. After that it uses expect scripts to reconfigure switches (optional).

Initially the user has to specify routers and switches to be monitored. Those are referred as monitored network devices from now on. No other router or switch will be discovered. **Only Cisco devices can be handled.**

Netinfo consists of:

- The netinfo binary. It collects data from the network using SNMP and it has to be run as a cron job.
- The web interface. After netinfo is installed, this is how the user interacts with it.
- A shell script. It creates some expect scripts and runs them to reconfigure switches. It should be run as a cron job too.

The netinfo binary uses SNMP to collect information from routers and switches. From routers:

- The interface names and aliases.
- The ARP cache and the IP-to-interface mappings.
- The MAC addresses of the interfaces.
- The internal MAC addresses.
- The configured IP networks.

From switches:

- The interface names and aliases.
- The MAC-to-port mappings.
- The internal MAC addresses.
- The interface MAC addresses.

After that it combines this information by:

- Identifying ports that are connected to other Monitored Network Devices. Those interfaces are isolated. This means that no device will be ever reported on those interfaces.
- Creating a table of  $(IP, MAC, router, router\_interface)$  pairs.
- Creating a table if  $(MAC, switch, switch\_interface)$  pairs.
- Combining the tables to report IP-to-MAC, IP-to-interface and MAC-to-interface associations.
- Logging all new information to a history log for future reference.

All data are stored in a PostgreSQL database.

The web interface consists of php scripts but can be used under sthe suexec wrapper too. Netinfo does not require any privileges at all.

## 3 Requirements

To use Netinfo you'll need:

- PostgreSQL  $\geq 7.4$  - <http://www.postgresql.org/>
- PHP 4 - <http://www.php.net/>
- Net-SNMP - <http://www.net-snmp.org/>  
(This is version 5 of ucd-snmp)
- v-lib  $\geq 1.5.3.0$  - <http://aetos.it.teithe.gr/~v13/vlib>
- OpenSSL - <http://www.openssl.org/>  
You'll need this only if your PostgreSQL or Net-SNMP installation uses it, but in that case you'll have it already installed.

## 4 Installation

### 4.1 Configure

After installing the required libraries, run configure. The most interesting parameters are:

<code>--with-vlib=DIR</code>	where vlib is installed
<code>--with-postgre=FILE</code>	where postgresQL is installed
<code>--with-openssl=FILE</code>	where OpenSSL is installed
<code>--with-snmp=DIR</code>	where libnetsnmp is installed
<code>--with-php=FILE</code>	the php executable
<code>--with-expect=FILE</code>	the expect executable
<code>--with-htmldir=DIR</code>	where the interface will be installed
<code>--enable-static-vlib</code>	Use static version of vlib
<code>--prefix=PREFIX</code>	install architecture-independent files in PREFIX

Since vlib is not part of any distribution it is most probable that it will not be already installed in your system. It is possible to install it in a temporary directory (lets say /tmp/vlib). After that you may run configure like:

```
./configure --with-vlib=/tmp/vlib --enable-static-vlib
```

This will statically link it and it will not be needed anymore after the compilation stage.

The default `htmldir` is `www/` under `${prefix}`

You're encouraged to use a prefix other than `/usr/local` (e.x. `/usr/local/netinfo`). The installation procedure will create a tree as shown in Figure 1:

```
prefix/  
+-- bin/  
+-- db/  
+-- etc/  
+-- maclock/  
\-- www/
```

Figure 1: Installation tree

## 4.2 ‘make’ and ‘make install’

When `configure` is finished run “make” and “make install”. This will place:

- The web related scripts, the web pages and a configuration file in `htmldir` (default: `${prefix}/www`).
- The `netinfo` binary in `${prefix}/bin`.
- The `netinfo` configuration file in `${prefix}/etc` (named `netinfo.conf`).
- A ‘`create.sql`’ in `${prefix}/db`
- A ‘`maclock.sh`’ in `${prefix}/maclock`

From now on it is assumed that you’ve installed `netinfo` in `/usr/local/netinfo/`.

## 4.3 Database

Next you will have to setup the database:

- Create a database user that will be used by netinfo to access the database. It is ok if you use an existing user. Read the PostgreSQL manual for the syntax of the 'CREATE USER' command. For a quick start, as a database administrator issue:

```
$ psql template1
Welcome to psql 7.4.1, the PostgreSQL interactive terminal.

Type: \copyright for distribution terms
      \h for help with SQL commands
      \? for help on internal slash commands
      \g or terminate with semicolon to execute query
      \q to quit

template1=# CREATE USER netinfo UNENCRYPTED PASSWORD 'test';
CREATE USER
```

where 'netinfo' is the username and 'test' is the password.

- Create the database that the program will use. Assuming that you have postgresql binaries in your path, select a name for the database (lets say netinfo) and issue:

```
$ createdb netinfo -O netinfo
CREATE DATABASE
$ createlang plpgsql netinfo
```

This has to be done as a database administrator, since they are the only ones that may create databases.

- Now you'll have to create the database tables and populate the vendors table. Go to the db/ dir under the installation prefix and issue:

```
$ cd /usr/local/netinfo/db/
$ psql -U netinfo -f create.sql netinfo
$ psql -U netinfo -f vendors.sql netinfo
```

Assuming that the database user you want to use is netinfo and the database is named netinfo. You'll be prompted to enter the password.

## 4.4 Configuration Files

Now you're ready to create the configuration files:

- Enter `/usr/local/netinfo/etc` and rename `netinfo.conf.sample` to `netinfo.conf`:

```
$ cd /usr/local/netinfo/etc
$ mv netinfo.conf.sample netinfo.conf
```

- Edit `netinfo.conf` like this:

```
dbname=netinfo
dbuser=netinfo
dbpass=test
resolvers=3
```

- Now enter `/usr/local/netinfo/www/` and rename `.dbconf.sample` to `.dbconf`:

```
$ cd /usr/local/netinfo/www
$ mv .dbconf.sample .dbconf
```

- Edit it like this:

```
<?php
$dbname=netinfo;
$dbuser=netinfo;
$dbpass=test;
?>
```

*IT IS MANDATORY NOT TO ENTER ANY EMPTY LINES BEFORE ‘<?php’ AND AFTER ‘?>’!!!*

- Finally enter `/usr/local/netinfo/maclock` and edit `maclock.sh`. If you are not using ‘netinfo’ as the database name you have to change the line:

```
DBNAME=netinfo
```

## 4.5 Web server

Next you will have to configure your web server to provide access to the `www/` directory. Netinfo is only tested and known to work under the Apache web server. *Don't forget to password protect this directory!*

### 4.5.1 Apache configuration

Edit your httpd.conf and add:

```
Alias /netinfo "/usr/local/netinfo/www/"
<Directory /usr/local/netinfo/www>
    AllowOverride AuthConfig
</Directory>
```

If you have used `--disable-mod_php` when configuring netinfo you'll have to add:

```
Options ExecCGI
```

in the Directory section and:

```
AddHandler cgi-script .cgi
```

in the global section. Next go to `/usr/local/netinfo/www` and create a file named `.htaccess`:

```
$ cd /usr/local/netinfo/www
$ cat << KOKO > .htaccess
> AuthType Basic
> AuthName "Restricted Access"
> AuthUserFile /usr/local/netinfo/www/.htpasswd
> Require user netinfo
> KOKO
$
```

Finally, while you're in `/usr/local/netinfo/www` run:

```
$ htpasswd -c .htpasswd netinfo
```

and enter a password. At this point you've setup the apache server and you have password protected the netinfo web interface. Next you'll have to restart your apache server with one of the following:

```
# apachectl restart
# /etc/init.d/apache restart
# /etc/rc.d/apache restart
```

or something similar depending on your distribution. From now on, I assume that you can access Netinfo as `/netinfo` from a web browser.



## 4.6 Cron jobs

Now you should create two crontab entries:

### 4.6.1 data collection

The first should invoke the netinfo binary that will collect the information. Add something like this to your crontab: `0,10,20,30,40,50 * * * *  
/usr/local/netinfo/bin/netinfo >/tmp/netinfo.log 2>&1`

This will collect data every 10 minutes.

### 4.6.2 MAC locking

Next you should create a script for the maclocking:

```
#!/bin/sh
# cd to the script location
cd /usr/local/netinfo/maclock

# run the script
./maclock.sh
```

Assuming that you've put this in `maclock/cron_maclock.sh`, add this line to your crontab:

```
15,45 * * * * /usr/local/netinfo/maclock/cron_maclock.sh >/dev/null 2>&1
```

*Note: You should not add this cronjob at the first time. Use the MAC locking feature only when you've become familiar with Netinfo and you really know what you're doing.*

It is not a good idea to run the maclock script very often. There are more than one reasons for that:

- There will be unpredictable results if the maclock script is run when another instance is already running. Created scripts will be overwritten while they are running and more than one instances will try to configure the same device.
- In case of a network problem, errors will be logged every time that script is run.

- The script requires the same system resources even if no device configuration needs to be changed.

## 5 Using netinfo

Now that you've installed netinfo you're ready to start using it.

### 5.1 General guides

#### 5.1.1 Web browser notes

Netinfo was developed and tested under Linux and KDE. The web pages are tested and known to work when using Konqueror from KDE 3.1 or Netscape Navigator 7. It uses HTML 4 and CSSv1 (and some v2) for all of its pages and most of the images are in PNG format. It seems that until now, Internet Explorer is not able to display transparent PNG images. Since this is a browser limitation I'm not considered in 'fixing' it. IE is also known to have other problems too. In my tests it is shown that each version of IE will render the web pages in a different way and introduce different problems. Since I've tried to use standard HTML 4 and CSSv2 and the stylesheet was verified by the W3C verifier (this may not be true for the current version of netinfo but it was true for older versions, where IE had the same behavior), I consider most of the problems as a browser 'bug'. If you ever found invalid HTML then sent me a note and I'll correct it.

I've tried not to produce any web pages that are unusable when using IE. If you find (another) one then contact me.

#### 5.1.2 Upper bar

The upper bar is the main menu of netinfo. As of version 3.0.0 there are 5 options:

**Configuration:** This is where monitored devices are configured and run-time parameters are set.

**Data:** This is the place where all collected data can be found.

**Registry:** The registry holds device information and is required for spotting policy violations and make possible the MAC locking feature.

**Monitor:** Here you can look for network changes that may or may not be a policy violation.

**Policy:** Finally, the policy menu can be used to locate violations and watch the log entries.

## 5.2 Configuration

There are 2 sub menus:

### 5.2.1 Devices

Here you can add, edit or delete monitored network devices. When adding a new network device you should add at least an ip address, a name and a read-only community. The username and passwords are not required unless you want to use the maclocking feature. In that case you'll have to check the 'Do locking' option too.

### 5.2.2 Options

Those are the available run-time configuration options for netinfo:

**Hide Community names and password:** Specify whether the community names and the password should be shown as cleartext or as stars. You should set this to 'No' when configuring netinfo for the first time because you'll be able to check for typos in community names and/or passwords.

**Auto-discover subnets:** Whether the available subnets should be fetched from routers. You most probably want this enabled unless you don't want to monitor your complete IP address space.

**Max auto-discovered subnet mask (bits):** This will instruct netinfo to filter out all subnets with a greater subnet mask (in bits). Usefull to avoid discovering subnets for point-to-point links or for addresses with 32 bit subnet mask (/32).

Filter-out IPs that don't belong to a known subnet: This will drop all discovered IPs that are not part of a discovered or entered subnet. If you set this to 'No' then you may find some 1000s of unknown addresses because of proxy-arp.

Expire time for resolver cache (seconds): How long should the resolved hostnames remain in cache.

## 5.3 Data

This is the place where you can view all the collected information and set the associations between them:

### 5.3.1 Devices

The *Devices* section lists all the monitored network devices and some statistics about them:

Locking: Whether MAC locking should be performed on this device.

Flags: What maclock related data are entered for this device:

U: Username

T: Telnet password

E: Enable password

Interfaces:

Total: Total number of interfaces

With netdevs: Number of interfaces that connect this Monitored Network Device to another Monitored Network Device.

Routed: Number of routed interfaces.

Locked: Interfaces that locking should be performed.

Hunted: Interfaces that locking is activated because of a hunt.

Restricted IPs: Interfaces that allow specific IPs only.

Restricted MACs: Interfaces that allow specific MAC addresses only.

Discovered IPs: Number of IP addresses that were discovered from this device.

Discovered MACs: Number of MAC addresses that were discovered from this device.

Clicking on a device name will show the known interfaces of this device and some information about each interface.

Clicking on an interface name will show the known IPs and MACs on this interface.

It is also possible to view all interfaces at once. When viewing an interface, you can navigate from the quick bar (3rd from above) to each interface. On that bar there is also an interface name named 'ALL+'. If you select it you'll see all known IPs/MACs on all interfaces even if there is a network device discovered behind them.

Finally you can click on the 'Edit' option which will lead you to the registry editor. More on this later. Whenever you click on a IP or MAC address will lead you to the registry editor too.

### 5.3.2 IPs

The *IPs* section groups all discovered IP addresses and allows easy navigation between them. You should not need any explanation on this.

### 5.3.3 Subnets

Here you can view all the entered and/or discovered subnets/supernets of your network. The 'Major' flag means that this subnet/supernet is a superset of other known subnets.

### 5.3.4 Stats

Here you can view some statistics about the collected data.

### 5.3.5 Lookup

Last but not least, the lookup or search facility. Here you can perform a (possibly combined) query to:

- Find what NICs exist behind a switch port (interface).
- Find who is currently using an IP address.
- Find the location of an IP address or a MAC address.

## 5.4 Registry

From the registry you can edit registry entries. A registry entry contains information about an IP address, a MAC address or an Interface. Information includes:

- A short description
- Some comments
- One or more associations:
  - An IP address can be associated with one or more MAC addresses and with one or more Interfaces.
  - A MAC address can be associated with one or more IP addresses and with one or more Interfaces.
  - An interface can be associated with one or more IP addresses and with one or more MAC addresses.
- Restrictions regarding the associations:

Only listed IPs:

For MAC addresses: Means that this MAC address cannot use an IP address that it is not associated with. (Note that this doesn't prohibit other MAC addresses to use this IP address)

For Interfaces: Means that this Interface cannot serve an IP address that it is not associated with.

Only listed MACs:

For IP addresses: Means that this IP address cannot be used by a MAC address that it is not associated with.

For Interfaces: Means that this Interface cannot server a MAC address that it is not associated with.

Only listed Interfaces:

For IP addresses: Means that this IP address cannot exist on an interface that it is not associated with.

For MAC addresses: Means that this MAC address cannot exist on an interface that it is not associated with.

- Options regarding MAC locking (TODO: WRITE ME)

## 5.5 Monitor

From this section you can watch the 'interesting' network activity. You can view:

- MAC addresses that have changed IP address or MAC addresses that use more than one IPs.
- Possible IP conflicts. This will list all IP addresses that are known to be used by more than one MAC address. Because of the way switches and routers work it is almos impossible to tell between a conflict and a simple change. Just watch this section and remove entries that seem invalid.
- MAC addresses that changed interface. This means that a user that was connected to a switch port is now connected to another one.

At first the above reports may not seem very sane. This is because of routers that have more than one IP addresses on each port or for IP addresses that are handled by a dhcp server. You should use the 'Filters' to filter-out all those false-alarms. After some configuration, the Monitor section should be cleared from invalid entries/false alarms and it will be ready for production use.

## 5.6 Policy

After configuring the IP-MAC-Interface associations for your network you can use the Policy section to monitor for bad people trying to mess with the network.

### 5.6.1 Violations

The *Violations* screen lists all known policy violations in your network. Netinfo examines all available information and looks for IP-MAC-Interface pairs that don't comply with your policy restrictions.

For example:

Suppose that you have edited IP address 10.1.1.1 and set that it is associated with MAC address 12:23:34:45:56:67 and that only this MAC address should use it. After that, someone with a MAC address of 22:22:22:33:33:33 takes this IP address and uses the network. Netinfo will locate him and list him in Violations.

**NOTE:**Violations lists only the current violations. This means that if someone causes a policy violation but he has shutdown his computer, he will not be listed in 'Violations'!

### 5.6.2 Blacklist

Blacklist is a history of all users that cause a policy violation. Whenever a policy violation is encounter, the MAC address that caused it is entered in the blacklist. Even if he shutdown the computer he will remain in the blacklist until he is manually removed (!!!). When using the MAC locking feature, all MAC addresses that exist in the Blacklist will be locked out of the network.

### 5.6.3 Log

The log holds some log messages generated by netinfo. Log entries are cleared after 7 days.



## 5.7 MAC locking

TODO: WRITE ME

## 6 License

- This program is distributed under the terms of the GNU GPL v2. A copy of the license is included in the distribution.
- This license may change without further notice but will only affect future versions.
- You're using the program at your own risk and you're the only responsible for any damage that it may cause. It may be illegal to collect this kind of information from your (or another one's) network.
- If you believe that this license doesn't fit your needs then contact me.

## 7 Home - contact

The homepage of netinfo is at <http://www.it.teithe.gr/vtildev13>.

Send notes, bug reports, comments and requests to [v13@priest.com](mailto:v13@priest.com).

# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
<b>2</b>	<b>How it works</b>	<b>1</b>
<b>3</b>	<b>Requirements</b>	<b>3</b>
<b>4</b>	<b>Installation</b>	<b>3</b>
4.1	Configure . . . . .	3
4.2	‘make’ and ‘make install’ . . . . .	4
4.3	Database . . . . .	4
4.4	Configuration Files . . . . .	5
4.5	Web server . . . . .	6
4.5.1	Apache configuration . . . . .	7
4.6	Cron jobs . . . . .	8
4.6.1	data collection . . . . .	8
4.6.2	MAC locking . . . . .	8
<b>5</b>	<b>Using netinfo</b>	<b>9</b>
5.1	General guides . . . . .	9
5.1.1	Web browser notes . . . . .	9
5.1.2	Upper bar . . . . .	9
5.2	Configuration . . . . .	10
5.2.1	Devices . . . . .	10
5.2.2	Options . . . . .	10
5.3	Data . . . . .	11
5.3.1	Devices . . . . .	11
5.3.2	IPs . . . . .	12
5.3.3	Subnets . . . . .	12
5.3.4	Stats . . . . .	12
5.3.5	Lookup . . . . .	13
5.4	Registry . . . . .	13
5.5	Monitor . . . . .	14
5.6	Policy . . . . .	15
5.6.1	Violations . . . . .	15

Netinfo 3.0.0	18
<hr/>	
5.6.2  Blacklist . . . . .	15
5.6.3  Log . . . . .	15
5.7  MAC locking . . . . .	16
<b>6  License</b>	<b>16</b>
<b>7  Home - contact</b>	<b>16</b>