BUILDING A TEMPORARY NETWORK IN A HURRY

There are any number of reasons you might need to build a temporary network in a hurry. Drawing from their experience in putting together the InterOp ShowNet, the authors offer tips in what to consider when installing a temporary network.

by Karl Auerbach, Empirical Tools and Technologies and John McMahon, TGV, Inc.

Karl Auerbach is President of Empirical Tools and Technologies, a recently formed software company that is developing a new category of proactive network integration tools. John McMahon part of the development team at TGV, Inc., creators of MultiNet, a TCP/IP solution for VMS networks. Both authors have been extensively involved in setting up and running the InterOp ShowNet over the years.

For various reasons, a corporation or institution may need to build a temporary computer network in a hurry. Sometimes you can plan ahead and foresee where and when a new network may have to be "thrown together," such as when a company moves its offices. In other cases, the need is triggered by unplanned external events, such as natural disasters. In these cases, the network will merely serve as a temporary expedient, but you still have to apply many of the laws of "good networking" to make sure that even a temporary installation goes in smoothly and runs properly.

We have accumulated some expertise in putting together "instant" networks from assembling the InterOp™ ShowNet™ over the years. One of the first things we learned was that even temporary networks are far from "instant." However, we also learned that the skills applied to creating the ShowNet for InterOp are readily transferable to the real world. So here we will offer some of our insights into the hows and whys of designing and assembling a temporary computer network in a very short period of time.

Why is This Article Important to You?

Believe it or not, everyone should know how to build a temporary network. There are any number of unforeseen circumstances that will make it necessary for you to build a network in a hurry. Let's look at some hypothetical situations:

- Disaster recovery — Fires, floods, earthquakes, chemical spills, and other unforeseen disasters do occur. Sometimes they happen to just your building, and sometimes they are regional. Consider, for example, that both of the authors of this article live in Santa Cruz, Calif., an area that is still recovering from a large earthquake in 1989.

  In order to stay in business following any disaster, your organization will have to restore its operational infrastructure, including its computer systems and computer networks. Your company may be forced into temporary quarters for an unknown duration, and the network will have to move with it.

- Corporate expansion or acquisition — The corporate games of the '80s may be over, but companies still do grow and still do merge. And although senior management may have advance knowledge of an impending move or acquisition, the networking department is often the last to know. You need to be prepared. You may find yourself surprised with a demand for almost instantaneous network growth following some corporate consolidation.

- Trade shows — For high-tech companies, these are the epitome of the quickly built, temporary computer network. But what is the difference between a trade show network in a convention center and a disaster recovery network in a rented space? Quite simply, it is that the time and place of a trade show are foreseeable, but a disaster is not. The same kind of planning and preparations that make trade show networks workable also make other temporary networks functional.

The point is, you have to be prepared. What if you receive the following late night e-mail?

```
To:          John, Karl
From:        The Grand Poo Bah
Subject:  Drop everything else and do this immediately

John, Karl -- The company has just suffered a fire. All of our
computers have burned up. We've rented a warehouse and ordered a
few truckloads of computers, cables, and networking gear. It is
exceedingly important that you immediately turn it into a working
network.

(Please don't spend time wondering how you received this e-mail
despite the total destruction of your computer systems.)

              s/ G. P. B.
```

Welcome to The Stress Zone, an experiment in sleep deprivation. Be prepared, this kind of network installation is not for the faint-hearted.

Advance Planning is the Key

As with most things, advance planning will significantly help. Realistically, however, it is impossible to plan for all possible contingencies. Therefore, you need to be flexible, but flexibility also has its costs.

Principle #1 — Plan ahead and stay flexible; you must be prepared to deal with the unknown.

Corollary #1A — Design and build redundancy into everything. If you put all trust into any vital network element, Murphy's Law will make that element fail.

Corollary #1B — Understand that the construction effort and resulting network will be sub-optimal. It is exceedingly important to be prepared to accept retrospective criticism from non-participants who will state that the network you have built is wasteful and inelegant. Remember that the goal is to build a *working* network in an impossibly short time, not to build a perfect network.

Know What You Need To Do

Whether you are trying to develop a plan or are in the throes of a surprise implementation, it is very useful to know exactly what are your goals and non-goals.

Principle #2 — When you are implementing a temporary network your most valuable resource will be time. You cannot afford to waste time.

Corollary #2A (The Lazy Rule.) — Avoid doing anything not strictly necessary to achieve your express goals. It is much harder to apply the Lazy Rule than any other recommendation in this article. Your managers, vice presidents, presidents, friends, and even yourself will have pet projects that they will want supported by the network. In many cases, what you may think of as a pet project will, in fact, be critical to the healthy survival of the organization. In other cases you will be right in perceiving a project as trivial.

In planning and implementing any network you will be called on to make critical choices that will directly bear on the ultimate success or failure of the network, and often on the success of failure of the organization itself. In practice, this means that you ought to be somewhat liberal in accepting other people's opinions with respect to what are the critical missions of the network.

When we build a new network, our first step is to make sure we have a clear understanding what services our network is to provide, how extensive the network plan must be, and what external connections are required. For example, in constructing the InterOp ShowNets, the services always include TCP/IP, ISO CLNP, DECnet, IPX, AppleTalk, plus various routing protocols. These are usually hosted on a cable plant composed of 10BASE-T, Ethernet™, Token Ring, FDDI, and various point-to-point technologies. We are not particularly concerned what higher level protocols will be carried, since we are fortunate enough to have far more than adequate bandwidth for all reasonable purposes. However, we do need to engineer ancillary applications such as name services.

Principle #3 — The network will be bigger and contain more parts than you ever conceived possible.

Corollary #3A (The Oops Rule) — Unless you intentionally overbuild, you will almost certainly end up underbuilding.

Corollary #3B — Cables will be too short or too long, but never just right.

One of the apparently simple jobs is to create a bill of materials. However, it is amazingly hard to add up all the cable lengths, connectors, patch panels, and such. The reason for this is that an accurate estimate of materials depends of an extremely detailed network design. For example, cable runs will often be much longer than straight lines drawn on blueprints (and that often has an impact on technologies with cable length limits, such as 10BASE-T).

While planning or building it is easy to forget that you are building a temporary network. Being temporary, the design can avoid some of the niceties of a permanent installation. But it is quite surprising how many things which at first glance are merely adornments are actually quite necessary, especially given the controlled-panic that prevails when a temporary network is constructed and first turned on. For example, it is extremely important not to skimp on infrastructure for network monitoring, control, and repair. And proper cable labeling is as critical as always.

One thing to consider is the possibility that the temporary network will ossify into a permanent installation. (Every college and university in the country is still using ancient "temporary" buildings.) This is clearly a tertiary-level consideration.

Principle #4 — You can never review your plan enough.

Corollary #4A — Small flaws are often symptoms of big errors.

Mentally walk through every wire, every connector, and every device. Be especially careful to consider the correct sex of each connector — a sex mismatch almost always indicates a significant design flaw.

It is always "fun" to find that basic assumptions are not true. For example, we had always assumed that all RJ45 (8-wire) connectors were mechanically equal. They're not. Some have tabs on the sides (which we had to prune off using pocket knives). And some have shells which are too wide to be plugged in adjacent receptacles of a wiring concentrator or patch panel. One year, during ShowNet installation, we almost had a disaster when we unknowingly used RJ45s for stranded cable on the standard solid-wire cable.

In Silicon Valley we are fortunate enough to have "nerd supply" stores. These stores are open late and carry everything from Ethernet terminators to potato chips. Most parts of the country aren't so lucky and, as a consequence, it will be necessary to maintain a larger supply of spare parts and "just-in-case" tools and supplies.

Choosing the Appropriate Equipment

When we design the InterOp ShowNet, we typically have vendors lining up at the door to offer equipment. We can assure you that this is not a luxury. One of *our* goals with the ShowNet is to demonstrate interoperability across a wide spectrum of equipment. That is unlikely to be *your* goal.

When designing or building a private temporary network, you would be well advised to avoid unfamiliar equipment. Fair selection of vendors is a luxury to be avoided whenever possible. This will save considerable time, even if it means that your network doesn't contain the "best" equipment for the job. Time saved is far more important than network efficiency when installing a temporary network.

However, some new technologies that might save you time. Recent improvements in network management capabilities, including SNMP, can be quite useful. If you aren't in an emergency situation, it would be well worth the time and effort to learn these new technologies and incorporate them into your organization's current network. Then, as these technologies become familiar, they can be adopted into the temporary network plans.

Be sure that you can get the equipment you need when you need it. Getting equipment and supplies in hurry can be exceedingly difficult, especially if you are trying to use them for a limited period of time. And during a regional emergency situation, there will be strong competition for whatever equipment is available. Acquisition of the rights to use equipment is worthless unless you can actually gain physical access to that equipment when and where you need it.

You will need to be imaginative. Consider lease/purchase options or some arrangement with a manufacturer to offset any extra inventory costs that they may incur to ensure that you set a priority claim to necessary equipment. Also consider pooling arrangements with friendly companies in other regions of the country. It is unlikely that both companies would suffer from a disaster at the same time, particularly if they are in different regions, and the costs could be shared.

Design Considerations — Some Basic Rules

There are many ways to make your life easier, or harder, when building a temporary network (or any network, for that matter).

Principle #5 — Limit the range of error propagation.

Corollary #5A — Always use a hub-based technology and design.

Corollary #5B — Avoid coaxial cables and non-hubbed rings.

Corollary #5C — Minimize the use of bridges; maximize your use of routers.

Whether you use bridges or routers will often be dictated by the protocols you use. Some older technologies require bridges because they depend on a system in which every host can hear broadcasts and multicasts. These protocols are typically (but not always) ones that export NetBIOS services or are called "Network Operating Systems."

More modern protocol technology supports routers. However, routers are much more difficult to use than bridges. Rather than blindly adopting a routed or bridged technology, you should remember that you ought to use equipment with which you are familiar.

Use a segmented network approach. No matter how hard you try, the network will have problems. It is important to design the network so that these problems tend to be limited. The best way to build barriers against the spread of problems is to segment the network.

At the very least, use hubs and concentrators as the basis for your LANs rather than running multidropped coaxial cables. A good concentrator or hub will allow you to spot and disconnect any misbehaving hosts fairly quickly.

If your network protocols are reasonably well architected protocol suites (i.e., TCP/IP, ISO/OSI), you should plan for a routed architecture. Routers, although troublesome in themselves, tend to contain network misbehavior. Bridges, on the other hand, tend to propagate network malfunctions across the entire network. Try to avoid bridges.

It also pays to avoid coax; use 10BASE-T instead. Unshielded twisted pair wiring is by far the most reliable, most tractable, and least expensive cabling medium. Some of the newer shielded twisted pair is also relatively tractable. By contrast, coaxial cables and some the highly overdesigned shielded twisted pair cabling are extremely difficult to use.

Try to use 10BASE-T or other schemes that use RJ45 jacks at the ends of the cables rather than extremely complex connectors (such as those found on some Token Rings). 10BASE-T is easy to set up, it's inexpensive, it has an almost 100% interoperability rate with equipment from various vendors, and it is extremely robust in the face of electrical interference.

In addition, 10BASE-T has a little-mentioned but extremely useful characteristic — the link state test. Most 10BASE-T MAUs have an LED that lights when it is correctly communicating with a peer at the other end of the wire. This LED serves as a good alternative to specialized test equipment. If you are buying 10BASE-T gear, try to spend the few extra dollars to get MAUs and interface boards that have a visible link state indicator LED. We also recommend that you use MAUs that have transmit and receive lights to indicate network activity.

One final point with respect to wire. There are various cable "levels" rated from 1 to 5. We have found that the level 5 unshielded twisted pair (e.g. AT&T 1061) is quite superior. It can carry a 10BASE-T signal, for example, significantly further than can lesser grades of UTP.

Also be aware that for relatively short runs (e.g. 100 feet or less for 10BASE-T), it is quite reasonable to use standard 25-pair telephone cables with the standard large connectors. You can purchase "octopus" cables from many vendors (ModTap, Nevada Western, etc.) to splay out the 25-pair into six RJ45 connections.

With RJ45-based wiring, it is desirable to terminate all runs on patch panels rather than using punch-down blocks. 10BASE-T allows for a reasonably high number of patch panels. But beware, most cable faults occur within a few inches of the connector.

Build Your Working Network Off-site First

It is extremely important to build as much of the infrastructure you need in advance. We have found that no matter how much planning you do, it's not until you really get down to doing the physical infrastructure that you find errors. Building the infrastructure in advance is also important to make sure that everything works, is properly labeled, mapped, and ready to parachute in.

If you are dealing with a disaster recover plan, keep the pre-built network warehoused well off-site. It won't help you with disaster recovery if all your redundant equipment stored in the back room is lost in the same earthquake that destroyed your office. Also, work a deal with other companies to share hardware in case of disaster — you scratch my LAN and I'll scratch yours.

It is essential to create VERY good network blueprints.

Principle #6 — Document and label everything.

Corollary #6A — Documentation and labels must be comprehensible to someone who is exhausted and who is not one of the architects of the design.

Corollary #6B — Label all cables at both ends twice, once near the connector and again 10 feet back.

Only one things is more frustrating than to be staring at the end of a cable you designed and wondering where the other end is: Staring at the end of a cable that someone else designed and wondering where the other end is.

In addition to superb cable labeling, it is important to keep a detailed notebook. Actually, keep many copies of that notebook. This notebook should include everything anyone would ever want to know about the network, including a total cable inventory, an up-to-date list of suppliers and contacts, equipment manuals, installation and configuration cookbooks, etc.

Prepare a configuration recipe for every device on the network. Put a copy into the design notebook and paste a copy onto the appropriate device. (It goes without saying that you ought to preconfigure as much of the hardware as is practical.)

Know Your Tools

Make sure your tools match your needs — have crimping tools, screwdrivers, etc., available. And make sure you have the right tools for the job. We recommend that you use connectors and equipment that you can deal with using normal hardware-store tools. For example, avoid the inexpensive $0.35 crimp-on RJ45 connectors. Instead use the $3 versions that you can build with a pair of channel-lock pliers. Similarly, avoid equipment that uses Torx™ screws and the like.

Remember that tools walk away when you aren't looking. Buy lots of spare tools.

In installing the ShowNet, we have found the following to be worth their weight in gold:

- electric screwdrivers (with Phillips, straight blade, and 1/4-inch hex bits)
- small screwdrivers (Phillips and straight blade)
- small channel lock pliers
- small side or diagonal wire cutters (cheap ones)
- small flashlights
- gaffer's tape
- walkie-talkie radios (real ones, not toys) with lots of spare batteries.
- fanny packs

In addition to those listed above, you will need various specialized network tools.

When building cables, for example, you will need a cable tester to look for the most common form of error, miswiring. These testers cost a few hundred dollars. There are more expensive testers, costing a couple of thousand dollars, which also perform electrical tests. In our experience, you will often need the former type but only rarely the latter. Our experience proves that unshielded twisted pair cables are either good or very bad, rarely marginal. We have found that the 10BASE-T link status is a good alternative to the more sophisticated testers, but we always have a sophisticated tester handy just in case.

If you follow our advice and use hub-based technologies, you won't need Time Domain Reflectometers.

If you are using fiber optics, you may need specialized tools. And if you are using fiber, be especially certain to keep things extraordinarily clean. Avoid dust at all costs. Use the dust caps!

It is important to see whether the network is carrying packets. Simply looking at the receive LED on a MAU is often proof enough, but in many cases you need to delve deeper. To do this you will need a packet monitor, such as LANwatch from FTP Software, Lantern from Novell, or a Sniffer from Network General. We personally prefer to use versions that can run on a battery powered notebook computer.

Similarly, some SNMP based tools can be useful. These range from sophisticated engines such as SunNet Manager to more simplistic (but sometimes just as useful) tools such as FTP Software's "mon" program (the sole job of which is to tell you which hosts seem to be responding on the network.)

Once you have done the simple job of getting a working cable plant, you will begin the hard job of dealing with network layer protocols and above. For this you will need not only packet monitors, as mentioned above, but toolsets, such as those from Empirical Tools and Technologies. Empirical's toolset, for example, are designed to be highly portable so they can easily be carried to random places on the network. Empirical's tools are also designed to perform a wide variety of active and passive diagnostic tests, evaluating the state of the network's upper layer protocols and the configuration of hosts and other network devices.

Don't Be Afraid to Ask for Help

This kind of network installation is very specialized. If the current systems administration staff can't handle it, be sure you have contractors and vendors available who can handle it. Be sure to find these people well BEFORE you need them.

Once you have your equipment list together, it is a simple matter to go to the vendors and seek out the experts among their development and support staffs.

Other sources of support may be a little harder to find, but there places you can find network gurus. One logical source is trade shows and technical conferences. Collect business cards from the gurus walking the show floor, feel them out about their areas of expertise, and see if their availability in case of emergency. You can also find experts on forums on various computer bulletin boards and the Internet. Set up your own network of contacts.

Also check your local telephone book. Find local integrators and resources and make sure they are available when disaster strikes. If you gain a commitment from them in advance, they will be available when you are trying to recover from flood or fire instead of working on someone else's network.

Make sure you write down the names and contact information for vendors and consultants and keep them in your master notebook. In addition to Internet addresses (which will be hard to access without your network), be sure to keep telephone numbers, beeper numbers, and other contact information on file. Be sure to review your contact information periodically to make sure it's current.

Testing the Network

Once the network is installed, there are specific applications and protocols you can use to verify connections and perform some basic troubleshooting:

Ping — Ping uses ICMP (Internet Message and Control Packets) Echo messages to "bounce" data packets off of a remote host., making it an easy, simple-to-use function to test connectivity between nodes. Also, since every ICMP Echo packet is numbered, it is possible to identify connections where packets are dropped or duplicated. Ping will keep track of the time a packet takes to travel round trip as well, which can be useful in identifying bottlenecks in your temporary network. The "flood" option available on many PING commands can be used to generate heavy traffic along a network path, which can be useful for stress-testing a network.

The following is a sample of a Ping session between two good nodes:

```
$ PING YOYODYNE.COM
PING YOYODYNE.COM (89.0.0.70): 56 data bytes
64 bytes from 89.0.0.70: icmp_seq=0 time=10 ms
64 bytes from 89.0.0.70: icmp_seq=1 time=10 ms
64 bytes from 89.0.0.70: icmp_seq=2 time=0 ms
64 bytes from 89.0.0.70: icmp_seq=3 time=10 ms
64 bytes from 89.0.0.70: icmp_seq=4 time=0 ms
64 bytes from 89.0.0.70: icmp_seq=5 time=0 ms
<Control-C>
----YOYODYNE.COM PING Statistics----
6 packets transmitted, 6 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 0/5/10
```

The following session shows how Ping can be used to reveal packet duplication:

```
$ PING 89.0.0.255
PING 89.0.0.255 (89.0.0.255): 56 data bytes
64 bytes from 89.0.0.93: icmp_seq=0 time=50 ms
64 bytes from 89.0.0.66: icmp_seq=0 time=50 ms
64 bytes from 89.0.0.112: icmp_seq=0 time=60 ms
64 bytes from 89.0.0.111: icmp_seq=0 time=60 ms
64 bytes from 89.0.0.87: icmp_seq=0 time=60 ms
64 bytes from 89.0.0.70: icmp_seq=0 time=70 ms
64 bytes from 89.0.0.94: icmp_seq=0 time=70 ms
64 bytes from 89.0.0.114: icmp_seq=0 time=70 ms
64 bytes from 89.0.0.77: icmp_seq=0 time=80 ms
64 bytes from 89.0.0.90: icmp_seq=0 time=80 ms
64 bytes from 89.0.0.3: icmp_seq=0 time=80 ms
64 bytes from 89.0.0.1: icmp_seq=0 time=100 ms
64 bytes from 89.0.0.78: icmp_seq=0 time=100 ms
64 bytes from 89.0.0.71: icmp_seq=0 time=110 ms
64 bytes from 89.0.0.67: icmp_seq=0 time=110 ms
64 bytes from 89.0.0.93: icmp_seq=1 time=10 ms
64 bytes from 89.0.0.114: icmp_seq=1 time=10 ms
64 bytes from 89.0.0.90: icmp_seq=1 time=20 ms
64 bytes from 89.0.0.1: icmp_seq=1 time=30 ms
64 bytes from 89.0.0.94: icmp_seq=1 time=30 ms
64 bytes from 89.0.0.112: icmp_seq=1 time=30 ms
64 bytes from 89.0.0.3: icmp_seq=1 time=40 ms
64 bytes from 89.0.0.78: icmp_seq=1 time=40 ms
64 bytes from 89.0.0.111: icmp_seq=1 time=40 ms
64 bytes from 89.0.0.87: icmp_seq=1 time=50 ms
64 bytes from 89.0.0.67: icmp_seq=1 time=50 ms
64 bytes from 89.0.0.70: icmp_seq=1 time=50 ms
64 bytes from 89.0.0.66: icmp_seq=1 time=60 ms
64 bytes from 89.0.0.77: icmp_seq=1 time=60 ms
64 bytes from 89.0.0.71: icmp_seq=1 time=60 ms
<Control-C>
----89.0.0.255 PING Statistics----
2 packets transmitted, 30 packets received, -- somebody's printing up packets!
round-trip (ms)  min/avg/max = 10/57/110
```

Traceroute — Traceroute makes use of the TTL (Time To Live) Counter included in an IP packet to generate a router path between two nodes. Packets are sent out with an increasing TTL value, which causes routers along the path to respond back to the sender. This allows you to "see" how the routers are forwarding IP packets, and can assist in the diagnosis of broken routing or routing loops:

(The following is a sample of a Tr0aceroute across the Internet:

```
$ TRACEROUTE EISNER.DECUS.ORG
traceroute to EISNER.DECUS.ORG (192.67.173.2), 30 hops max, 38 byte packets
 1  TGV.BARRNET.NET (161.44.128.71)  10 ms  0 ms  10 ms
 2  UCSC.BARRNET.NET (131.119.46.7)  20 ms  20 ms  10 ms
 3  SU1.BARRNET.NET (131.119.1.5)  40 ms  10 ms  20 ms
 4  SU-B.BARRNET.NET (131.119.254.201)  10 ms  20 ms  20 ms
 5  E-NSS.BARRNET.NET (192.31.49.244)  20 ms  20 ms  10 ms
 6  t3-1.cnss9.t3.nsf.net (140.222.9.2)  20 ms  20 ms  30 ms
 7  t3-3.cnss8.t3.nsf.net (140.222.8.4)  20 ms  20 ms  20 ms
 8  t3-0.cnss16.t3.nsf.net (140.222.16.1)  30 ms  40 ms  20 ms
 9  t3-0.cnss64.t3.nsf.net (140.222.64.1)  60 ms  60 ms  60 ms
10  t3-0.cnss72.t3.nsf.net (140.222.72.1)  90 ms  90 ms  80 ms
11  t3-1.cnss48.t3.nsf.net (140.222.48.2)  100 ms  100 ms  100 ms
12  t3-0.cnss49.t3.nsf.net (140.222.49.1)  100 ms  110 ms  100 ms
13  t3-0.enss134.t3.nsf.net (140.222.134.1)  120 ms  100 ms  100 ms
14  mit2-gw.near.net (192.54.222.5)  110 ms  110 ms  100 ms
15  bbn1-gw.near.net (131.192.2.1)  110 ms  110 ms *
16  harvard-gw.near.net (131.192.5.1)  140 ms  140 ms  130 ms
17  prospect-gw.near.net (131.192.33.1)  130 ms  120 ms  110 ms
18  wpi-gw.near.net (131.192.60.2)  120 ms  140 ms  140 ms
19  decus-gw.near.net (131.192.81.2)  230 ms  110 ms  120 ms
20  EISNER.DECUS.ORG (192.67.173.2)  1050 ms  1120 ms  1080 ms
```

Telnet — The virtual terminal program, Telnet, can be used for connectivity testing, to access remote pieces of hardware (e.g. routers) ,and to drive certain basic TCP applications, such as FTP and Mail, when a real client isn't available.

SNMP — A significant amount of hardware is available that speaks the Simple Network Management Protocol (SNMP). Combined with a set of SNMP tools, such as a network management station or SNMP command line toolset, you should be able to monitor and adjust many of your network components from a central (and potentially remote) site.

Packet Analyzers — Most types of cabling can be tapped and monitored to read the packets as they are transmitted. Using a packet analyzer, the packets can be decoded to gain a better understanding of what is occuring on the network.

All of these testing tools can be built into a network "swiss army knife." This would normally be a notebook PC running a TCP/IP package along with the proper interfaces (Ethernet, Token Ring, etc) to connect to most parts of your network. With this combination of software support and hardware, you would have a luggable node that you can use to test and monitor any part of your network.

Tools — Make sure that you have the proper gear to test your various cables and connectors. If you are working with coaxial cable, a Time-Domain Reflectometer fcan be handly. Some feel a TDR is too expensive, but the testing unit will pay for itself the first time it saves you from scrapping an entire cable. Keep in mind that even the most reliable hardware can fail, and that the proper testing tools can save you from scrapping more of a broken network than you really need to.

Troubleshooting — Take a Number Please

As you get the network up and running, be sure you have a trouble ticketing system in place so you can swat your network bugs in their order of priority. To keep track of network problems, you should have a centralized location to log in problems. A trouble-ticketing notebook is one way to handle this. Each problem should be logged in, including the name of the person reporting the problem (so you can get back to them), a description of the problem, and how the problem was solved. Each problem should be logged in, and logged out, with appropriate records so, in the future, someone else can follow what was done.

It is also important to prioritize these problems so each of them is dealt with in turn. It's all too easy to get distracted by a new network fire that may have broken out. Perhaps the easiest approach is to use actual numbered trouble tickets, such as those with serial numbers used at carnivals. As each problem is resolved, the ticket can be discarded or stapled to the tracking sheet in the notebook to indicate the work has been completed.

When it comes right down to it, there's nothing mystical about putting together a working computer network in a short period of time. Many of the lessons outlined in this article were learned on the InterOp show floor from the school of hard knocks, but these lessons are readily applicable to any disaster-recovery or other installation situation you may encounter. The next time you have to install a complex network in a hurry, draw from our experience, be prepared to lose a lot of sleep, and make sure you apply common sense.

-30-

Artwork

3. Sample configuration chart - what do your tags need to say?

Here is an example of the kind of information you should attach to each and every piece of equipment.

```
Device:                    Rib 3 router
Name:                      rib3-router
Domain:                    nobody.com
DNS server:                127.0.0.1
Time server:               127.0.0.1
Default route:             N/A
IP address:                127.0.0.0
Subnet mask:               255.255.255.0
SNMP read string:    public
SNMP write string:   private
SNMP trap receiver:        127.0.0.1
Password:            A#elm34

     For more information contact:
     Fred at (408) 123-4567
```