Network Connection Overview for Ethernet Based Instruments

Introduction

Keithley's Ethernet compatible instruments fully integrate instrument-quality resolution and sensitivity with Ethernet long distance networking capability. These instruments can be used on a 10BaseT or 100BaseT Ethernet network. As with other Ethernet devices, this requires the installation and configuration of associated network interface cards (NICs) in a PC controller, installation of the TCP/IP protocol, and setting up TCP/IP addresses. This network primer is a short tutorial on how to accomplish these steps. Appendix B provides a glossary of networking terminology.

Setting Up Network Configurations

Ethernet is a type of Local Area Network (LAN) that works with a variety of transmission media. Some of the more popular variations are 10/100BaseT, 10Base2, and 10BaseF, which use unshielded twisted pair (UTP), coaxial cable, and optical fiber respectively.

Keithley's Ethernet compatible instruments area designed for a 10/100 BaseT network and uses a standard RJ45 connector. This is an eight-wire connector, but only four wires are used: one pair to transmit and one pair to receive data. A 10BaseT network can accommodate transmission speeds up to 10Mbits/second; 100BaseT operates at up to 100Mbits/second. Both types of networks usually require Ethernet hubs to make connections. The exception is a one-to-one connection using a crossover cable.

When using Ethernet to collect and distribute test data, the first step is deciding which connection scheme is most convenient. Unlike instruments with GPIB and RS-232 interfaces, Keithley's Ethernet compatible instruments offer options other than simply connecting the instrument directly to a PC controller in a closed loop. These instruments can be connected to a TCP/IP network using its own subnetwork, or it can be connected directly to an existing network, including a corporate intranet.

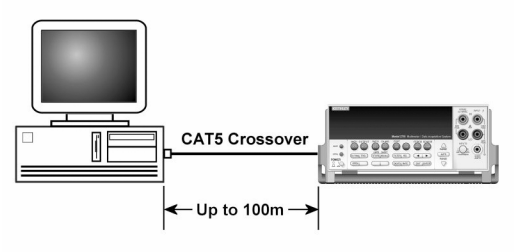

Figure 1. One-to-one connection with a crossover cable

One-to-One Connection—A network crossover cable connection is similar to a typical RS-232 hookup using a null modem cable. The crossover cable has its receive (RX) and transmit (TX) lines crossed to allow the receive line input to be connected to the transmit output on the network interfaces. With Keithley's Ethernet compatible instruments, this is only done when one instrument is being connected to a single NIC.

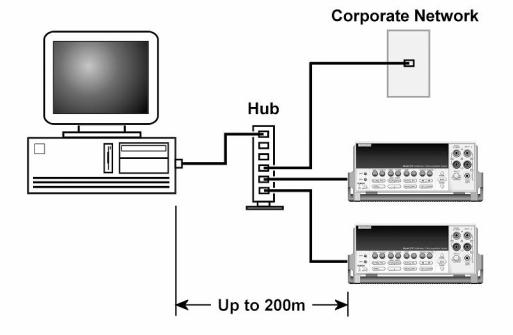

Figure 2. One-to-many connection scheme using a network hub

One-to-Many Instruments Connection—With an Ethernet hub, a single NIC can be connected to as many instruments as the hub can support. This requires straight-through network (non-crossover) cables for hub connections. The advantage of this method is easy expansion of measurement channels when test requirements exceed the capacity of a single instrument. With only Keithley's Ethernet compatible instruments connected to the hub, this is an isolated instrumentation network. However, with a corporate network attached to the hub, these instruments become part of the larger network and the network resources must be obtained from the network administrator.

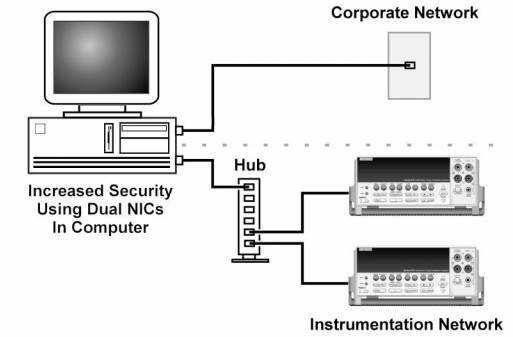

Figure 3. Use of two NICs for connections to a corporate network and instrumentation hub.

Dual NICs for Independent Networks—When it is desirable to interconnect independent corporate and instrumentation networks, two NICs are required in the PC controller. While the two networks are independent, stations on the corporate network can access the instrumentation, and the corporate network using the same computer. This configuration resembles a GPIB setup in which the computer is connected to a corporate network, but also has a GPIB card in the PC to communicate with instrumentation.

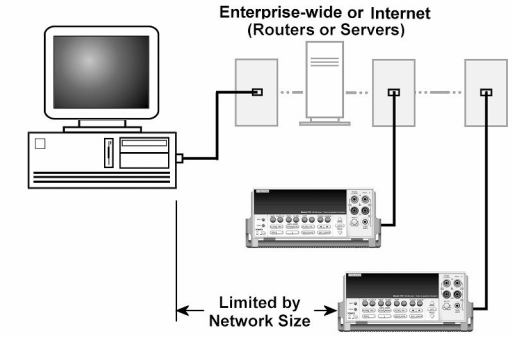

Figure 4. Instrumentation connection to enterprise routers or servers.

Enterprise Network Connections—This connection scheme uses an existing network infrastructure to connect Keithley's Ethernet compatible instruments to the PC controller. The network resources must be obtained from the network administrator. Usually, the instruments are kept inside the corporate firewall, but the network administrator could assign resources that allow them to be outside the firewall. This would allow Keithley's Ethernet compatible instruments connection to the Internet using appropriate security methods. Thus, data collection and distribution could be controlled from virtually any location.

TCP/IP Protocol

The Basics—Regardless of the type of network connection used, there must be a way to identify each instrument and its location on a network. Software on the PC provides the means of controlling the instrument. A data communication protocol defines the method of exchanging instructions and data between the PC and each instrument.

WARNING

When connecting to a corporate network, the network administrator MUST provide all of the network settings for the Ethernet compatible instruments. Failure to use settings provided by the network administrator could result in failures at other locations on the corporate network. Failure to work through the network administrator could also be considered a breach of company policy. Always consult with the network administrator before attempting to connect instrumentation to the network.

Keithley's Ethernet compatible instruments use the TCP/IP protocol to communicate with other hosts on the network. A host is defined as any device on the network that can transmit and receive IP packets. In addition to instruments, it includes workstations, servers, and routers. Each host on a TCP/IP network is assigned a 32-bit logical address that is unique to that host.

IP Addressing—No two hosts on a network can have the same IP address. There are two ways of assigning an IP address to a host. For a network server running Dynamic Host

Configuration Protocol (DHCP), a network resource such as an IP address is assigned each time the host connects to the network. Typically, this type of IP addressing is used for corporate networks, and is supported by Keithley's Ethernet compatible instruments. The other method is called static IP addressing and is used in the majority of isolated networks. The these instruments also support static addressing.

Static IP addressing means that network settings assigned to a host stay the same each time it is connected to the network. When setting up Ethernet compatible instruments on an isolated network, it usually is the user's responsibility to configure the network settings for those hosts. Thus, the user assigns the unique logical address for each instrument.

The IP address is 32 bits wide and is divided into two main parts: a network ID number and a host ID number. The address is expressed as four decimal numbers separated by periods. Valid addresses range from 0.0.0.0 to 255.255.255.255, for a total of about 4.3 billion unique addresses. Each of the four numbers represents the decimal value of the numbers' 8-bit bytes. The way these four numbers are assigned for host ID and network ID depends on the class of network being used.

The network ID must be unique among all network subnets that connect to the Internet (or corporate intranet). If the subnet will in fact be connected to the public Internet, then the network ID must be obtained from the Network Information Center, which assigns and preserves unique IDs. In any case, each host ID must be unique among all the hosts on the same network (which presumably has a unique network ID number).

In the TCP/IP protocol, a Subnet Mask separates the network ID from the host ID. The Subnet Mask looks like an IP address, but sets a data bit high for each position of the IP address that makes up the network ID. Three different classes of network are defined with the IP address and subnet mask, as shown in Table 1.

Table 1. Network classes defined by IP address and subnet mask combinations.

Network Class	IP address	Subnet Mask	Available Subnets	Available Hosts
A	nnn.hhh.hhh.hhh	255.0.0.0	126	16777214
B	nnn.nnn.hhh.hhh	255.255.0.0	16384	65534
C	nnn.nnn.nnn.hhh	255.255.255.0	2097151	254

Note: In the IP address format, 'n' is a network ID position, and 'h' is a host ID position. For simplicity, the first byte definition has been omitted from the table. Refer to the network manual for further details.

Class C networks are the most common and use the subnet mask 255.255.255.0. The first three bytes are the network ID number and the last byte is the host ID on the network. Host ID numbers 1 through 254 are available for assignment. All hosts on the same isolated network must have the same subnet mask. As a general rule, the top and bottom host numbers are reserved. The top one (nnn.nnn.nnn.255) is the broadcast address and the bottom one (nnn.nnn.nnn.0) is shorthand for the whole subnet.

Setting Up an Isolated Instrument Network

The following paragraphs describe how to set up a simple isolated Class C network for communicating with two Keithley's Ethernet compatible instruments. This network example is similar to Figure 2, but without the corporate network connection to the hub. If connecting using just a cross over cable without a hub like Figure 1, follow the procedure below without the use of the hub or the second Ethernet instrument.

The standard Ethernet hub basically repeats anything it receives from one port, making that data available to all its other ports. Hub connections are made with straight-through cables. The hub is connected to the network interface card in the PC. The NIC and its driver must be properly installed on the computer according to the manufacturer's instructions.

The next step is to create IP addresses for the three hosts (the NIC and Ethernet compatible instruments) on the network. This is a Class C network, so the subnet mask will be 255.255.255.0. From Table 1, note that the first three parts of the IP address make up the network ID. For purposes of this example, a network ID of 192.168.1 is used.(If a corporate network is also connected to the same computer using dual NICs, the instrumentation network ID must be different than the corporate network ID.) Next, the host ID portions of the three IP addresses are assigned. In this example, a host number of 1 is assigned to the NIC; the first instrument is assigned a host number of 10; the second instrument becomes host number 20. The complete IP addresses are listed in Table 2.

Warning

If there is an existing IP address that is already configured for the NIC network settings, the IP address for the Ethernet Instruments can be modified to match the IP address that is already configured in the NIC. If existing network configuration information is modified on the NIC, it is highly recommended that the old network configuration be captured before any modification is done. Once the network configuration settings are updated, the older information will be lost. This may cause a problem when trying to reconnect to a corporate network

Table 2. Host IP addresses for text example.

Host	IP Address
NIC	192.168.1.1
First Ethernet Instrument	192.168.1.10
Second Ethernet Instrument	192.168.1.20

In a Windows operating system, install the NIC's IP address with the Windows Control Panel. The exact steps differ somewhat for each version of Windows. See Appendix A for details. The final step is to assign the other two IP addresses Ethernet compatible instruments. *. It's a good idea to record IP addresses so they can be easily found when needed. This is especially important when changing the existing network settings on the computer; otherwise, those settings will be lost.

* As part of IP address installation process, the user may be asked for a default gateway. This is the IP address of the router used to connect devices on a network. However, an isolated network does not use a router, so a value of 0 is entered for the default gateway. When connecting Ethernet compatible instruments to a company network, the network administrator may supply the number that is used for the default gateway.

APPENDIX A

Configuring a Network Interface Card (NIC) Card

To configure a network interface card, the TCP/IP protocol must also be installed and configured. In each version of the Windows operating systems, this is done differently. Also, the procedures described here may differ slightly on computers made by different companies.

Configuration in Windows 95/98/ME

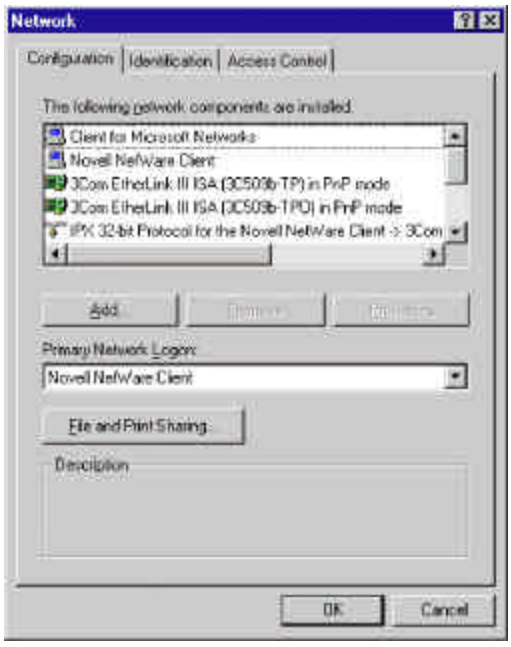

Figure 7

(Refer to the network configuration window shown in Figure 7.)

1. Click on the Windows Start button.
2. Select Settings, then Control Panel.
3. Open the folder named Network.
4. Look for a TCP/IP entry. If configuring a computer with two network cards, there should be two entries, one for each card. It's possible to tell the difference by the listing; after the TCP/IP notation, there will be a reference to the NIC card(s). If there is no TCP/IP protocol listed, one must be added. This is done by clicking the Add button. Then click on Protocol, select Microsoft, and click TCP/IP.
5. After selecting the TCP/IP protocol, click the Properties button. On the IP Address tab, select the method of obtaining the IP address. For an isolated network, click on Specify An IP Address.

6. Complete the IP Address and Subnet Mask according to the network configuration.

7. The Default Gateway and the DNS settings could be needed when connecting to a corporate network. For an isolated network, these settings are not used.

8. Follow the instructions on the screen and reboot as necessary.

Configuration in Windows 2000

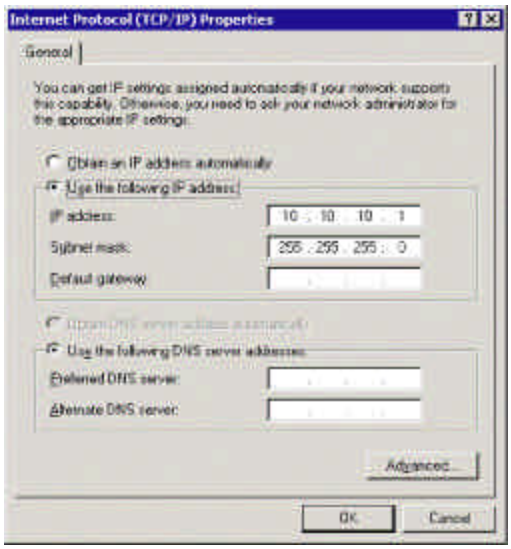

Figure 8

(Refer to the network configuration window shown in Figure 8.)

1. Click on the Windows Start button.

2. Select Settings, then Control Panel.

3. Click on Network and select Dial-Up Connections.

4. Right click on Local area Connection, then select Properties.

5. In the General tab window, the TCP/IP protocol should be listed and selected. If not, click on Install, then select Protocol, and click Add.

6. Select the TCP/IP protocol, then click Install.

7. Go back to the General tab window, select the TCP/IP protocol and click on Properties.

8. Select Use the Following IP Address, then enter the IP address and subnet mask for the network.

9. The Default Gateway and the DNS settings could be needed when connecting to a corporate network. For an isolated network, these settings are not used.

10. Follow the instructions on the screen and reboot as necessary.

Configuration in Windows XP

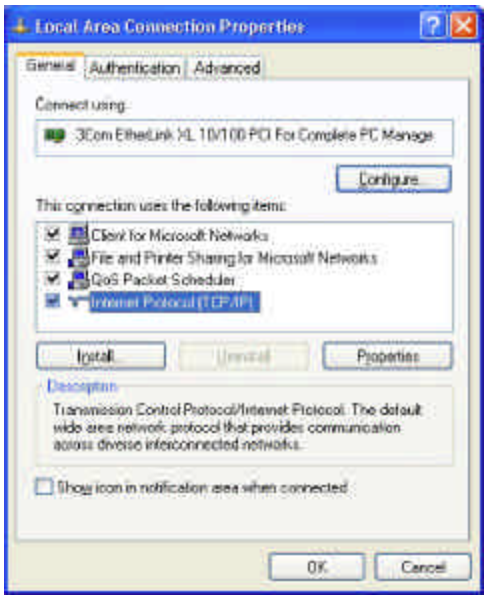

Figure 9

(Refer to the network configuration window shown in Figure 9.)

1. Click on the Windows Start button.
2. Select Network and click Internet Connections
3. Under “or pick a control panel icon”, select Network Connections
4. Right Click on “Local area connection” and select Properties
5. In the General tab window, the TCP/IP protocol should be listed and selected. If not, click on Install, then select Protocol, and click Add.
6. Select the TCP/IP protocol, then click Install.
7. Go back to the General tab window, select the TCP/IP protocol and click on Properties.
8. Select Use the Following IP Address, then enter the IP address and subnet mask for the network.
9. The Default Gateway and the DNS settings could be needed when connecting to a corporate network. For an isolated network, these settings are not used.
10. Follow the instructions on the screen and reboot as necessary.

APPENDIX B

Glossary

API (Application Programming Interface): A set of callable software functions that applications use to make requests to the operating systems

Default Gateway: The IP address of the computer that is attached to the network running TCP/IP that knows how to route data to other networks.

Dynamic Host Configuration Protocol (DHCP): A feature of Windows NT server that automatically assigns IP addresses to hosts on a TCP/IP network whenever the hosts start up.

Bridge: A device that passes network data between two segments of a network.

Ethernet: A network standard that uses either coaxial or twisted pair cable. Ethernet is the most widely used form for a LAN communication and is the IEEE standard 802.3.

Firewall: A hardware or software component in the data path between the internet and an internal network. The firewall filters packets by examining them on one side and deciding what to pass along to the other side.

Host: Defined as anything on the network that can transmit and receive IP packets on a network. This would include workstations, servers, and Ethernet Instruments

Hub: A passive hub is a device that split the received signals among other connected nodes. An active hub amplifies or repeats incoming signals before distributing them.

INterNIC Internet Network Information Center: The organization responsible for assigning Internet network addresses and domain names to hosts that are connected to the Internet.

IP Address: A unique 32-bit address assigned to each host attached to the network. An IP address specifies both the network and the host address.

IS/IT: Short for Information Services or Information Technology, which encompass all aspects of managing information. Computer departments inside companies are commonly referred to as IS departments, as computers are the main tools used in information management. Management Information Services (MIS) is an older term for the same subject.

Gateway: A computer that acts as a translator on the network or as a router between two network technologies. It can also act as a translator between two different network protocols.

MAC Address: The Media Access Control Address is a host's unique identity. It is a six byte hexadecimal number that can be represented in HEX or decimal. Ethernet Instrument may use a decimal number, much like an IP address structure, to represent the MAC address. The MAC address is usually assigned to the host at the factory. The host transmits its address with each packet of data. It may also be referred to as a hardware address, Ethernet address, node ID, or adapter address. This is not required when using an isolated network. A systems administrator may require a host's MAC Address when it is connected to a corporate network.

Network: Two or more computers connected together, allowing them to communicate.

NIC: A network interface card is an electronic board installed in a computer so the computer can communicate with a network.

Packet: A chunk of information that contains both the original data to be transmitted along with additional addressing information. If the packet is too large to be transmitted by the data link layer, the network layer breaks in into multiple pieces, transmits them, then reassembles the packet at the receiving end.

Peer-to-Peer Network: A type of network in which no two computers have more control over the network than another. Each can act as both a server and a client. This means that each can supply resources to the other peer computer.

Protocol: A formal set of communication conventions used by two network nodes to communicate properly with each other.

Repeater: A device that amplifies incoming transmission signals before regenerating them on its output. This will maintain signal integrity along a longer media run than is normally possible.

Router: A device that forwards data packets from one network to another.

TCP/IP: Transmission Control Protocol/Internet Protocol. A set of network protocols and associated tools that originated in the UNIX and Internet environments. It has become the standard protocol used when configuring networks.

Subnet Mask: A 32-bit binary number expressed as four three-digit segments, like an IP?address. The Subnet Mask is used in conjunction with an IP?address to determine the network number and Host number of the IP?address.

10BaseT/100BaseTX: Unshielded twisted pair running at 10/100 Mbps. Maximum cable length is 100m. 100BaseT is often referred to as 100BaseT fast Ethernet.