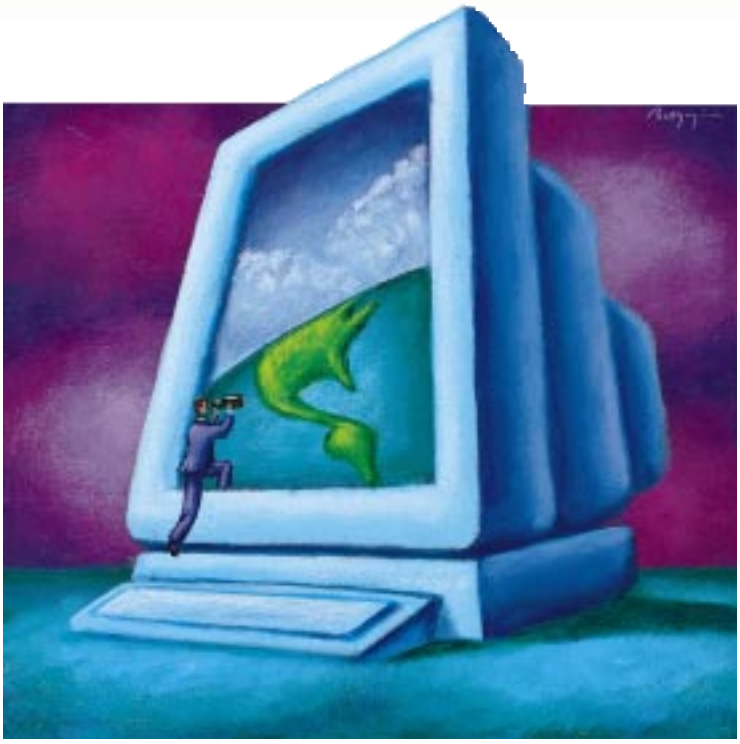
by S. Lee Henry



JAMES BOZZINI

The Lay of the LAN

Imagine yourself sitting in front of a Sun workstation. It's situated inside a bland cubicle with absolutely nothing to make you think a human has ever worked in this spot. No one else is around, but someone is logged in and an open terminal window is tempting you to investigate the system and network, which appear to be at your beck and call.

It reminds you of all those times you went to customer sites expecting to get some work done, but there was no one around who could explain to you even the simplest things about how the systems were connected, how large a network it was connected to, or even what services were provided by other systems or by the workstation on which you were supposed to be working.

With no one else around and no idea what you're expected to do, you decide it's time to "let your fingers do the exploring" and see what you can figure out while you wait for someone to show up and tell you what you're supposed to be doing.

Twenty Questions

There are a lot of questions you'd be asking if someone were around to answer. You start making a list of some of the things you might want to know. Let's see:

1. What operating system is running?
2. What is the system's name?
3. What naming service is running?
4. If NIS or NIS+ is running, what is the name of the master server?
5. If DNS is running, what name servers is it binding to?
6. What printers are available?
7. Are there user accounts on this system?
8. When was the system last backed up?
9. Who's logged in? Who logged in last? Who uses this system most often?
10. How much disk capacity is there? How much swap? How much memory?
11. What file systems are being made available for other systems?
12. What file systems are being mounted from other systems on the network?
13. What type of network cabling is in use?
14. How heavy is network traffic?
15. Is email received directly on this system or is there a mail exchanger?
16. What applications are installed? Do they start up when the system boots?
17. Are disk quotas in use?
18. Who knows the root password?
19. Is the system heavily loaded?
20. What SCSI addresses are in use?

OK, let's start sniffing around on this system and see what we can learn.

1. What operating system is running?

From the look of the screen, it seems CDE (Common Desktop Environment) is running. That suggests we're running Solaris 2.5 or better. We can quickly `cat` the `/etc/motd` file or, if this has been replaced by announcements about the company's chili contest, look at the bottom of a `man` page. But the easiest thing to do is to use the `uname -r` command,

which will tell us the OS release:

```
boson% uname -r
5.5.1
```

2. What is the system's name?

Duh! Because we're obviously logged in with a `/bin/csh` shell, the name is part of the prompt (by default). If we'd been logged in with the Bourne or Korn shells, we could have used the `uname -a` command and listed more information about the system:

```
boson% uname -a
SunOS boson 5.5.1 Generic sun4u sparc SUNW,Ultra-1
```

This tells us the system is running Solaris 2.5.1, is called `boson`, and is a SPARC system of the `sun4u` class; an `Ultra-1`, in fact.

3. What naming service is running?

This is a little more interesting. You could, after all, send a note back to the office if the system can resolve host names from the "real world." Checking whether it's running NIS or NIS+ would help us figure out most of the information we'd like to know. If it's running NIS, it should be able to handle this:

```
boson% ypwhich
ypwhich: can't communicate with ypbind
```

OK, so much for that. Let's try NIS+ by seeing if we can use the `nisls` command:

```
boson% nisls
PARTICLE.PHYSICS.:
org_dir
groups_dir
```

Particle physics, huh? No wonder there's no one here. They're probably out chasing quarks. No, they're probably just taking a very long lunch. We can look at the `/etc/nsswitch.conf` file to see whether we're using local files or NIS+ tables to resolve host names. Or DNS! We might be running DNS as well.

```
boson% grep hosts /etc/nsswitch.conf
# "hosts:" and "services:" in this file are used only if the
#hosts: nisplus [NOTFOUND=return] files
hosts: nisplus files dns [NOTFOUND=return] files
```

Aha, it seems we are running DNS. That's good. We can probably log into the server back at the office to check email and send a message to the boss. Maybe *he* knows why we're here.

```
boson% cat /etc/resolv.conf
domain particle.physics.sci.org
nameserver 123.123.2.1
nameserver 123.123.3.1
```

Hmm, there are two name servers, but no one bothered to include the names in the `/etc/resolv.conf` file. That's odd. Anyway, we should have no problem telneting to the office if this place is on the Internet. Maybe we should run an `nslookup`:

```
boson% nslookup world.std.com
xxx
xxx
```

4. If NIS or NIS+ is running, what is the name of the master server?

If we had gotten an answer to our `ypwhich`, we'd already know this. Let's try the `nisstat` command:

```
boson% nisstat
Statistics for domain PARTICLE.PHYSICS.:

Statistics from server : TOPQUARK.PARTICLE.PHYSICS.
Stat root server' = ON'
Stat NIS compat mode' = ON'
Stat DNS forwarding in NIS mode' = ON'
Stat security level' = 2'
```

5. If DNS is running, what name servers is it binding to?

See question three.

6. What printers are available?

Because we're running Solaris, the best way to list printers is to use the `lpstat -a` command. However, that still won't tell us whether we can actually print to all of the printers listed. We could be listed in a file for denying printer access. After all, who'd trust someone who goes off for a long lunch and leaves themself logged in? Anyway, let's go ahead and take a look at the printer list:

```
boson% lpstat -a
scribe accepting requests since Fri Jan 3 17:00:32 EDT 1997
ps accepting requests since Mon Oct 7 11:11:11 EDT 1996
```

7. Are there user accounts on this system?

There are a number of ways to check this. First, check to see if there's a mounted `/export/home` and if it's local. Otherwise, we can see if there's a `/home` and if there are any file systems automounted from somewhere else. We could also check `/etc/passwd` to see where locally defined users have their accounts, or we could list the contents of the NIS+ table `passwd.org_dir` to see where users defined in NIS+ have their home accounts.

```
boson% ls /export/home
danielle  eric   mallory  onowa  slee  vail
```

```
boson% niscat passwd.orgdir | awk -F: {print $6}'
/home/boson/danielle
/home/boson/eric
/home/boson/mallory
/home/boson/onowa
/home/boson/slee
/home/boson/vail
```

Perhaps this is a much smaller organization than we thought. It looks as if the accounts are all local to this machine.

8. When was the system last backed up?

We won't know the answer to that question unless the `/etc/dumpdates` file is updated when backups are done with `ufsdump`. It might be the case that some other software is used that may or may not update this file. Let's check anyway. If we're going to end up doing any work on this system, it would be nice to know if it was backed up recently.

```
cat /etc/dumpdates
/dev/rdsk/c0t2d0s7   0 Fri Apr 11 23:34:09 1997
/dev/rdsk/c0t2d0s7   5 Tue Apr  8 22:06:00 1997
```

With entries like these, it looks like full and incremental backups are done fairly regularly.

9. Who's logged in? Who logged in last? Who uses the system most often?

If we say `who`, we're going to see who is logged in now and who left their session unattended. Let's run `who` against the `/var/adm/wtmp` file to get an idea of recent logins along with the current one:

```
boson%
who /var/adm/wtmp | tail -3
peterpan  pts/3    Apr 10 09:17   (neverneverland)
suzyq     pts/0    Apr 11 10:05   (nextdoor)
eric      console  Apr 11 13:13
```

So, someone named Eric is logged in now, and some other users we didn't see in the NIS+ table have logged in from other systems. Let's see if this Eric guy is the one who normally works here:

```
boson%
who /var/adm/wtmp | tail -1000 | awk {print $1}' | sort \
    awk -f count_same | sort -t: -n +1 | tail -3
root:13
suziq:51
eric:794
```

Oh, by the way, I forgot to tell you that I was writing that little `count_same` script while you were nodding off on the last page. It counts consecutive lines that are the same. It looks like Eric is the primary user.

10. How much disk capacity is there? How much swap? How much memory?

I don't know about you, but I'm getting a little tired of adding columns of numbers that are some number of 512-byte blocks, or some number of kilobytes if I remember to use the `-k` option with my `df` command. Let's toss an `awk` script together to add any arbitrary column of numbers for us.

```
#
{
TOT = TOT + $COL
}
END { print TOT }
```

That was easy. Now let's count up our disk space:

```
df -k | grep /dev | awk -f add COL=2
1826834
```

OK, sliding the decimal point into the right place, I'd say that's just about 2 GB. I could use that much space myself. I'm glad I don't have to share with Eric, Mallory, Vail and the others.

To Be Continued...

Oh, sorry, looks like someone's trying to tell me this column is long enough already. Guess we'll have to answer the rest of the questions next month.

***S. Lee "slee" Henry** is on the board of directors of the Sun User Group and is temporarily living a bi-coastal life with one foot just outside the nation's capital and the other in California. Anyone with nothing better to do and room in their trunk should write to* `slee@cpg.com`.