Test & Measurement World, May 2000

Connect Instruments to the Corporate Network

Before you can connect, you must work with your network administrator.

By Bruce Fuller, Fluke, Everett, WA

Network administrators are the guardians of the corporate network. They're responsible for smooth, reliable, fast, and secure data flow, and they know the network's configuration, equipment, and bandwidth capability. But they may know little about taking measurements. Before you can place measurement instruments on your corporate network, you need to exchange information with your network administrator.

Take the first step by explaining your needs and how your equipment operates to your network administrator. Depending on your network type, network components, and network software, you may walk away with IP addresses, subnet masks, a default gateway address, and socket-port information to enter into your instruments. You'll also need to discuss physical connections such as cable and connector types. Regardless of the information you exchange, you'll find a visit with your administrator important before you connect your instrument remotely.

Explain Your Needs
Expect to tell your administrator:

• what physical connections and protocols your instruments use to communicate (TCP/IP protocol, in most cases, and the Ethernet physical network),

• what areas, departments, or people in your company need access to your instrument, and

• how much bandwidth (in kbytes/s) you expect to occupy. Bandwidth will depend on your scan speeds, number of channels, number of instruments, and how often you use your instruments. How you transfer data from your instrument—in real time or through file transfer—will also affect the network resources you need.

Your administrator can tell you if the network contains routers, bridges, gateways, or other devices that divide the network into subnets. If you intend to connect your PC and your instruments on different subnets, your administrator will need to verify that the network devices serving the subnets can route IP packets. You may have difficulty connecting your instruments to some older Novell networks; the network hardware may contain devices that route only Internet Packet Exchange (IPX) packets, which use a proprietary protocol. In this case, you may need to limit your operations to one subnet and forgo routing or else invest in a router or gateway capable of routing multiple protocols.

Your instrument and your PC need IP addresses to communicate over a network. IP addresses use the following format: XXX.XXX.XXX.aaa. The three "XXX" groups represent network class and ID values. The last portion (aaa) is the host ID and has a range of 0 to 255. Each instrument you place online, as well as your computer, will have a unique host ID number. This identifies each instrument and computer as a unique host and prevents communication conflicts. Depending on your network, you may be able to use your instrument's default address set at the factory. You also may need an IP address for your computer.

If you have subnets in your network and they fall between your instrument and your computer, you may receive a subnet mask assignment from your administrator. Subnet masks use the same format as IP addresses. By using the subnet mask, the network software can detect a destination address in the local subnet, and it therefore knows when the packet must go to another subnet through a router or gateway.

Some networks contain equipment that supports the proxy Address Resolution Protocol (ARP). ARP establishes routing paths between any two hosts (a *host* can be a PC or an instrument). If your network supports ARP, you won't need to enter the subnet mask or default gateway information into your PC or instrument.

There are times, though, when you may need the default gateway address. When the network ID of the source (instrument) and destination (your PC) addresses are on different subnets, as determined by the subnet mask, the network must forward packets to your default gateway for delivery. The default gateway knows the network ID's of the other subnets, so it forwards the packet to other gateways until the packet arrives at the proper destination.

You also may need socket-port assignment information. Socket-port assignments range from 1024 to 65535. These numbers tell recipients of data packets where the packet originated so other network hosts know where to send replies. Once the network establishes the routing and opens a port within each host, communications become similar to full-duplex connection from host to host.

Many instrument makers use a socket-port assignment number that hasn't been officially assigned in the network industry. I strongly suggest you use the number set by your instrument's manufacturer. You may also need to enter this number into your computer when setting up your instrument's control software. Your administrator will want to ensure there are no conflicts with other numbers that may be in use on your network. If your user manual doesn't specify the socket-port number, then contact your equipment maker to get it.

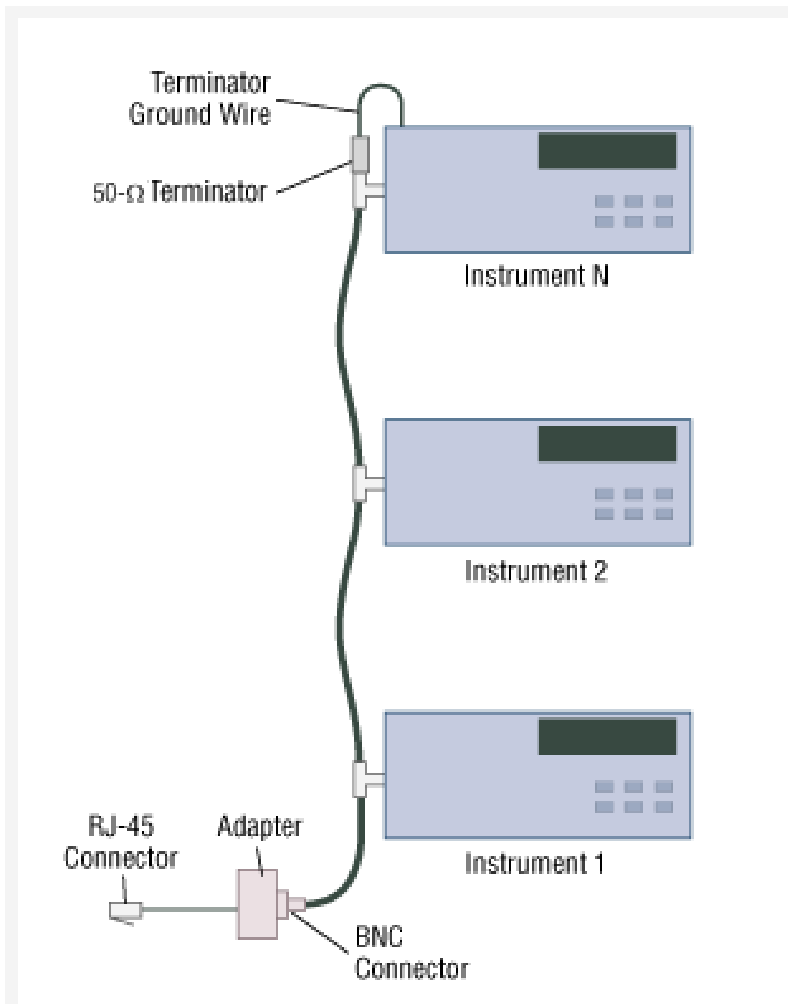
Make the Connection

With the address issues resolved, you're ready to tackle the physical issues. Most Ethernet networks use 10BaseT unshielded twisted pair (UTP) cables that have RJ-45 connectors or 10Base2 thin coax cables that have BNC connectors. 10Base2 cables work well when you must place your instruments at one or more remote sites (up to 100 m) from your network connection (called a "network drop").

The shielded 10Base2 cables often make runs that traverse industrial electrically noisy machinery and manufacturing floor areas. 10BaseT cables work well in most office areas, and you can find these connections in many locations throughout your physical network area. Your instrument may have either type of connector. Hubs and adapters can change between connector types.

The two types of connections require different topology when you need to connect more than one instrument in a local area. When connecting multiple instruments on a 10Base2 (coax) system, you use a daisy-chain style connection going from the host or network drop to each instrument in sequence through a "T" connector at each instrument (**Fig. 1**).

Both end connections require termination with a 50-V load connector. You should have at least 20 in. of cable from PC to instrument or from network drop to the nearest PC or instrument.



10BaseT cables use a hub when connected in a star (**Fig. 2**) or fan-out configuration. If you've been using Ethernet to communicate with your instruments locally (not over the corporate network), you must change your 10BaseT *crossover* cable to a *straight-through* cable for your corporate network. Changing these cables can save you hours of troubleshooting.

Figure 1. Daisy-chain connections require a terminator at the end of the cable run. Adapters convert BNC connectors to RJ-45 types.

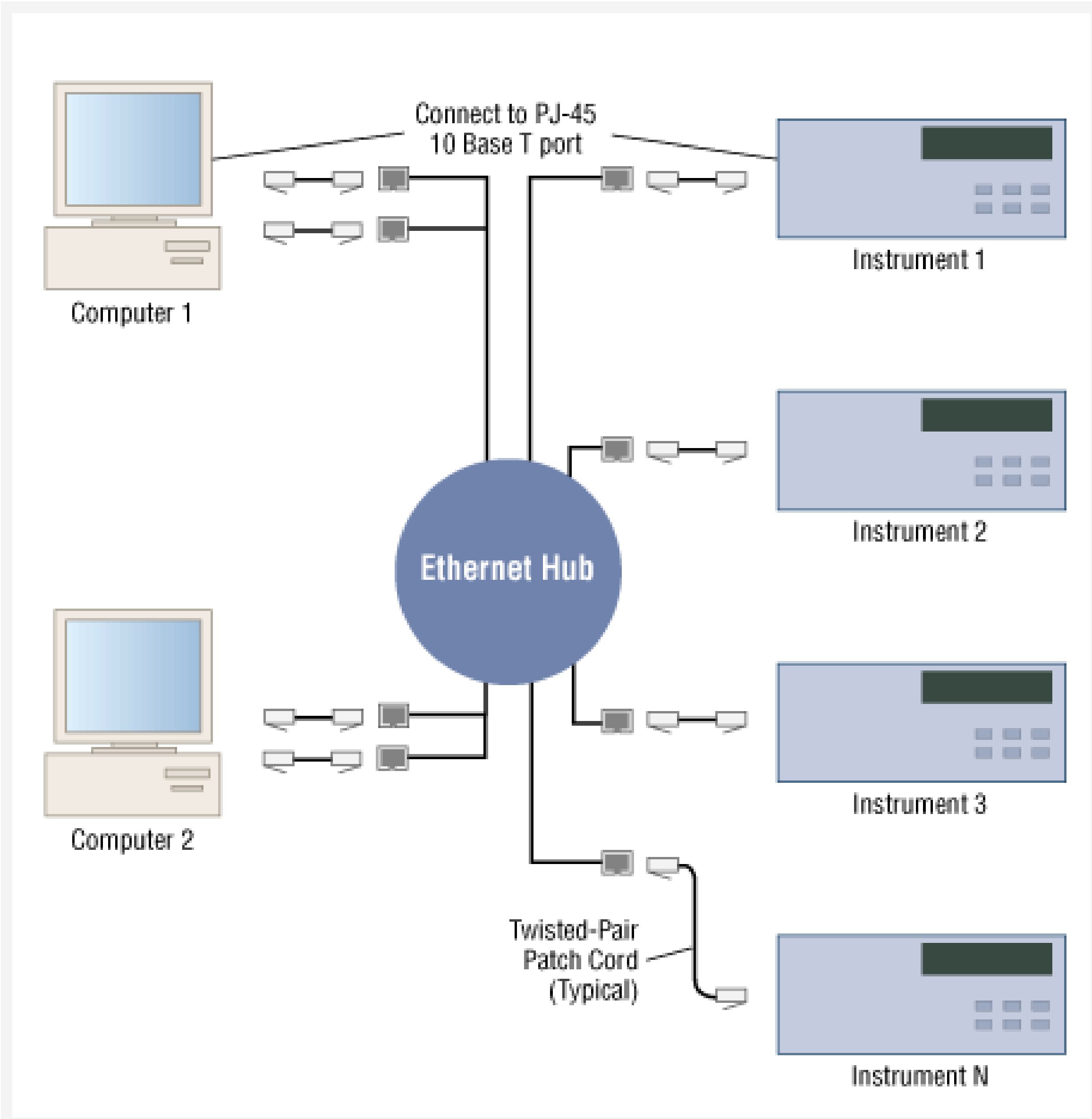


Figure 2. An Ethernet hub connects several host devices, forming a subnet.

If your PC doesn't already have a network interface card (NIC) installed, you'll have to install one. Depending on your company's policies, the network administrator may have to supply and install the NIC. After all, your IT department may "own" your office PC. You then have to install any instrument-control software.

If you use Windows, you can easily configure your network settings. Your PC may already have the drivers you need for your NIC, or you may need to get the original Windows CD-ROM to install them. If you're using other operating systems or network software such as Banyan Vines or Novell, your administrator may advise you to follow additional steps for your setup. You may have to reboot your computer to map the new settings into your PC software.

Next, you have to set up your instrument and connect the cables. Many instrument-control programs can pass

IP, subnet mask, default gateway, and socket-port information to your instrument. Other instruments require manual entry from a front panel. If you're connecting more than one instrument to the network, record each instrument's IP address so you don't duplicate addresses. Connect the cables, and you should be able to send data over the network.

Once you have measurement data flowing over the network, you may need to share the information with several people. You can save data files to a network server so others can view and work with the data. You also can view data in "real time." Some applications let you serve real-time data to other users directly from a Web site. If you need to publish your measurements on the Web, be sure to involve your network administrator here, too. T&MW

Bruce Fuller *is the product marketing manager for data-acquisition products at Fluke. E-mail: bruce.fuller@fluke.com.*

Glossary

address resolution protocol (ARP) A Transmission Control Protocol/Internet Protocol (TCP/IP) that dynamically binds a network-layer IP address to a data-link-layer physical hardware address such as an Ethernet address.

gateway A network node equipped for communicating with another network that uses different protocols. A gateway may contain equipment such as protocol translators, impedance matching devices, rate converters, fault isolators, or signal translators as necessary to provide system interoperability. Gateways also require mutually acceptable administrative procedures between the two networks. A protocol translation/mapping gateway interconnects networks with different network protocol technologies by performing the required protocol conversions.

Internet protocol (IP) A Department of Defense (DoD) standard protocol designed for use in interconnected systems of packet-switched computer communication networks. The Internet protocol provides for transmitting blocks of data, called datagrams, from sources to destinations, where sources and destinations are hosts identified by fixed-length addresses. The Internet protocol also provides for fragmentation and reassembly of long datagrams, if necessary, for transmission through small-packet networks.

router A unit that interconnects two or more networks. Routers operate at the network layer (layer 3) of the ISO Open Systems Interconnection—Reference Model. The router reads the network layer address of all packets transmitted by a network and forwards only those addressed to another network.

socket An application program interface (API) that provides applications programs with access to a network. In Microsoft Windows, the socket resides in winsock.dll. (Source: www.cisco.com/univercd/cc/td/doc/product/software/ioss390/ios390sk/sklibfun.htm)

subnet address An extension to an IP address that lets users of a network use a single IP network address for multiple physical subnetworks. The IP address contains three parts: the network, the subnet, and host addresses. Inside the subnetwork, gateways and hosts divide the local portion of the IP address into a subnet address and a host address. Outside of the subnetwork, routing continues as usual by dividing the destination address into a network portion and a local portion.
subnet mask (address mask) Used to identify the parts of an IP address that correspond to the different sections (separated by dots). (Source: www.vcnet.com/topcc/newversion/glossary/glossa.htm.)

subnetwork A collection of equipment and physical transmission media that forms an autonomous whole and that can interconnect systems for communication purposes.

*Source: glossary.its.bldrdoc.gov/fs-1037/ (unless otherwise noted)