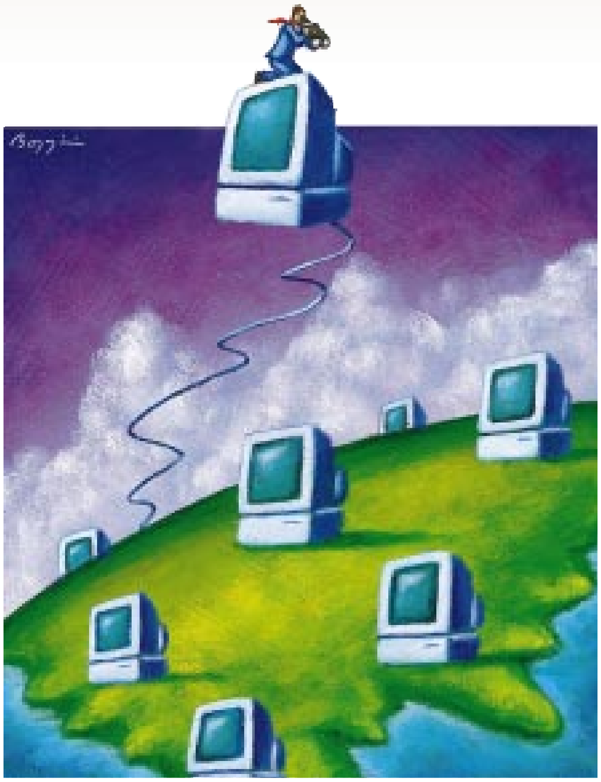
Systems Administration

by S. Lee Henry



JAMES BOZZINI

The Lay of the LAN, Part 2

When we left off last month, we were using a simple `awk` script to calculate disk capacity on the system we found ourselves standing in front of. We asked ourselves a list of questions that would give us a good base of information regarding the configuration of the system. The questions we didn't get around to answering were as follows:

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 cable is in use?
14. How heavy is network traffic?
15. Is email generally 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?

Recall that the fictitious system we were examining was running Solaris 2.5.1 and was a Sun Ultra-1. In addition, it was running both NIS+ and DNS. There were a small number of users with local accounts.

11. What file systems are being made available for other systems?

Because we're looking at a Solaris system, the command to figure out if file systems are being exported and to which hosts is

```
boson% share
```

This command, without arguments, as shown here, lists the file systems that are exported (i.e., shared) along with the hosts (if defined) that have been given permission to mount. If there is no response other than the next shell prompt, no file systems are being shared.

We may not know from the result of the `share` command whether the list of hosts contains any netgroups (groups of hosts) or only host names. We can check by looking at the `hosts` table and the `netgroup` table (if it exists) with the commands `niscathosts.org_dir` and `niscatnetgroup.org_dir`.

While looking at the file systems that are exported for sharing, we might also want to use the `showmount` command to generate a list of the systems that are mounting file systems from this workstation. If we want to know which systems are mounting a file system (e.g., `/export/home`), we can use `showmount -a` and pipe the output to a `grep`.

```
boson% showmount
fermion
orchid
```

If no file systems are exported, we'll probably get an error message ending in `RPC: Program not registered`, telling us that the NFS daemons are not registered with RPC.

12. What file systems are being mounted from other systems on the network?

This is easy to answer. We can simply use the `mount` command to view everything that's mounted and then visually eliminate the file systems that are mounted from the local system. Alternately, we can use `mount` and `grep -v` to restrict the display to file systems that are not local. The command `mount | grep -v "/dev"` should give us a list that's a little nicer to look at.

13. What type of network cable is in use?

If we are curious about the type of cable connecting us to the network, we might have to climb behind the workstation or under the desk and take a look at the cable itself. Most of the newer Sun systems will have a built-in UTP port that may or may not be the network connection in use. Further, the cable that attaches this workstation may or may not be representative of the network on a larger scale. It may be that a number of local systems connect to a UTP hub that subsequently attaches to a coaxial (e.g., thinnet) network somewhere beyond our view. The presence of any kind of transceiver will indicate that we are changing cable types.

On the grand scale, the network could be a mix of every variety of legitimate Ethernet cable, and there is now a way to determine this from the local connector.

14. How heavy is network traffic?

One of the best ways to gauge network traffic is to take a look at the number of collisions that are occurring. Because each Ethernet interface only concerns itself with its own packets, comparing the number of output packets with the number of collisions will give us a rough idea of how heavily congested the network is. If we see only a percent or two of output packets colliding with their network brethren, we can conclude that network traffic is fairly light. In heavy traffic, packets from different workstations are much more likely to be sent at the same time. If we see a large percentage of output packets colliding, we can conclude that network traffic is slowing down our system's performance with respect to network-based computing (e.g., resolving host names, updating NFS file systems and so on).

```
boson% netstat -I le0 10
        input  (Total) output
packets errs   packets errs  colls
740730  0      116137  1     25
```

Clearly, in this example, the percentage of collisions (25 out of 116,137) is extremely small.

15. Is email generally received directly on this system or is there a mail exchanger?

One thing we might do to determine the role that this workstation plays in handling email is to take a look at the `/etc/mail/sendmail.cf` file. This file may have a `mailhost` specified. If so, this host is used to send mail out and is likely to be receiving email for the local system as well. Because we're running DNS, we might want to check this file to see if there's an MX record defining a mail exchanger for our domain.

```
# major relay mailer
DRmailhost
CRmailhost
```

If the tag `mailhost` is used, we should check to see if this is the name (or more likely an alias for some host on our network). We can also use `nslookup` as shown here to determine if there is a mail exchanger defined for our domain and display its fully qualified name, if there is one:

```
nslookup
set querytype=MX (or whatever)
> highenergy.physics.com
Server: topquark.physics.com
Address: 192.1.2.3
highenergy.physics.com canonical name=flux.highenergy.physics.com
flux.highenergy.physics com preference=0, mail exchanger=flux.highenergy.physics.com
```

16. What applications are installed? Do they start up when the system boots?

This is a harder thing to determine but, generally, application software will be installed in `/opt` or `/usr/local`, at least on a well-managed Solaris system, or in file systems designated for particular data-intensive applications (you might, for example, find a `/oracle` file system). Perusing these directories will tell you a lot about the software installed on the system.

You can also take a look at the `/etc/init.d` directory to see if additional start-up/shutdown scripts have been added to the system. This will also answer the second part of our question dealing with software that is invoked on bootup. We might also look for new entries in files such as `/etc/services` and `/etc/rpc` (or the NIS+ equivalents). Most sysadmins adopt the practice of providing comments when they update these files to indicate the purpose of the added entries (e.g., `# The following lines added to support rblip tools`).

17. Are disk quotas in use?

Disk quotas can be used to limit the amount of space that a user is able to occupy on any particular file system, either by actual disk space used or by the number of files or both. Any file system that is managed with quotas will have a file called `quotas` at its base. This file will have an entry for each user for whom a quota has been established, indexed by that user's numeric UID. The file system must also have the quotas specified within the options field of the `/etc/vfstab` file.

Just knowing that quotas are in use doesn't tell us whether they are used across the board. Because there is no tie between `admintool` and the quota mechanism, new users will not automatically be set up with quotas and will have no quotas applied (i.e., unlimited access) unless a quota is specified.

18. Who knows the root password?

The best way of telling who has the root password is to examine the `sulog` file if it exists–only failures will be captured in the `/var/adm/messages` files.

Indications of successful `su` to root operations tell us these users have the root password. Others may as well, but unless we capture successful switch user operations, we won't know.

19. Is the system heavily loaded?

We can always assume that if the system is slow it is heavily loaded. However, there are so many reasons that a system can be slow that we shouldn't be too quick to blame high CPU demand. Contention for disk accesses and slow network response can slow systems down. So can inadequate swap space or low memory.

If we run something like the `top` utility, we can get a handle on the number of processes waiting for the CPU as well as which processes are using most of the processing power. Alternately, we can take a look at disk performance. We already looked at network response by checking into collisions as a percentage of overall traffic, and we can check into swap and memory use as well with the `swap -1` and `vmstat` commands.

20. What SCSI addresses are in use?

The best source of this information is probably the `/var/adm/messages` file, because we don't want to take the system down to the `ok` prompt just to run `probe-scsi`. Disk SCSI addresses are clearly indicated in Solaris by their device names. The file system, `/dev/dsk/c0t3d0s6`, for example, is clearly on the disk with SCSI address 3. The SCSI targets of tape and other nondisk devices are not quite so obvious. The address `/dev/rmt/0c`, for example, doesn't give us any clues about the SCSI address in use. We can pull SCSI addresses, however, from the `/var/adm/messages` files by grepping on the word `target` as shown here:

```
boson% grep target /var/adm/messages*
May 19 12:28:53 boson unix: sd3 at esp0: target 3 lun 0
May 19 12:28:54 boson unix: sd4 at esp0: target 4 lun 0
```

Questions Answered

We've answered all our original questions. There are still many things that we might want to figure out once we know why our boss sent us here and why everyone who works in this room is taking so long to come back from lunch. Once they've returned, however, we will likely be ready to go to work.

__S. Lee "slee" Henry__ recently took off from the Washington, D.C., area and headed toward Los Angeles with a trailer full of books, musical "toys" and other personal stuff. Three days and three exploded tires later, she arrived and started working as a security services engineer for Infonet, a global networking company, in El Segundo, CA. You can send email to `slee@cpg.com`.