System Developer Guide

Using LAN in Test Systems: Network Configuration

Application Note 1465-10

This set of application notes shows you how to simplify test system integration by utilizing open connectivity standards such as local area networking (LAN). The collective goal of these notes is to help you produce reliable results, meet your throughput requirements and stay within your budget.

Using LAN in Test Systems: Network Configuration, the second note in the series, describes potential risks, suggests two secure topologies for LAN-based test systems, and outlines the essential aspects of system configuration. This note builds on the concepts presented in Application Note 1465-9, *Using LAN in Test Systems: The Basics,* which provides an introduction to the essential elements of local area networking, the basic attributes of test systems, and the benefits of using a LAN interface for control and data transfer in a test system.

Please see page 9 for a list of the other titles in this series.

Table of contents

Agilent Technologies

Creating a safe haven

The decision to use LAN in a test system delivers important benefits to your company and your team. From a business perspective, intense competition among equipment vendors has produced a wide selection of high quality, low-cost solutions for local area networking. From an organizational view, widespread use of LAN technology simplifies connectivity and enables new levels of communication and collaboration between team members, wherever they may be in the world.

Of course, the use of any pervasive computing technology also carries risks. Adding a LAN connection can open the door to inadvertent threats carried on a company's intranet, and may expose a test system to a variety of malicious threats from the Internet (Figure 1).

Fortunately, there are effective, practical solutions that can protect your system from internal and external risks. Our recommended starting point is to create a protected, private LAN for the test system. The standard capabilities of most Microsoft® Windows® PCs and many low-cost networking products enable two viable approaches, one router-based and the other PC-based. Several factors will influence your choice, and your decision has implications for the selection and configuration of the PC, the network and the test instrumentation.

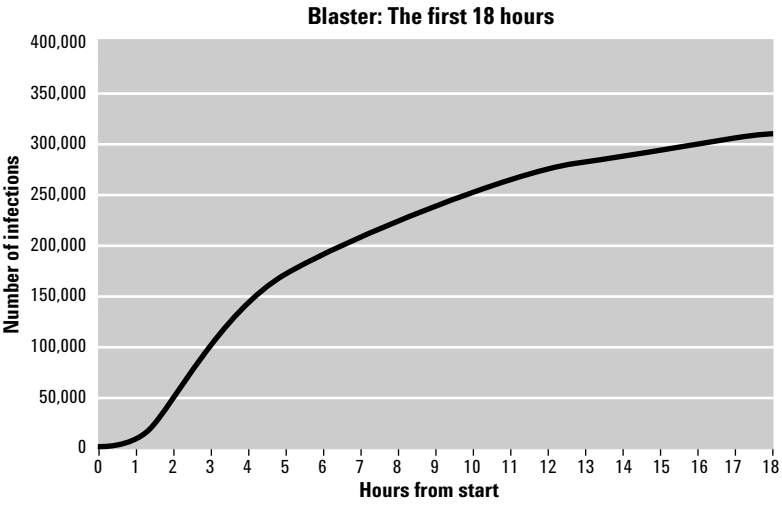

Figure 1. The Blaster worm infected more than 300,000 computers in less than 18 hours.

Recapping Application Note 1465-9

Several factors can dramatically increase the burden on the I/O connection in a test system. Examples include the number of instruments in the system, the number of tests being performed, and the volume of commands, status messages and test data being transferred. LAN technology is one of the best ways to handle that burden. It offers a fast, low-cost alternative to GPIB, and it surpasses USB with longer reach and locking connectors. LAN is also pervasive in most enterprises, making it much easier for colleagues to share data, results, reports and so on.

Most current-generation PCs have built-in LAN ports, which means the computing portion of a test system needs minimal physical configuration. LAN ports are also becoming more common in current- and next-generation test equipment. Devices such as the Agilent E5810A LAN/GPIB gateway make it possible to connect older, GPIB-only instruments to a LAN-based test system.

Many of today's LAN-enabled instruments are also equipped with built-in Web servers. By pointing a browser at such an instrument's IP address, you can view its configuration, change the settings, start a measurement and see the results. Some LAN-equipped instruments provide greater functionality: every Agilent Infiniium oscilloscope contains a Windows PC running custom software. Windows has several LAN services built in, enabling capabilities such as sharing of files, folders, drives and printers.

Understanding the pitfalls

Test systems that aren't connected to enterprise networks are sometimes labeled as "islands of automation." However, their isolation provides an unintended benefit: standalone test systems are insulated from the viruses, worms and Trojans that might strike a company's network.

For a system on an island, the biggest risks come from human interference. System errors might arise if a configuration change is made via the front panel or if two instruments are set to the same GPIB address. These problems are easy to fix and the integrity of the system remains intact.

Recognizing potential threats

Connecting the system's host PC to the company network builds a bridge to the island. It also opens the door to a wider range of threats—including some that may compromise system security and integrity.

Inadvertent threats may reach the system via the company intranet. Some are programmatic: another PC on the network may cause a configuration change in one or more instruments. Others are systematic: configuring the test instruments for dynamic rather than static IP addresses may cause unexpected operation. As an example, if the IP addresses of two power supplies are reversed, the device under test (DUT) could receive the wrong voltages at the wrong points and suffer severe damage.

Malicious threats from the Internet may breach the company's firewall, spread via the intranet and infect the system's host PC. These threats also pose a potential risk to any instruments that contain a Windows PC. One answer is to include a hardware or software firewall in each instrument—a solution Agilent is enabling in next-generation instruments.

Examining other issues

A LAN-based system is also subject to the quirks and limitations of the deployed hardware. As an example, the simplest way to connect a system to the corporate network is through a hub. However, hubs let all network traffic flow in both directions: all intranet traffic would be present within the test system and all test system traffic would appear on the intranet. Excess network traffic could degrade system throughput and the broadcasting of test results on the intranet could be a security risk. Using a switch or router is a better choice because both are specific and selective about filtering and forwarding network traffic.

Some older LAN-enabled instruments also have two weaknesses that must be addressed or acknowledged. For example, those that don't support the VXI-11 communication protocol (or provide partial support) probably can't create a locked LAN I/O session between the instrument and a PC. Locking ensures a stable PC-to-instrument connection and also blocks other attempts to access the instrument for the duration of a session.

Instruments that do support VXI-11 have an important shortcoming when not locked into a session: they have no authentication capabilities (e.g., password protection) to block unauthorized access. In this case, any PC on the network that supports VXI-11 can access the instrument and easily disrupt its behavior. The solution is a private LAN that limits access to only those devices you trust.

Designing the private, protected LAN

Our basic prescription for any LAN-based test system is to create a private, protected network that includes the host PC and the test equipment. Fortunately, there are two practical, effective ways to set up this type of network. One approach is built around a LAN router, which provides a buffer between the test system and the corporate intranet. The other approach uses the host PC as the buffer by configuring it with two LAN cards and the Internet Connection Sharing (ICS) feature of Windows XP.

Sketching the router-based solution

A router is a standalone box with multiple LAN connectors—one for the external or "public" network and four (or more) for the internal or "private" network. The router links these networks through its ability to handle high-level communication protocols such as TCP/IP. Routers allow one- and two-way communication between devices and also enable "awareness" among devices on a network.

Routers also utilize a feature called network address translation (NAT) that allows devices to hide their presence from public networks. It does this by using a private set of IP addresses that are not revealed to devices on the public side. This is the key attribute that enables the creation of a private LAN for a test system.

As shown in Figure 2, the router is the focal point of the network. In the simplest router-based system, its "external" port—usually labeled Internet or WAN (wide area network)—is connected to the corporate intranet; its other ports—usually labeled LAN—are connected to the host PC and a few LAN-enabled instruments. Additional instruments can be added by connecting a switch or hub to one or more LAN ports on the router (Figure 3).

The router-based approach has several advantages. First and foremost, it protects the test system from the potential hazards carried on the intranet or Internet. It also prevents any type of outside access by limiting communication to only those devices that reside within the private LAN—and, unlike a hub, it shields the system from intranet congestion by isolating all but local traffic. What's more, the router safeguards system operation from the effects of administrative activity or hardware problems on the local intranet because it provides all of the network services needed by the instruments and the host PC. At the same time, the router gives the PC unhindered access to the system network as well as the corporate intranet and the Internet. It also gives all LAN-enabled instruments access to TCP/IP resources on the intranet and the Internet.

Defining router and PC features

Successful implementation of the router-based private network requires a few essential capabilities.

Must-have router features:

- **Network address translation (NAT)** — NAT allows the router to act as an agent between the public and private networks, mapping private IP addresses to public IP addresses and enabling communication between networks.
- **De-militarized zone (DMZ)** — The DMZ feature makes it possible give a PC (or instrument) complete access to the Internet, effectively putting it "outside the firewall." With DMZ, other computers outside the private network can connect to the host PC and use its public services (e.g., shared file folders or a Web server). Because DMZ is implemented differently on most router models, you should verify that you are able to achieve essential tasks such as communication with a manufacturing database.

Should-have router features:

- **Sufficient ports** — Each device should have its own LAN port, either in the router or via one or more LAN switches or hubs connected to router ports.
- **Adequate port speed** — The router should support at least 100 Mbps (100Base-T) on each LAN port (the private side) and either 100 Mbps or 10 Mbps (10Base-T) on the WAN port (the public side).
- **Built-in DHCP server** — The router assigns IP addresses to the LAN devices attached to its private LAN ports. Some routers keep a table in non-volatile memory that provides a mapping between the assigned IP addresses and the associated Ethernet devices on the private network. Vendors call this capability by many names, including "static DHCP," "DHCP client reservation," "fixed mapping," and "MAC address to IP mapping." (MAC stands for media access control.)

The router-based approach also requires a host PC that uses TCP/IP rather than NetBEUI, IPX or SPX [1] as its network communication protocol. The PC may use DHCP to ensure assignment of a unique IP address, or it can be configured with a static, internal IP address that is compatible with the router's configuration.

1 NetworkBIOS Extensions User Interface, Internetwork Packet eXchange and Sequenced Packet eXchange are alternatives to TCP/IP for network communications. If installed in the host PC, their presence can create problems within the network.

Outlining the configuration changes — The configuration process is relatively simple for the router and the PC—to the extent that you won't have to burden corporate IT personnel with the task. For example, a host PC that's already equipped with a LAN card doesn't require any hardware modifications. The only PC configuration change—made after the router is installed and enabled—is to activate dynamic host configuration protocol (DHCP), which is a method of automatically assigning an IP address to any device connected to a LAN. (DHCP may be turned on by default, but it's best to verify this setting.)

Instrument configuration is also quite simple. The only changes are deactivating DHCP then setting the IP address, subnet mask and default gateway. These tasks are easy to complete via the front panel of most LAN-enabled instruments.

A more detailed description of the configuration process is presented in the appendix on page 8.

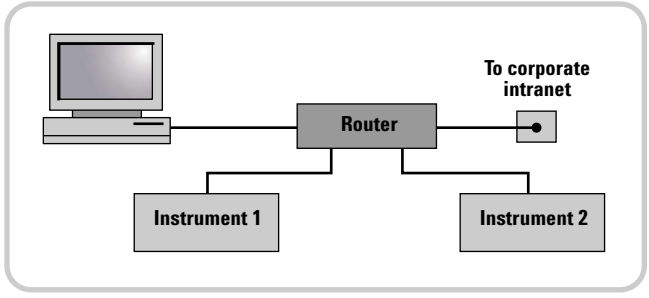

Figure 2. A test system that uses a router-based private, protected LAN.

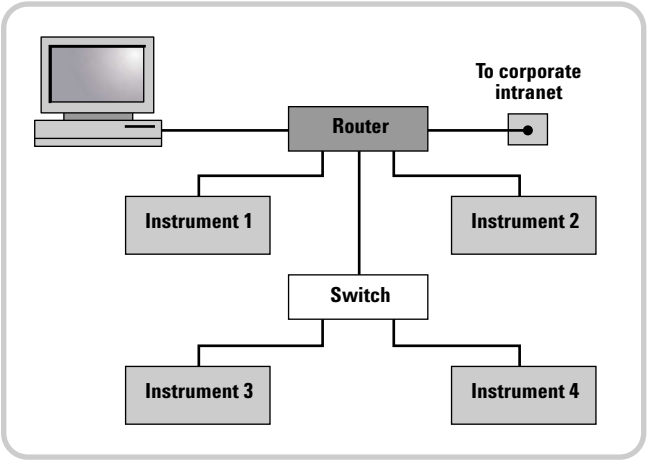

Figure 3. An expanded network that uses a switch to connect additional instruments to the test system.

Sketching the PC-based solution

By adding a second LAN card and activating ICS in Windows XP, the host PC can serve as the router in the network (Figure 4). ICS routes traffic from one LAN card to the other and provides NAT capabilities for the private addresses.

This method has several advantages in common with the router-based solution: it provides access control, blocks Trojans and worms, and gives the host PC unhindered access to the system network, the intranet and the Internet. LAN-enabled instruments can also access the intranet and the Internet. However, if the host PC is configured to use DHCP rather than a static address then it will have to rely on the corporate intranet being functional and able to provide an IP address.

Although it probably isn't a major obstacle, this approach requires that you are comfortable with the prospect of opening up the PC, installing the second LAN card, and configuring the PC to ensure the peaceful coexistence of two LAN cards.[2]

The most important step is the configuration of ICS within the host PC, which must be running Windows XP with Service Pack 1 (SP1), Service Pack 1a (SP1a) or Service Pack 2 (SP2) (Microsoft service packs are cumulative).[3] Through the Network Connections control panel, both LAN cards can be enabled and the one connected to the public network can be shared. You then use the Local Area Connection Properties window to enable ICS (Figure 5).

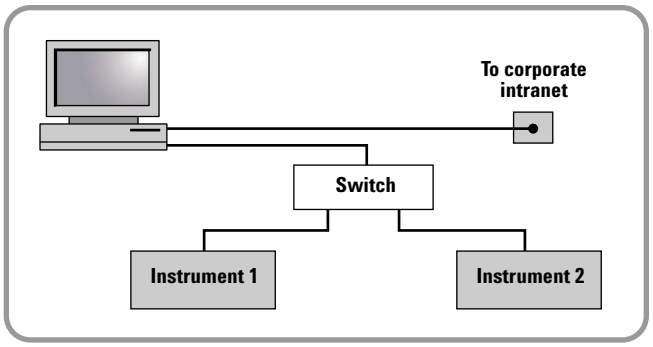

Figure 4. The PC-based solution, with two LAN cards in the PC and a switch to connect the instruments.

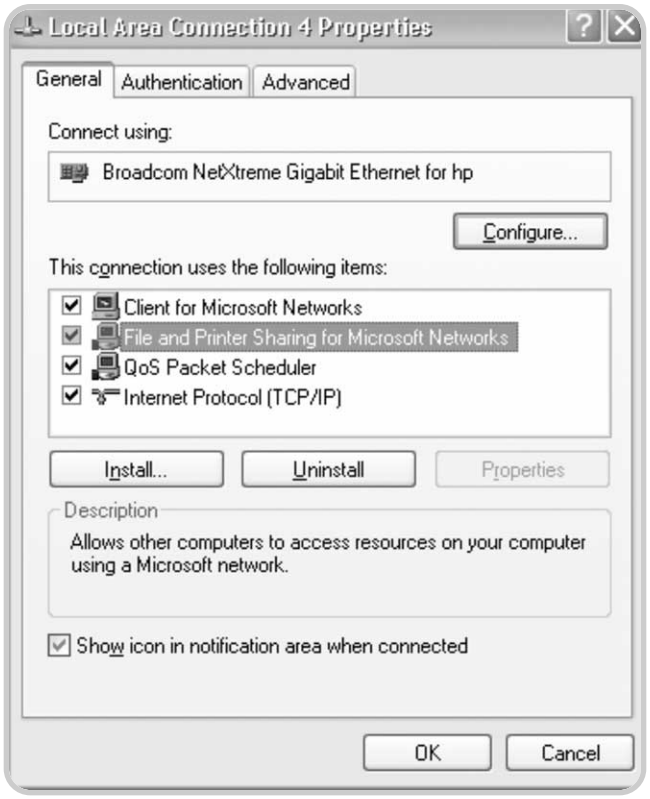

Figure 5. Use the Local Area Connection properties window in Windows XP to activate Internet Connection Sharing.

2 It is also possible to use a USB-to-Ethernet adapter as the second LAN port, but there would be some latency in this connection—and the configuration process is slightly more complex.

3. Other operating system configurations may work but this note focuses on the most recent versions of Windows.

Configuring the instruments

Keep one important caveat in mind when using either ICS or a router: their default mode is to dynamically assign an IP address to every device that joins the network. This is done via DHCP, which prevents addressing conflicts but also creates the possibility of assigning a different address to each test instrument every time it is powered up or reconnected to the network. As described earlier, unwanted address changes can cause improper operation and damaged DUTs.

The easiest way to prevent address changes is to disable DHCP in each instrument and then enter a static (fixed) IP address. Though this will be easy to accomplish via the front panel of most newer LAN-enabled instruments, it may not be possible with some older equipment. In those cases, the easiest solution is to use the GPIB interface on the instrument and add a LAN/GPIB gateway such as the Agilent E5810A to the network.

The IP addresses you assign to the instruments should only differ from the IP address of the router by the last of the four numbers in the IP address (e.g., 192.168.0.x). You may want to use numbers higher than 200, reserving the first few digits for any DHCP-enabled devices for which the router will typically assign an address in that low range. Applying these ideas to a system that includes a router at the IP address 192.168.0.1, the instruments could use numbers in the range of 192.168.0.200 to 192.168.0.255.

It is also necessary to configure the instruments with the proper subnet mask—usually 255.255.255.0—and default gateway, which is the IP address of the router itself (typically 192.168.0.1, 192.168.1.1 or similar, depending on the router maker).

Once you've saved these settings, you'll have to cycle power on each instrument for the changes to take effect. After each instrument has completed its boot-up operations you can then connect it to a LAN port on the router.

Shaping the future of test systems

Fast and inexpensive LAN technology has achieved widespread adoption in the computer world and is now shaping the future of test system development. The decision to use LAN for system I/O delivers valuable benefits to your company and your team. However, it also opens the door to malicious threats and inadvertent risks that can affect system performance and integrity. The creation of a private LAN can protect the test system from those risks, and ensure maximum throughput.

LAN connectors and adapters are becoming more common in current- and next-generation test equipment, and the inclusion of both LAN and GPIB interfaces may be quite common for the next few years. Older instruments won't be left behind: LAN/GPIB gateway devices make it easy to include them in new and future test systems. Agilent is committed to supporting GPIB well into the future—and we are also committed to developing new-generation test equipment that includes both LAN and GPIB interfaces.

To discover more ways to simplify system integration, accelerate system development and apply the advantages of open connectivity, please visit the Web site at **www.agilent.com/find/systemcomponents.**

Appendix: Configuring the router-based system

Of the two solutions described in this note, the router-based system (Figure 2, page 4) is more flexible and, therefore, more likely to be widely used. The specifics of the configuration process will depend on the actual products used to assemble the system. However, three essential steps provide a framework for the implementation of any router-based solution: capturing network information, configuring the router and setting up the test instruments.

Capturing network information

You'll need to record that information and use it to set up the router, which will be inserted between the PC and the intranet. That way, the PC is already programmed with everything you need to know about its network configuration. You'll need to record that information and use it to set up the router.

What you need: the host PC, powered up and connected to the intranet; the router; one LAN cable for the PC and one LAN cable for each instrument.

The process:

1. Power up the router.
2. Disconnect the intranet LAN cable from the PC. Use another LAN cable to connect the PC's LAN port to any LAN port on the router.
3. From the PC's Start menu, open a DOS or Command window and type in *ipconfig/all*. This will display several items including "Host Name" and "Physical Address." The PC's host name is registered with the corporate DNS services. The physical address is the unique MAC or Ethernet address of the LAN card in the PC. Write down the host name, the physical address, and the IP address of your computer: you'll use that information later when configuring the router.

To create a new, private network that consists of just the PC and the router, return to the DOS or Command window and type in *ipconfig/renew*.

Configuring the router

The router must be configured to mimic the test system PC on the corporate intranet. Most routers provide a browser-based interface that lets you use any Web browser to log in and modify the configuration.

Consult the router's manual for its URL and the default login values for user name and password. Launch your Web browser, type in the proper URL and log in to the router's configuration page. At this point, the details vary by vendor and product. There might be a built-in wizard function, or you may have to navigate through various configuration screens and enter values manually. Either way, you need to accomplish five tasks:

1. Enter the PC's host name.
2. Enable cloning of the PC's MAC address.
3. Modify the security settings to disable blocking of anonymous ping requests. (Allowing other computers to ping the host PC may be a requirement of some corporate intranets.)
4. Enable the DMZ capability and set the DMZ host IP address to 192.168.x.100 (the x must match the value used by your router). This is the default first address assigned by the router's DHCP server and must be used as the IP address for the host PC. Some routers may use different initial addresses: type in the *ipconfig/all* command to find out what address the router assigned the PC after they were connected.
5. Save all of these settings.

Locate the intranet cable that was originally connected to the PC and plug it into the router's WAN or Internet port. To verify proper operation, open a DOS or Command window and type *ipconfig/release*. Next, type *ipconfig/renew*: the host PC should now be able to access the corporate intranet via the router.

Setting up the instruments

The final step is to configure the test instruments with static IP addresses. Use the front panel keys of each LAN-enabled instrument to access the I/O or "IP Setup" configuration menu and disable DHCP. Next, give each instrument a unique IP address in the range of 192.168.x.200 to 192.168.x.255 (Figure 6). These values are outside the range of IP addresses routers typically assign to network devices (192.168.x.100 to 192.168.x.149).

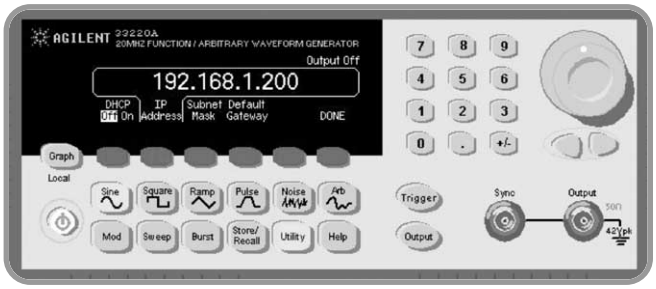

Figure 6. The IP Setup menu of the Agilent 33220A function/arbitrary waveform generator makes it easy to set the IP address, subnet mask and default gateway.

You'll also need to navigate the configuration menu and set the subnet mask to 255.255.255.0 and the default gateway to the router's IP address (192.168.0.1, 192.168.1.1 or similar, depending on which brand of router you're using).

Once you've saved these settings, you'll have to cycle power on each instrument for the changes to take effect. After each instrument has completed its boot-up operations, use a LAN cable to connect each instrument to a LAN port on the router.

To verify proper configuration, open a DOS or Command window and type *ping 192.168.1.200* or any other valid IP address you assigned to an instrument. To verify access to the intranet, launch a Web browser and try a few internal URLs. If these load as expected, this verifies proper communication with the intranet.

Glossary

Adapter — the LAN card and connector that provides an electrical interface to the network

Bridge — a LAN device that connects segments of a network

DHCP — dynamic host configuration protocol; a method of automatically obtaining an IP address for a LAN-connected device (e.g., PC, router, instrument, etc.)

DMZ — De-militarized zone; a firewall configuration that helps secure the private LAN

DDNS — dynamic domain name server; a service that allows a network device to establish its host name when it connects to the network. This lets other devices use that host name with DNS to find the device's IP address and connect to it.

DNS — domain name server; maps specific names to IP addresses, enabling use of names in place of IP addresses in test programs

DUT — device under test; the component, subassembly or product to be measured by the test system

Ethernet — a specific LAN technology that is the dominant implementation of the physical and data link layers; also known as IEEE 802.3

Firewall — a hardware device or software program (or combination) that protects a computer network from unauthorized access

Gateway — a hardware device that connects devices that use different standards and protocols (e.g., LAN to GPIB)

GPIB — General Purpose Interface Bus; the dominant 8-bit parallel I/O connection for test equipment and test systems

HP-IB — Hewlett-Packard Interface Bus; another name for GPIB

Hub — a multi-port LAN device that connects multiple devices together, usually in a star topology

ICS — Internet connection sharing

IP — Internet protocol; requires an address to communicate

IPX — Internetwork Packet eXchange; a communication protocol used in the Novell Netware network operating system

LAN — local area network

MAC — media access control; every LAN device has a unique MAC address

NAT — network address translation; maps private addresses to one or more public addresses to enable access to an intranet or the Internet

NetBEUI — NetBios Extended User Interface; a network communication protocol used in many versions of Windows

Router — a LAN device that joins multiple networks and enables creation of small, private networks

SPX — Sequenced Packet eXchange; a communication protocol used in the Novell Netware network operating system

Subnet — a group of connected network devices; used to partition networks into segments for easier administration

Subnet mask — a setting that accompanies an IP address and defines the boundaries of a subnet

Switch — a LAN device that connects multiple devices to a single LAN line; however, unlike a hub, it preserves full network bandwidth to each device

TCP/IP — Transfer Control Protocol and Internet Protocol; the two standards that provide the data communication foundation of the Internet

USB — Universal Serial Bus; designed to replace the RS-232 and RS-422 serial buses used in PCs

Related literature

The other notes in this series provide additional information about the successful use of LAN in test systems:

- *Using LAN in Test Systems: The Basics,* AN 1465-9 (pub no. 5989-1412EN) **http://cp.literature.agilent.com/litweb/pdf/5989-1412EN.pdf**
- *Using LAN in Test Systems: PC Configuration,* AN 1465-11 (available in October 2004)
- *Using USB in the Test and Measurement Environment,* AN 1465-12 (available in October 2004)
- *Using SCPI and Direct IO vs. Drivers,* AN 1465-13 (available in November 2004)
- *Using LAN in Test Systems: Applications,* AN 1465-14 (available in January 2005)

Other Agilent application notes provide additional hints that can help you develop effective test systems:

- *Creating a Wireless LAN Connection to a Measurement System* (AN 1409-3) pub no. 5988-7688EN **http://cp.literature.agilent.com/litweb/pdf/5988-7688EN**
- *Introduction to Test-System Design* (AN 1465-1) pub. no. 5988-9747EN **http://cp.literature.agilent.com/litweb/pdf/5988-9747EN.pdf**
- *Computer I/O Considerations* (AN 1465-2) pub. no. 5988-9818EN **http://cp.literature.agilent.com/litweb/pdf/5988-9818EN.pdf**
- *Understanding Drivers and Direct I/O* (AN 1465-3) pub. no. 5989-0110EN **http://cp.literature.agilent.com/litweb/pdf/5989-0110EN.pdf**
- *Choosing Your Test-System Hardware Architecture and Instrumentation* (AN 1465-5) pub. no. 5988-9820EN **http://cp.literature.agilent.com/litweb/pdf/5988-9820EN.pdf**
- *Understanding the Effects of Racking and System Interconnections* (AN 1465-6) pub. no. 5988-9821EN **http://cp.literature.agilent.com/litweb/pdf/5988-9821EN.pdf**
- *Maximizing System Throughput and Optimizing Deployment* (AN 1465-7) pub. no. 5988-9822EN **http://cp.literature.agilent.com/litweb/pdf/5988-9822EN.pdf**
- *Operational Maintenance* (AN 1465-8) pub. no. 5988-9823EN **http://cp.literature.agilent.com/litweb/pdf/5988-9823EN.pdf**

Agilent Technologies' Test and Measurement Support, Services, and Assistance

Agilent Technologies aims to maximize the value you receive, while minimizing your risk and problems. We strive to ensure that you get the test and measurement capabilities you paid for and obtain the support you need. Our extensive support resources and services can help you choose the right Agilent products for your applications and apply them successfully. Every instrument and system we sell has a global warranty. Support is available for at least five years beyond the production life of the product. Two concepts underlie Agilent's overall support policy: "Our Promise" and "Your Advantage."

Our Promise

Our Promise means your Agilent test and measurement equipment will meet its advertised performance and functionality. When you are choosing new equipment, we will help you with product information, including realistic performance specifications and practical recommendations from experienced test engineers. When you receive your new Agilent equipment, we can help verify that it works properly, and help with initial product operation.

Your Advantage

Your Advantage means that Agilent offers a wide range of additional expert test and measurement services, which you can purchase according to your unique technical and business needs. Solve problems efficiently and gain a competitive edge by contracting with us for calibration, extra-cost upgrades, out-of-warranty repairs, and onsite education and training, as well as design, system integration, project management, and other professional engineering services. Experienced Agilent engineers and technicians worldwide can help you maximize your productivity, optimize the return on investment of your Agilent instruments and systems, and obtain dependable measurement accuracy for the life of those products.

Agilent Email Updates

www.agilent.com/find/emailupdates

Get the latest information on the products and applications you select.

Agilent Open Connectivity

Agilent simplifies the process of connecting and programming test systems to help engineers design, validate and manufacture electronic products. Agilent's broad range of system-ready instruments, open industry software, PC-standard I/O and global support combine to accelerate test system development. More information is available at **www.agilent.com/find/openconnect.**

For more information on Agilent Technologies' products, applications or services, please contact your local Agilent office. The complete list is available at:

www.agilent.com/find/contactus

Phone or Fax

United States:
(tel) 800 829 4444
(fax) 800 829 4433

Canada:
(tel) 877 894 4414
(fax) 888 900 8921

China:
(tel) 800 810 0189
(fax) 800 820 2816

Europe:
(tel) 31 20 547 2111
(fax) +31 (0)20 547 2190

Japan:
(tel) (81) 426 56 7832
(fax) (81) 426 56 7840

Korea:
(tel) (080) 769 0800
(fax) (080)769 0900

Latin America:
(tel) (650) 752 5000

Taiwan:
(tel) 0800 047 866
(fax) 0800 286 331

Other Asia Pacific Countries:
(tel) (65) 6375 8100
(fax) +65 675 50042
Email: tm_ap@agilent.com

Product specifications and descriptions in this document subject to change without notice.

Printed in USA, September 14, 2004
5989-1413EN

Agilent Technologies