The Network Centric Test System

Lynn Wheelwright
Agilent Technologies, Inc.
September 2003 – Presented at Autotestcon 2003

***Abstract*- Network topology is an important choice for the test system designer. There are several to choose from and each has its benefits. A comparison of topologies is made based on the benefits and drawbacks for various usage situations. Some of the topologies of interest are:**

- **Placing the instrumentation and the controller on the corporate intranet.**
- **Using switching hubs for traffic isolation**
- **Using a second LAN connection in the test system controller as a private network for the instrumentation.**
- **Placing a router between the intranet and the test system controller.**
- **Widely distributing test assets**

Test asset visibility to the rest of the network has both security and test integrity implications. Trading off the benefits of ready access and observation (which promotes collaboration) against system visibility needs to be carefully examined. Several use cases will be presented for examination:

- **Simply connected user**
- **Semi automated test**
- **Fully automated test**
- **Remote collaboration for system problem solving**

I. Introduction

The ready availability of high speed networking with its protocols has given the test system designers some new choices for accomplishing their goals. These choices fall primarily into three areas: cost of the connections, speed of the connections, and flexibility of the connections. These capabilities have progressed to the point where they now challenge the capacity and flexibility of the existing IEEE 488 standard (commonly known as GPIB). The discussion presented should help answer the questions: Am I ready for the network? And, what is a network going to do for me?

II. Why Use A Network

Let us examine the cost situation more closely by referring to Table 1. This data was gathered by querying the internet for these prices. For a typical small test system of a computer and one instrument, the cost of the GPIB cable is more than cost of the Ethernet interface and cables. If we extrapolate this to a large system of twelve instruments, it becomes obvious that the cost of networking components is approximately an order of magnitude less than the cost of GPIB. Given today's pressure on cost, the economies of scale of network connections have given them the advantage.

TABLE I
Connection Costs

GPIB		Ethernet	
Interface:	$500+	Interface:	$0 - $50
Cables:	$50 - $100	Cables:	$2 - $6

TABLE 2
Connection Speed

GPIB		Ethernet	
Large Block	<1 MB/Sec	Large Block	1-60+ MB/Sec
Round-trip Latency	0.2-2 ms	Round-trip Latency	0.1-5 ms

Connection speed or throughput is another area where the continued improvement in networking has overtaken GPIB. Table 2 contains some laboratory measurements on both throughput for large data blocks (greater than 100kB) as well as round-trip latency for small blocks (10 bytes). The speed in any given system will vary as a function of the mix of small and large blocks and of the processing speed of the computer and instrumentation processors. If one is willing to use larger block sizes on Ethernet than the normal default, it is possible to achieve 90 MB/second for large block transfers on gigabit Ethernet.

The third area where Ethernet excels is in cable and configuration flexibility. GPIB imposes a limit of 2 meters times the number of devices connected up to a maximum of 20 meters. Ethernet cables are readily available in lengths from half a meter to hundreds of meters and the test system is not constrained by total cable length. This simplifies the design of distributed test systems for physically or geographically large situations.

III. Common Tasks, Terms and Definitions

Before discussing the topologies and use cases of network centric test systems, some definitions are in order. Table 3 illustrates common tasks encountered when using instrumentation with computers. The term 'Remote' implies an action performed through the control port (or at a distance from the instrument). Table 4 defines some common networking terms used in configuring and setting up instruments on a network. Table 5 contains some common networking devices used to build a network.

TABLE 3

COMMON TASKS

Name	Task
Topology	Physically and logically attach an instrument to a computer. Load and configure software.
Remote Help	Find 'How To' information. Display instrument's help on PC screen (possibly served by the instrument to the PC).
Remote Monitoring	View instrument screen on PC and be able to save or copy it to a file or another program.
Remote Front Panel	Graphical User Interface (GUI) on computer which controls the instrument as if the user were using the actual front panel.
Remote Control	Change instrument settings and transfer measurement and signal data to and from instrument
Remote Collaboration	Work with one or more people to solve measurement or system problems. Multiple people monitor or share control of the instruments or system.
Remote Support	Work with third party personnel through firewalls to solve instrument setup, configuration, measurement problems, license issues, update software, or receive training.

TABLE 4

COMMON NETWORK TERMS

Name	Definition
DHCP	Dynamic Host Configuration Protocol—a method of automatically obtaining an IP address for a LAN connected device (computer, router, instrument, etc.)
DNS	Domain Name Service: maps names to IP addresses.
IP	Internet Protocol: requires an address to communicate.
Intranet	Typically, a network within an organization—local in scope to the organization. It usually will have protected access through a firewall to the Internet.
Internet	The publicly accessible wide area IP network (WAN).
LAN	Local Area Network: a network that is restricted in scope or access. Often used as a label to distinguish ports on routers and firewalls.
WAN	Wide Area Network: a network such as the internet, which has broader or public access. Often used as a label to distinguish ports on routers and firewalls.
VPN	Virtual Private Network: a protocol for secure communication between LANs across the public Internet—messages are encrypted, communicating parties are validated as authorized.

IV. NETWORK TOPOLOGIES USEFUL IN TEST SYSTEMS

Fig. 1 illustrates a typical network topology within a company or organization. The number of network segments depends on the size of the organization. A small company may collapse this to only one segment (using one router and firewall). A common practice is to use the built in DHCP server capability present in many routers. Depending on the use of the test system, it may need to be connected to the network within an organization.

TABLE 5

Common Network Devices

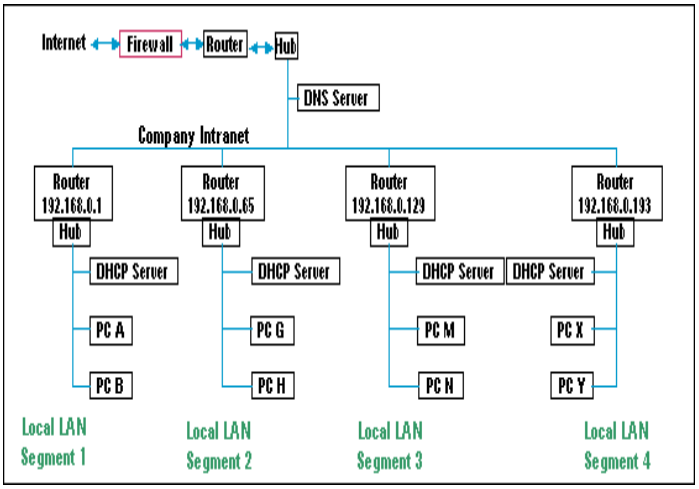
Name	Definition
Hub	A multi-port device, which transmits on all other ports any packet received by any port.
Switching Hub	An intelligent hub that looks at the traffic on each port to determine which addresses are present. It uses this information to switch received packets to the appropriate port instead of blindly sending incoming packets to all ports.
Router	A two port device used to separate a network into localized segments. The WAN port is connected to the larger network and the LAN port is connected to the local segment. This device only allows WAN traffic destined for the local segment through AND forwards packets from the local segment to the WAN when the destination address is outside of the local segment address range—also called a gateway.
Firewall	A two port security device used to examine incoming and outgoing traffic between the Internet and an internal network to prevent unauthorized access. Commonly located in a router or computer which acts as the Internet or WAN gateway.

The simplest topology is a direct connection between one instrument and a computer (Fig. 2). In this case, there is no connection to a larger network. For this connection a cross over cable will most likely be required until it becomes common practice to build all Ethernet ports with Auto MDIX capability (this automatically senses the polarity of the signals and adjusts the connection to match; it's standard on gigabit).

Because the instrument is only accessible from the connected computer, there is no interference possible by other network devices or computers. This provides excellent measurement integrity and security.

The simplicity of this topology makes it useful for field or portable testing (where only one instrument is required). This same simplicity also inhibits any cooperative collaboration or problem solving activities because of the lack of wider network connectivity.

Figure 1. Typical network topology within a company or organization.



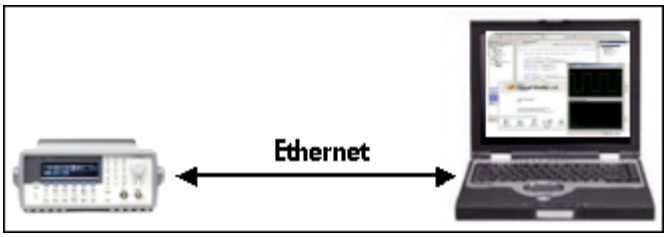


Figure 2. Direct Ethernet connection

The logical extension of the direct connection to more instruments is to use a hub (Fig. 3) between the instruments and the computer. In this case all of the cables would be straight through patch cables (those commonly available in most computer stores or IT departments). The other attributes of this topology are the same as the direct connection.

To take advantage of the power and flexibility of a network with all the possibilities of remote access and collaboration, it is necessary to provide a connection to the larger network. Fig. 4, is the simplest topology using a hub to connect to the local intranet. Unfortunately, connecting the hub to the intranet has some side effects that can degrade test system performance: all of the network traffic is now present within the test system and all test system traffic appears on the intranet. If the test system requires substantial network bandwidth, then measurement throughput as well as overall network throughput will be compromised. This can be overcome if we use a switching hub (now widely available) instead of just a plain hub. The additional benefit of this device is that it isolates each connection from traffic that is not destined for the device at the other end of the cable. This is a very economical solution for improving network throughput.

Another requirement of being on the intranet is that all of the instruments (as well as the computer) must have unique IP addresses on the network. This is most easily accomplished if there is a DHCP server on the network and the instruments are DHCP capable. Otherwise, some negotiations are in order with the network administrator to obtain the necessary static IP addresses. There are naming services available (such as DNS) that allow the use of names in place of IP addresses in test programs and configuration scripts. This is especially important when DHCP is used, because there is no guarantee that a device on the network will always receive the same address when it is powered on. (It is possible to configure a DHCP server to always return the same IP address but many administrators do not like to do this—it defeats one of the major reasons for using DHCP.)

Now that the instruments are visible to the rest of the network there are several advantages that can be utilized. Many of the newer instruments have built in web servers that allow the user to monitor (or control) the instrument while the test system programs are running. This certainly makes life easier for the engineer who has experiments running in environmental chambers located far away. To check on system or instrument status only requires the use of a web browser. A

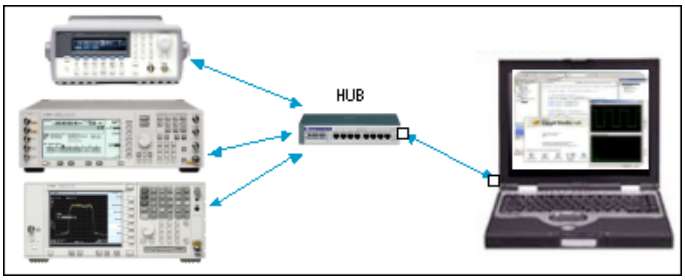


Figure 3. Connecting through a hub

significant advantage of this network visibility is that it opens up the possibility of collaboration with other colleagues. The ability to share screen images and measurement results interactively shortens the time required to solve measurement problems and system design issues.

One aspect of this topology is that it relies on the good behavior of other network citizens. Otherwise, either accidental or malicious interference with the control of the instruments can occur. A way to increase the security of a system is to put a second network interface into the computer. The intranet is connected to one interface and the instruments are attached to the other—which functions as a private LAN. The IP address range 192.168.xxx.xxx has been reserved for private LAN usage. It is possible that many such test systems on the intranet could be configured in this manner. While it is easy for the instruments to access nodes on the intranet (by enabling Network Address Translation in the computer), it is much more difficult for other users on the intranet to accidentally access the instruments. To do so, they must go through the system computer. This requires both the permission of the system computer as well as an appropriate route configuration in the requestor's computer.

To avoid the configuration hassles associated with two network interfaces in a computer, a router is an attractive alternative (Fig. 5). This moves the access protection from the computer to the router. It can allow selective access to the test system as determined by its configuration—thus allowing convenient access to the test system computer but limited or no access to the instrumentation.

For those systems that have stringent security requirements, there are routers available with built in VPN capability. This can be used to restrict access to only those who have the proper digital credentials (the requestor must also have a VPN client).

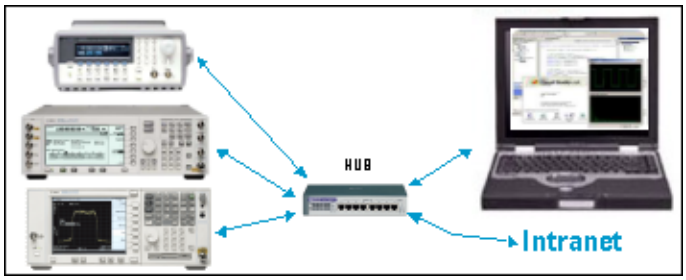


Figure 4. Connecting to the Intranet with a hub

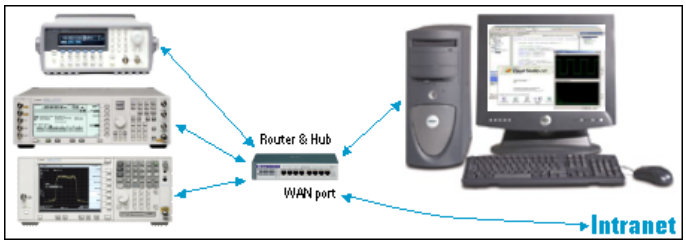


Figure 5. Connecting to the Intranet through a router

In addition, all traffic between the router and the accessing node is encrypted for protection against eavesdropping.

Lastly, for those cases where the test system needs to be directly connected to the Internet, there are VPN capable routers available with built in firewalls. Systems and instruments exposed in this manner are subject to hackers' attempts to penetrate them either for curiosity or for malicious intent. It is important to control and limit all access to only those protocols and ports needed for test system operation. An example of this type of system would be a set of instruments to monitor the health of a mountain top communication facility or placed at the end of a troublesome CATV trunk line.

V. Use Cases

There are several criteria we can use to classify the use cases. The first is: how often will this test be done? If the answer is only once or a very few times, then it may not be worth much time investment to develop a sophisticated test program. The second is: how many measurements or instruments are involved? If the answer here is one or only a few, then the amount of instrument control needed may be none to very little. In fact, it may be sufficient to set up the instruments manually. A third question is: what will be done with the measurement data or results? If the answer is a screen image or a few numbers back from the instrument that can be inserted into a report, then an off the shelf application or an instrument hosted web page is a satisfactory solution for the user.

Taking the answers to the above three questions as stated describes what some people call a "Simply Connected" user. All that is desired is a quick connection between computer and instrument and the gathering of a few screen images or measurement results for a report. Which topology this user would choose depends on the physical layout and the connection convenience. For example, if everything is being done at the user's desk, either the direct connection or a connection through the local Intranet might be appropriate. The other aspect of topology choice is how many of the common tasks from Table 3 would be applicable. If either 'Remote Collaboration' or 'Remote Support' are needed, then the topology choice requires a connection to the wider network and possibly to the Internet.

As the answers to the questions progress from the one or two to where many test iterations or more measurements need to be done, then the user moves into the realm of the "Semi Automated" case. Here, the testing is still reasonably simple, but may happen more often, or at scheduled times (as in a temperature chamber or life cycle test) or the data may need to be collected into a spread sheet. Macro like capabilities are typical of what this user needs—something to capture a simple sequence so it can be repeated later.

When the answers to the questions move toward many iterations of complex measurements which are archived in the corporate data base or filed for quality control statistics, the user is now in the "Fully Automated" case. Typical applications involve production line testing, satellite pre-launch testing, etc. All these are encompass situations where it is worth the investment to create a test system for long term use. Topology choices are now driven by size of the test system and device under test, security needs of the data, and collaboration and support needs.

Up until now, the perspective of the test designer has been used to define the use cases. If that is changed to the perspective of the support personnel, another use case is evident—that of the "Remote Support" case. These people provide consultation, upgrades, configuration management (including inventory and asset management), calibration, diagnostics and demonstrations to help the designer or operator keep the system in operating condition. Often, this involves accessing the system from a distance or through a firewall.

VI. Summary

Several network topologies and test system use cases have been illustrated to help guide system developers in deploying network centric test systems. Often the needs of the Simply Connected user can be met either by the Direct connection or and Intranet Hub. However, the greater measurement integrity needs of the Fully Automated user may call for a router or router with VPN (router setup or configuration is needed to enable access for some capabilities). Table 6 summarizes how the common tasks and topologies interrelate.

Table 6

Topology Versus Common Tasks

Topology	Security Integrity	Remote Help	Remote Monitor	Remote Front Panel	Remote Control	Remote Collaboration	Remote Support
Direct	Best	From Instrument					
Direct Hub	Best	From Instrument					
Intranet Hub	Poor	Y	Y	Y	Y	Y	Firewall Access
Intranet Switch Hub	Poor	Y	Y	Y	Y	Y	Firewall Access
Intranet 2nd LAN	Good	Y	Router Setup	Router Setup	Router Setup	Router Setup	Firewall Access
Intranet Router	Good	Y	Router Setup	Router Setup	Router Setup	Router Setup	Firewall Access
Intranet Router VPN	Better	Y	Router Setup	Router Setup	Router Setup	Router Setup	Firewall Access
Internet Router VPN	Better	Y	Authorized User	Authorized User	Authorized User	Authorized User	Authorized User