

Chapter 1

Network Hardware and Operating Systems

Magic through black boxes and cables

Science fiction author Arthur C. Clark once said that to anyone who could not comprehend it, any sufficiently advanced technology seems like magic.

That, of course, makes *you* the magician. Naturally, everyone in the office begs you for the magic words to make their mysterious machines work.

Of course you know better. Remarkable as they may be, all those black boxes contain are just millions of little switches saying yes and no.

Cables are not conduits for alchemy, but simple pathways to get electrical impulses where they're going.

This chapter covers vital but nevertheless non-critical elements of the network built around the Pima County Voter Registration System. We look at the network, hardware and operating systems (as configured at this writing) on which the applications run.

We hold off for later chapters the humongous database running on those awesome Solaris boxes.

So roll up your sleeves and let's get down into the nuts and bolts of the network.

The Voter Registration equipment and application



The Pima County Voter Registration program (affectionately known as Reg-E for Registration and Elections) is a Windows application called VOTER.EXE.

The executable file resides on the NetWare 4.1 server *RECORDER_APPS*, which is installed on a Dell PowerEdge SP590 PC in the Recorder's Office computer room.

The server runs a 90MHz Pentium® processor with 128 MB of RAM.

RAID on-line storage

The *RECORDER_APPS* server stores data in 4GB of on-line hard drives from a RAID (Redundant Array of Independent Disks) Level 5 configuration of three 2GB hard drives. The additional 2GB provide the redundancy factor that protects the RAID storage if the primary hard drives crashes.

When a user logs in to Reg-E on the network, she authenticates herself with her user name and password. The *RECORDER_APPS* network server reads the user's network login for identification and authorization levels. The user encounters no login screen, although you can install one to provide another security door.

Ethernet connections

Three Ethernet adapters are installed in the *RECORDER_APPS* server.

They provide the primary NetWare office connection, an administrator's direct line and two data routes to the outside world.

Main office server

The first connection is a 10/100 PCI adapter.

This adapter links *RECORDER_APPS* to the County Recorder's staff. It is via this link that this server becomes the primary connection point on the network. The staff logs into this server to start the day. All other servers in the office also connect to *RECORDER_APPS*.

This connection runs NetWare IPX and TCP/IP protocols. However, no printers or modems connect directly to *RECORDER_APPS*. Those attach elsewhere on the network.

Administrator's direct link

The second EISA 10/100Mbps board is also in a PCI slot. This is the network administrator's back door into the database server.

Because the Administrator's station is a Sun Sparc computer running the Solaris flavor of UNIX, this link only runs TCP/IP.

Think of this connection as a direct line to the key server. It diagnoses problems in the event that the standard connections fail.

Fiber optic links to the outside world

The third Ethernet adapter is a FDDI board with DAS connectors.

The two connectors on this fiber-optic line move data at a *minimum* of 100Mbps. They provide dual pathways for data to connect to the Internet and the rest of the outside world.

The first of these lines is a direct route out. The other runs through the county backbone and from there to outside data.

Emergency backups

Emergency preparedness can seem like paranoia—until the emergency happens. Then it just seems like common sense.

Computers are machines. Machines can fail. Be prepared.

In the event of a system crash, reinstall the *RECORDER_APPS* server from backup tapes to restore the system.

WARNING: *If you have no **current** backup available, you have no alternative but to completely restore the system from scratch.*

Reg-E takes to the Web

A vast amount of public information is entrusted to the County Recorder's office. So it was inevitable that the non-confidential portion of this data be made accessible to the public on the World Wide Web.

The Web site is not currently in use, but a server is in place for that purpose.

Reg-E's Web server is a Sun Ultra™ 2 computer with network machine name *web*. The web application is Netscape Commerce Server 1.12 running on the Solaris 2.5.1 operating system.

The *web* server has a 10/100 Ethernet adapter that connects it to a 100 Mbps hub, and from there to the rest of the system.

To create or edit this or any Web page, you need a working knowledge of HTML (Hyper Text Markup Language), a simple but essential system of text tags to display text and graphics on Web browsers such as Netscape Navigator, Microsoft Explorer and others.

Firewalls and selective communication

In an environment where both public and private information are stored, a firewall separates publicly available data from confidential information. It restricts unauthorized users from private records.

At the same time, the firewall allows only those people in the office who are authorized to connect to outside computers. So only those people with authorization can link to www.dirty-mind.com and other web sites of questionable professional value.

In a frenzy of creative designation, the firewall server is named *firewall* on the network. Like the *web* server, this runs on a Sun Ultra 1 computer under the Solaris 2.5.1 operating system.

This computer connects to the network with another 10/100 Ethernet card with an S-bus expansion board.

The computer is equipped with a Netra 3.0 software package with three other applications that have little to do with operating a firewall, but much to do with internal networks meeting the outside world. While it's at those tasks, *firewall* is also a repeater, amplifying the datastream before it moves down the line.

Let's have a look.

Playing Post Office

Since *firewall* is the barrier/connection between internal and external systems, it's in the perfect place to collect e-mail routed between the Recorder's Office and the outside world.

In fact, that's just what it does. The server runs POP (Post Office Protocol) Level 3. The recorder's staff members who have **outside** e-mail privileges log in here to send and receive those messages through this server. E-mail within the office routes through the NetWare internal network.

Authoritative Domain Name Server

Staff members with privileges to connect to outside sources are usually looking for information on the Internet. When they type in an Internet address on the browser, these words are converted to a numerical Internet address.

A Domain Name *Server* (DNS) looks up and converts back and forth between domain names and numerical IP addresses. A Domain Name *Client* requests the information.

Our *firewall* server is both client and server.

What's more, with the Recorder's Office responsible for naming the machines within its domain, this is an **authoritative** server. The actual Internet address names it distributes are correct, because this is the point where those addresses are assigned and authorized.

But do you have the exact time?

Finally, to synchronize databases and network lookups, we make sure everyone is on the same page, chronologically speaking.

To do that, *firewall* is a Network Time Protocol (NTP) server, setting the precise time for the other servers around the office.

Just how it accomplishes that task is a marvel of electronic computation and communication.

Firewall is a Stratum 3 server. It gets its time from a Stratum 2 server at UCLA in Westwood, California. The computer checks the time signal at the Stratum 2 server, calculates the time for the telephone signal to travel to Tucson and for the computer to process the calculation, then adjusts the time accordingly.

In turn, the NTP server at UCLA gets its time from the US Naval Observatory master clock in Washington, the Stratum 1 server which averages the time between several incredibly precise atomic clocks.

Meanwhile, back at the Recorder's Office, *firewall* passes its precise time to the network's other UNIX servers, making them Stratum 4 servers.

You can get the precise time from any PC logged on to the network. From a DOS prompt, type

systemtime recorder_data

and press enter and then read the time. The PC's clock resets to the correct time.

Next up

Next we move on to the heavy hitter, the database of voter registration information and images. This is the heart of the operation, so this would be a good time to make an effort to stay awake.

