What Happened to My IP Number?

NetDB Log Searches

IPM

DHCP log searches

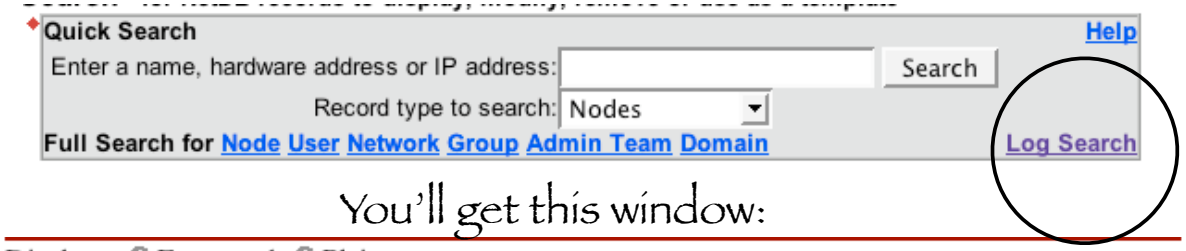
Purpose of class

- To help you answer questions such as "when was that node deleted?" "When did that node have its IP number changed?" "Did I really modify that node when I meant to use it as a template?" These we'll answer with NetDB log searches.
- To show you all the information you can get from an ipm search. Although it's mostly a log of all the arp tables, much useful information can be gleaned from it.
- DHCP searches (and a few other things) from the SUNet reports page.
- To be an interactive class, I'll happily do searches for real-world situations you've encountered on your networks.

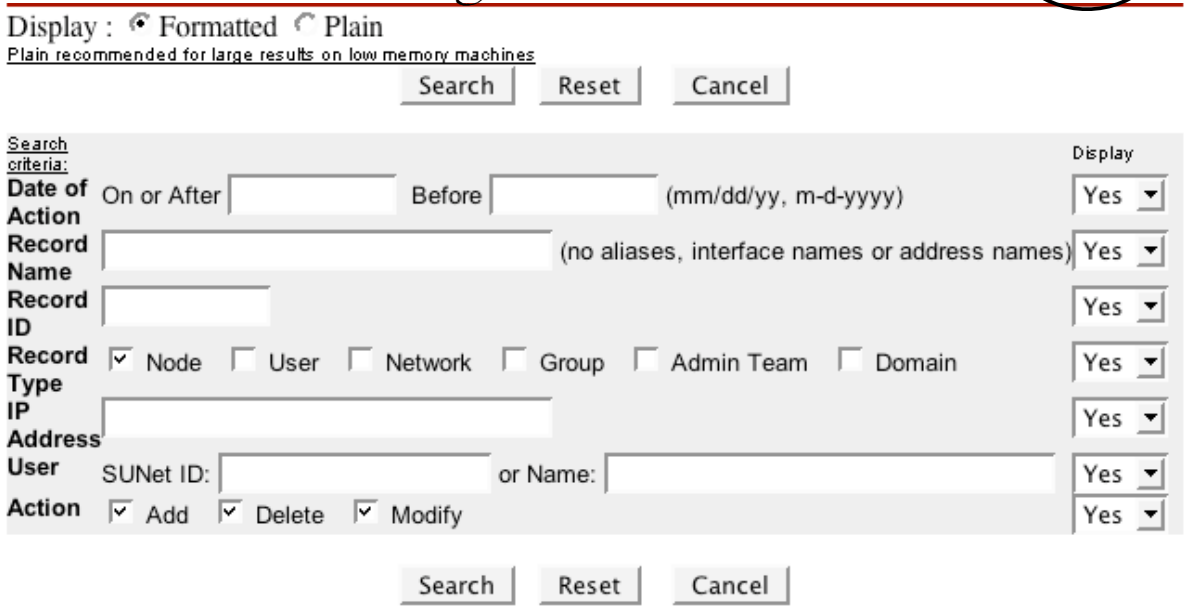
NetDB Log Searches

Note: Log searches take a very long time. Some browsers may quit after a minute if there's no response, so you may need to use a different browser.

Select from the lower right corner of the main NetDB window, where you've probably never looked before.



You'll get this window:



Log Search Fields

- Date of Action: Don't search on this alone, unless you really want to see absolutely everything that anyone did with NetDB on that date. Use it to help your searches.
- Record Name: The node name, not the alias. If the node name changed, you'll have to do another search, or search on another variable.
- Record ID: The most important search field. As names, IP numbers, etc. change, the ID stays the same until the node is deleted.
- Record Type: NetDB records aren't all nodes, and we log everything.
- IP address: Like name, if it changed, you'll need another search.
- User: another good way to limit the scope of your search.
- Action: Maybe you only want deletes, or modifies, etc.

Let's do a search.

- What's the history of the node named bogus-node? Search by name, what do you get?
- Search by IP number, are the results the same?
- Search by Record ID, now what do you get?
- On the next page is the history off all actions for that record, what doesn't show up?

The full sequence.

- Created by me
- Changed location to Polya
- Added alias “super-duper-bogus”
- Changed name to “hah-fooled-ya”
- Changed IP to 172.24.18.32
- Added IP 172.27.104.64
- Added hardware adderss “abba.abba.feeb” checked DHCP box
- Deleted alias
- Node deleted by Tim Poston

More Log Searches

- On your own, find all that you've ever deleted (be patient).
- Find any domains created this month, not modified or deleted.
- Find any domains that have been deleted this year.
- Others? Suggestions? Requests?

IPM

- From any "leland" system (just about any UNIX system with afs and Sident) the command is: `/usr/pubsw/sbin/ipm` You'll need a kerberos ticket, so yoy may need to to `kinit` first.
- Since command-line NetDB is also in `/usr/pubsw/sbin/` you may want to put it in your path. This varies by your shell so find a UNIX sysadmin to help you.
- The command without arguments gets the help screen!
-

```
elaine27:~> ipm

  usage: ipm [-d <days>] [-r <rows>] [-f <file>] [-amvs] name|addr ...

    Search for IP address names, IP addresses (dotted decimal format), or
    hardware addresses (in hex, with optional ':' or '-' delimiters)

    -a         display the IP address name instead of the NetDB entry name
    -d <days>  search for hosts last seen within this many days, default 30
    -f <file>  get names/addresses to look up from this file
    -h         print detailed usage instructions
    -m         print matches only
    -r <rows>  limit search results this many matches, default 1000
    -s         script-oriented output
    -u         print this message
    -v         verbose output
```

IPM argument modifiers

- The wildcard is "%" so to search for all nodes in a particular range, it's
  - `ipm 171.64.20.%` or `ipm 171.64.20.0/24`
- -a "display the IP address name instead of the NetDB entry name"
  Advanced nodes, such as my laptop, can have different names for different interfaces:`bramble23:~> ipm dru-macbook-en`

```
                                        Hardware              First     Last   Times
IP Address & Type   NetDB Entry      Address    NIC Type   Seen     Seen    Seen
----------------- --------------- ------------- -------- -------- -------- -----
171.64.20.57    n dru-macbook     0016cb:9ca75f  ---     09/08/06 12/18/08   356

[1 match returned, 0 items failed to match]
bramble23:~> ipm dru-macbook-en -a
                                        Hardware              First     Last   Times
IP Address & Type  Address Name      Address    NIC Type   Seen     Seen    Seen
----------------- --------------- ------------- -------- -------- -------- -----
171.64.20.57    n dru-macbook-en  0016cb:9ca75f  ---     09/08/06 12/18/08   356
```

- -d days "search for hosts last seen within this many days, default 30"
  - Especially useful for roaming hosts, or for searching a range of IP numbers, reduce the number of days. For hosts that may not have been used in a while, increase. You'll use this modifier more than any other.
- -f <file> get names/addresses to look up from this file
  - What if you want to search a large number, and there's no easy way to use a wildcard? Just put them all in a text file in your home directory and search on it. You'll want to use the -r modifier too.

IPM arguments continued.

- -h "print detailed usage instructions"
  - a.k.a. the "man" page.
- -m "print matches only"
  - Especially for -f searches, you may not want "Failed to match" results:

```
elaine27:~> ipm bogus

"bogus" failed to match

[0 matches returned, 1 item failed to match]
elaine27:~> ipm -m bogus
elaine27:~>
```

- -r <rows> "limit search results this many matches, default 1000"
  - If you expect a really large result, you'll want more rows, and a refreshing beverage.
- -s "script-oriented output"
  - write the data for each matching record glued together with vertical bars, '|'. May be more useful if you're dumping the data into a file or a script.
- -u "print this message"
  - The simple help screen again.
- -v verbose output
  - I'll show you the results of: `ipm -v dru-macbook-en`

IPM Samples

- Find an IP thief:
  - `ipm -d 5 [ip number]` to get all the hardware addresses used by that IP number over the past 5 days, assuming it's a recent "theft."
    - `netdb node info [node name]` to see what HW address is "supposed" to be used by that IP, if it's in the record. Or use whois.
  - `ipm [suspect hw address]` to get a history of the suspect's IP use, is it hopping? If it's using IP numbers in sequence, it might be hacked. Maybe they fat-fingered their IP number?
    - `whois -h whois [suspect hw address]` to see if it's registered and to find the administrator(s) or user to yell at them.
- IPM gets its data after a few hours, so you may have to wait to get accurate results.

More IPM Samples

- Find all the ip numbers used in your network in the last day: `ipm -d 1 171.64.[your net].%`
  - you can also use CIDR prefixes (`ipm -d 1 171.64.20.0/24`)
- Follow a roaming laptop for a week: `ipm -d 7 [hw address]`
- Your roaming range is .150~.169, who's been using it today?: `ipm -d 1 171.64.x.15%` and `ipm -d 1 171.64.x.16%`
- Find the IP history of an old computer: `ipm -d 2000 [hw address]`
- Find a "borrowed" or stolen piece of equipment: `ipm [ip address]` to get the HW address if you don't have it, then `ipm -d 1 [hw address]` then ping it to see if it's live. You could write a script that runs every day and uses `ipm -m -d 1 [hw address]` and emails you if it ever gets a hit. We've only actually found one stolen laptop this way, but we get asked a lot.

SUNet Reports

- Found on https://www.stanford.edu/group/networking/dist/sunet.reports/ which is linked of the main networking web page at http://networking.stanford.edu
- The one you'd use the most: "Check a specific DHCP/Bootp client": http://dhcplog.stanford.edu:9696/manage/dhcplog/check_db
- Are you running out of roaming DHCP numbers? "Dynamic DHCP address utilization": https://www.stanford.edu/group/networking/dist/sunet.reports/dynDHCP.list shows you the last 24 hours of use.
- Say the authorities are after you for hacking done by someone on your network at a specific time, but they've moved on and someone else has that IP number now? "List DHCP client given IP and time" at http://dhcplog.stanford.edu:9696/manage/dhcplog/who_had is very hard to use, but is the only way to get this information.

Check a Specific DHCP/Bootp Client.

- Search by name (no wildcards) IP address (can use wildcards to search for a whole IP range) or Hardware Address (must be complete).
- "Search by name" attempts to find all HW addresses associated with that name and gets results. This is useful for a laptop with both a wired and wireless interface if you want to see the results of each.
- "Search by IP address" will find all HW addresses that have used DHCP to get that IP address, which is useful for the history of a roaming address. Also, you can use wildcards (*), to search for all the activity on your whole network. Although messy, that can tell you quickly if DHCP is working or not on your network, which can help troubleshooting.
- "Search by Hardware Address" doesn't care what format 0000.0000.0000 or 00:00:00:00:00:00 or dashes, etc. but it must be a complete HW address, wildcards don't work.

DHCP client search, what's it all mean?

- At the top will be a summary that most people ignore of the most recent activity, which is often all you want to know: The date and time of the last request, type (DHCP or BootP), gateway (the router that passed your request to the DHCP servers), the status (you hope for "found") and the IP number and name that you received, if it worked.
- After that is the detail of all that's ever happened, which often causes fear and confusion when people first see it.

Assuage my fear and confusion!

- Here's all you get, in sequence, and what they mean.
- Discover: This will only ever have two lines, one for each DHCP server (dawn and dusk), since your requests are always sent to each server and you always get two replies. Discover means you've sought out a DHCP server, which, being a normally non-routed ethernet broadcast, is forward to the DHCP servers by the router, which is why you see the router's IP number in the last column.
- Offer: This is the history of all the IP numbers our DHCP servers have offered you, which for a roaming laptop can be a large list.
- Request: You then ask the DHCP servers if you can use a specific IP number, hopefully the IP number you were just offered by the servers. You'll often see 10.x or 192.168.x IP number here, which means some other DHCP server has offered an IP number to you and you want to use it.
  - *(continued)*

I'm less frightened and confused now...

- ACK: Acknowledgment from the server that you may use the IP number that the server gave you that you confirmed you wanted to use. How polite!
- NAK: Our DHCP servers saying you may not use an IP number, often these are the 10.x or 192.168.x numbers handed to you by a rogue DHCP server on your network. This is how you quickly determine that there is a rogue DHCP server on your network, finding it isn't so easy. You'll see regular Stanford IP numbers here too: when you wake your computer from sleep it will usually try to re-use the last number it was given (going straight to "Request" bypassing "Discover" and "Offer," and here the server is saying that number is no longer valid for this network, which usually means you've roamed to another network while your computer was napping.
- RELEASE: This is the client releasing the IP number back to the servers, which is quite rare.

DHCP Log Search Examples

- Look up a node with multiple interface entries:
  - Either look up by node name to see them all, or by individual HW address to each interface.
- Look up every node in your network range:
  - 171.64.20.* and wait a long time .
  - If you know the roaming range, you might be able to reduce the size of the result, i.e. 171.64.20.24*
- Requests?

List DHCP Client given IP and time.

- At http://dhcplog.stanford.edu:9696/manage/dhcplog/who_had
- Format: aaa.bbb.ccc.ddd yyyy-mm-dd:hh:mm
  - It's very picky about the time and date format. Use 2-digit months (01, 02, etc.) and 24-hour time
  - Examples: To find who was using 171.66.33.11 at 2:30 on 12/13/08: 171.66.33.11 2008-12-13:14:30
- Requests?

Questions? More examples?

- Inquiring mind wants to know...

A copy of this has been sent to the Tech Briefings group, it can be found on their web page:
http://www.stanford.edu/group/itss-customer/ip/techbriefings/