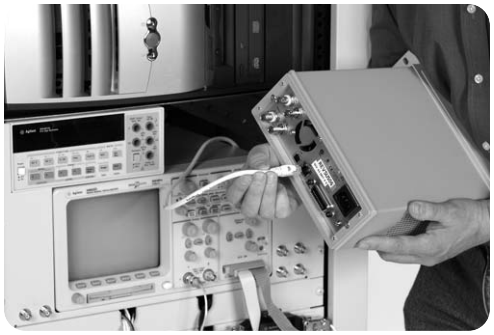
System Developer Guide

Using LAN in Test Systems: Applications

Application Note 1465-14



This set of application notes shows you how to simplify test-system integration by utilizing open connectivity standards. The 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: Applications, the sixth note in the series, offers advice on balancing cost, convenience and security in three common LAN scenarios: sharing instruments, remote monitoring and data acquisition, and functional test systems. These discussions include a look at the issues of public versus private networks and wired versus wireless networks. In addition, advice on configuring a virtual private network is provided, along with a comparison of data rates over various network and protocol combinations.

Please see page 11 for a list of the other titles in this series.

Table of contents

Agilent Technologies

Scenario 1: Sharing instruments

Sharing access to instruments or devices under test is one of the most obvious benefits of connecting test equipment over a LAN and, by extension, the Internet. However, you need to consider the security implications before exposing instruments and test data to any network and the public Internet in particular.

Sharing instruments over an unprotected LAN

The quickest and easiest way to share test equipment over a network is to simply plug LAN-enabled instrument into the local intranet. Most intranets will auto-configure Agilent's LAN instruments so that they can be accessed from PCs by their host name with a VISA VXI-11 address (such as "TCPIP::Jeffs_34980a.sanfran.tmre-search.com::inst0::INSTR"). If the host name is unknown or the intranet doesn't support auto-naming of computers, instruments can be reached via the IP address they are assigned by the local intranet, and local LAN instruments can be automatically found using the new Agilent Connection Expert utility provided with the Agilent IO Libraries Suite 14 connectivity software package.

Most Agilent LAN-enabled instruments have web servers built in that allow access to and control of the instrument from a remote client via a web page. The only information required to connect is the host name or IP address of the instrument and the only software required is a web browser. Moreover, many of these instrument web pages support simple cut-and-paste operations for sending data to or retrieving data from the instrument (see Figure 1).

Sharing instruments over a VPN

Although sharing instruments over a regular LAN is fairly simple, it's not secure—and exposing the instruments directly on the Internet is strongly discouraged. There is little risk for R&D use of the majority of LAN instrumentation, and most modern LAN instruments have some protection against the common viruses and Internet worms. However, security may be a concern for instruments that route or generate powerful signals, such as switches or power supplies, and some older Windows®-based instruments may have insufficient protection from infection by modern worms or viruses.

You can make a local network secure through a variety of methods that isolate it from outside access (see the earlier application note in this series, *Using LAN in Test Systems: Network Configuration*, AN 1465-10), although this of course eliminates the possibility of sharing physically separated resources.

To accomplish secure, long-distance sharing, you can deploy a LAN router that supports virtual private network (VPN) end-points with roaming clients. A VPN end-point feature means that the router can terminate one end of a secure, virtual "tunnel" between two points on the Internet or intranet. These endpoints are often used to connect geographically separated offices of an organization into one larger, virtual local area network. In addition, roaming client capability means that the VPN end-point is also optimized to allow remote PCs to create a direct connection to the router's VPN end-point, rather than just having two VPN-capable routers configured to talk to each other.

Figure 1. Most of Agilent's LAN-based instruments offer built-in web servers that make it easy to access and control instrument functions.

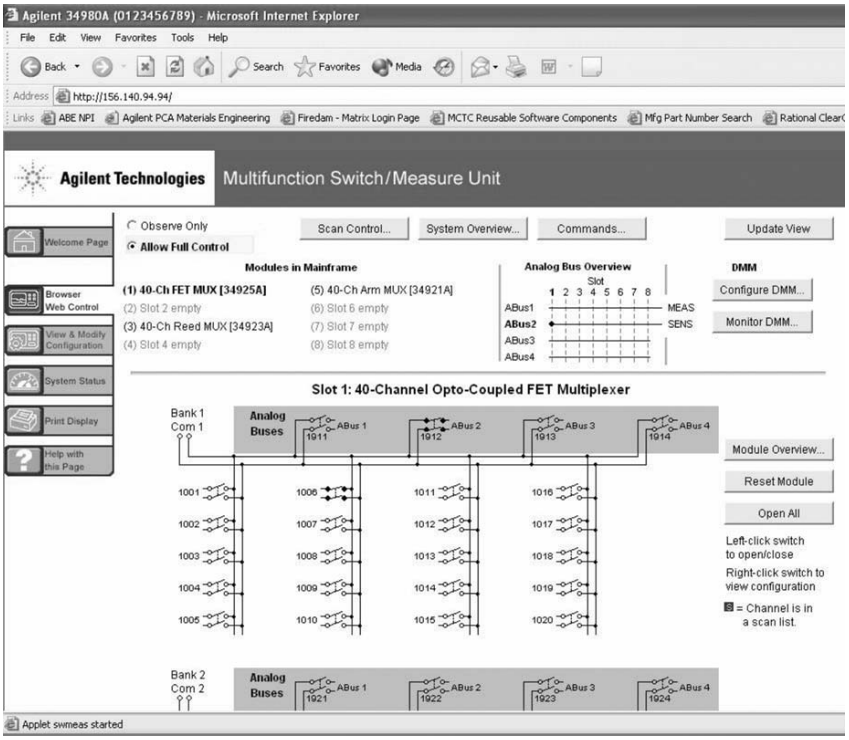


Figure 2 shows the physical layout of such a setup, and here are the basic configuration steps:

1. Physically connect the router and instruments as illustrated in Figure 2.

2. Via the web interface or other means, configure the VPN router's basic DHCP and other network settings to create a simple, private network on which the instruments (and PC clients connected via VPN) can communicate. See AN1465-10 for an example configuration.

3. Configure the router to have a VPN end-point to give roaming users a connection point. Windows XP provides a basic VPN client that supports the L2TP/IPsec and the PPTP VPN protocols, so pick a VPN configuration using one of those protocols unless you have a different preferred VPN client. (See page 8 for more on choosing a protocol.)

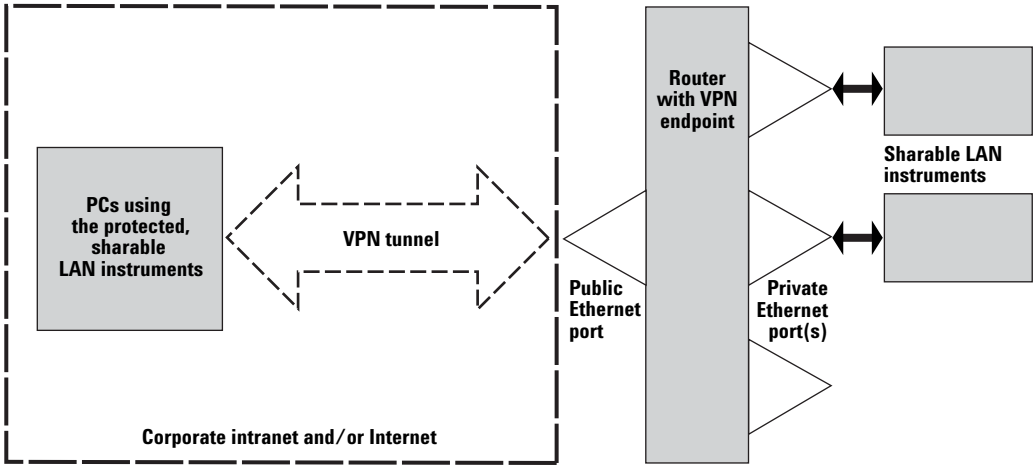
4. Configure your PC. For Windows XP, use the "Create New Connection" task in the task pane of the Network Connections utility that is accessible from the Windows Control Panel. When prompted by the wizard, use the public IP address or host name of the router.

5. After creating the connection, right-click the new VPN connection and configure the VPN type, tunnel name, and password/key you configured on the router.

A VPN router configuration for instrument sharing protects the instruments on the private side of the router from public intranet/Internet access but gives PCs configured with the VPN's parameters and passwords unlimited access to those instruments. (Note that for the duration of the VPN session, the external client PC has two IP addresses—one for the VPN connection and one for the standard intranet/Internet connection.)

By default, the VPN client PC can access only the virtual network behind the VPN router when the VPN connection is active. However, it is possible to configure Windows XP/2000 so that both networks can be accessed at the same time, with Windows deciding which connection to use based on the IP address of the remote device. VPN routers typically use non-routable, private network addresses in the range 192.168.x.x or 10.0.x.x for the private networks they create. If the local intranet also uses private addresses, care must be taken to configure the subnet of the VPN router's private network so that it doesn't conflict with the intranet, otherwise the PC client won't be able to route traffic to the proper network interface (either the real network interface or the virtual network interface created by the VPN connection.)

Figure 2. Using a VPN router to share LAN instruments securely



If you plan to expose instruments on the Internet via a VPN router, you'll need to work with your network administrators to configure the firewalls to allow such direct Internet connections. Your organization may have specific acceptable hardware lists or other policies for such configurations.

Also, when selecting a VPN router, bear in mind that capabilities and performance vary. For instance, most routers support multiple simultaneous VPN connections, depending on the model and the VPN protocol. However, performance can suffer if you initiate multiple connections through a lower-cost router, some of which have data rates less than a megabit/second for VPN connections. Higher-end models have hardware co-processors that handle the encryption necessary to make the VPN secure, which provides better VPN throughput.

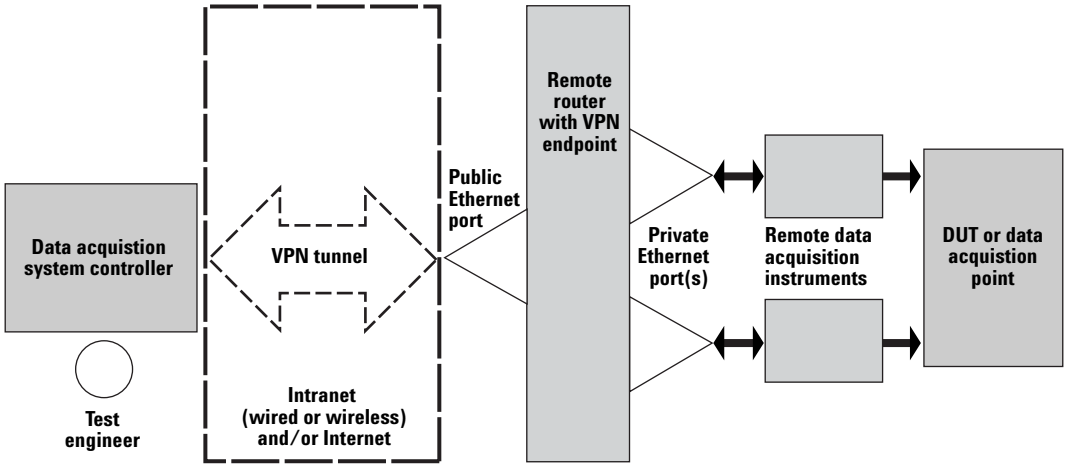
Scenario 2: Remote monitoring and data acquisition

The marriage of LAN technology and LAN-enabled instruments presents an ideal solution for many applications in data acquisition and remote monitoring. For example, the new Agilent 34980A Multifunction Switch/Measurement Unit combines a built-in digital multimeter, a modular mainframe that can be reconfigured for an endless variety of switching or data acquisition needs, and a LAN port for complete remote control of the instrument.

Before you deploy a remote monitoring or data acquisition solution, it's important to temporarily co-locate the controller PC, the remote instruments, system wiring, sensors, and any devices under test in order to complete the initial configuration tasks. Once these major configuration steps are complete, you can usually make most minor changes via the software in the controller PC.

By keeping the test system controller nearer to the engineer responsible for maintaining the data acquisition system (see Figure 3), you can dramatically shorten the turnaround time for follow-on configuration changes. Although this arrangement results in all the acquired data being transferred over the network, TCP/IP and Ethernet are optimized for such data transfers and there is little or no performance penalty for keeping the data acquisition system controller remote from the data acquisition instruments.

Figure 3. Recommended network design for remote monitoring and data acquisition applications.



Remote monitoring and acquisition over wired connections

If the point of measurement is physically located near or in the local corporate intranet, a wired LAN connection is the best choice. In most situations, using a VPN router to provide security is desirable to prevent unauthorized access to the measurement equipment and to prevent infection by viruses. See Figure 2 for the recommended VPN configuration for such a data acquisition system.

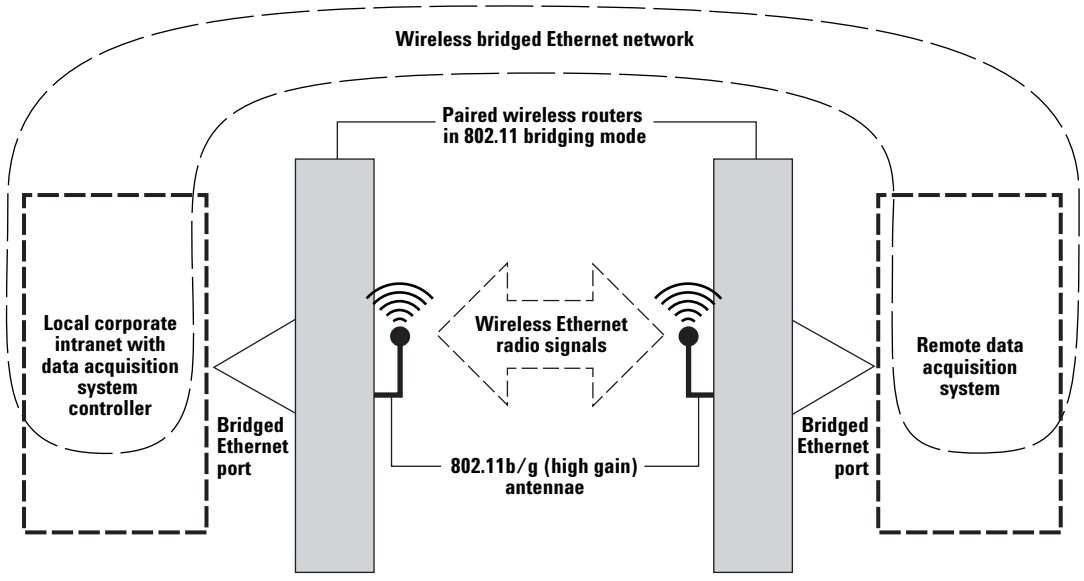
Remote monitoring and acquisition over wireless connections

For a data acquisition point that is not co-located with your LAN, you might be able to use a relatively low-cost wireless LAN (WLAN) solution. If the data acquisition point is within 10 miles of the nearest line-of-sight point of the corporate intranet, a commonly available wireless solution may be possible. Off-the-shelf, high-gain antennae are available for the common 802.11b/g wireless Ethernet standards that can, when properly paired and aligned, create a long-distance wireless Ethernet bridge between two points, connecting two Ethernet networks as though they were local (see Figure 4).

It's important to note that long-distance WLAN installations require specialized knowledge and equipment, and they are highly dependent on terrain and other environmental factors. Due to FCC restrictions on unlicensed equipment in the 2.4 GHz radio band in the United States, the signal cannot be amplified to achieve greater transmission range, but effective range can be increased by using a pair of highly directional (high-gain) antennae.

Because radio signals in the low gigahertz can be impeded by water, such signals are prone to degradation by changes atmospheric conditions and terrain. Consequently, it is not safe to assume an "always-on" connection for a long-distance installation. This might require keeping the system controller computer local to the instruments and point of measurement so that information and control is not lost for periods of time, rather than keeping the controller local to the test engineer for easier maintenance.

Figure 4. Establishing a remote data acquisition connection via wireless LAN



Choosing a wireless technology. Unfortunately, choosing a WLAN technology is not a simple matter, since there is a confusing variety of WLAN standards, both implemented and under development. Although all of these stem from the IEEE 802.11 base standard, you can see from Table 1 that the various single-letter suffixes represent a variety of technologies and protocols within the 802.11 framework.

As you plan a wireless implementation, keep in mind that the data rates you'll achieve in a real-world system are likely to be, at best, half of the rate of the physical layer speed (5 Mbps for 802.11b, for example). In addition, signal loss can limit the speed negotiated between two WLAN radios, and error correction can further reduce effective bandwidth.

Addressing wireless security

A quick perusal of Table 1 should convince you that security is an important—and complex—issue in wireless networking. *Authentication* (are all talking parties who they say they are), *encryption* (can any unauthorized listener understand the communication), and *data integrity* (can any unauthorized party interject or change data in a communication session) are all concerns when anyone can listen on or talk through a public medium such as the airwaves.

The first attempt at a security mechanism for WLAN was wireless equivalent privacy (WEP). At its simplest, it merely describes an encryption and data integrity solution through a private, pre-shared encryption key of 64 or 128 bits (actually 40 or 104 bits when the initialization vector is factored out). Add-ons such as 802.1x permit scalable, enterprise-level authentication. Unfortunately, there is a flaw in the WEP design that allows it to be reliably broken if enough data encrypted with the same encryption key is intercepted. This means that any wireless channel encrypted with WEP could eventually be compromised if enough data passes across the channel.

Microsoft® recommends[1] deploying either WEP plus 802.1x or WPA (or, assumedly, 802.11i when available) for secure, scalable solutions. Of the two, only WPA and its successors can be used securely in non-enterprise-level installations because 802.1x relies on a RADIUS server, such as Microsoft Windows Active Directory (the technology that centrally manages Windows passwords and identities for many corporate intranets).

Table 1. Wireless networking standards

Standard	Type	Description
802.11b	10 Mbps Ethernet in the 2.4 GHz radio band	The most common WLAN standard; being replaced by the faster 802.11g.
802.11g	54 Mbps Ethernet in the 2.4 GHz radio band	The fastest-growing WLAN standard; still operates in the crowded 2.4 GHz radio band.
802.11a	54 Mbps Ethernet in the 5 GHz radio band	A standard that was approved before 802.11 b/g but has taken longer to roll out. Its primary benefit is operation in the less crowded 5 GHz radio band, but it is not capable of the range of 802.11b for the same power level and is more readily absorbed.
802.11 WEP	Weak wireless security protocol	Wired Equivalent Privacy encryption/authentication standard for 802.11 security; has been found to be inherently insecure. If an unauthorized listener captures enough encrypted data, the encryption key can be broken and the security compromised. For example, a few gigabytes are required to break 128-bit (actually 104-bit) WEP keys. Automated tools are available for compromising WEP encryption.
WPA	Strong wireless security protocol	A stronger (as-yet unbroken) encryption and authentication standard for 802.11; an interim specification until 802.11i is approved.
802.1x	Wired or wireless port-based authentication	Applies to all Ethernet configurations but is particularly useful for 802.11a/b/g networks. Forces users to authenticate themselves before being given access to the network, with centralized authentication such as Microsoft Windows Domain servers allowing for an enterprise-wide solution. In wireless access points that support it, 802.1x can be used with WEP encryption to auto-generate WEP encryption keys so that there is a limited period of time that each WEP key is used, preventing listeners from discovering the WEP encryption key and thereby compromising security.
802.11i	Strong wireless security protocol	Sometimes called WPA2, the 802.11 wireless security protocol that will eventually replace WEP; believed to be secure and unbreakable.
802.11n	100 Mbps wide-area wireless network	A not-yet-ratified draft standard that will have roughly 4-6 times the throughput of 802.11g and have greater range than comparable standards. Pre-standard equipment is commercially available.

1 Joseph Davies, *Deploying Secure 802.11 Wireless Networks with Microsoft Windows,* Microsoft Press © 2004

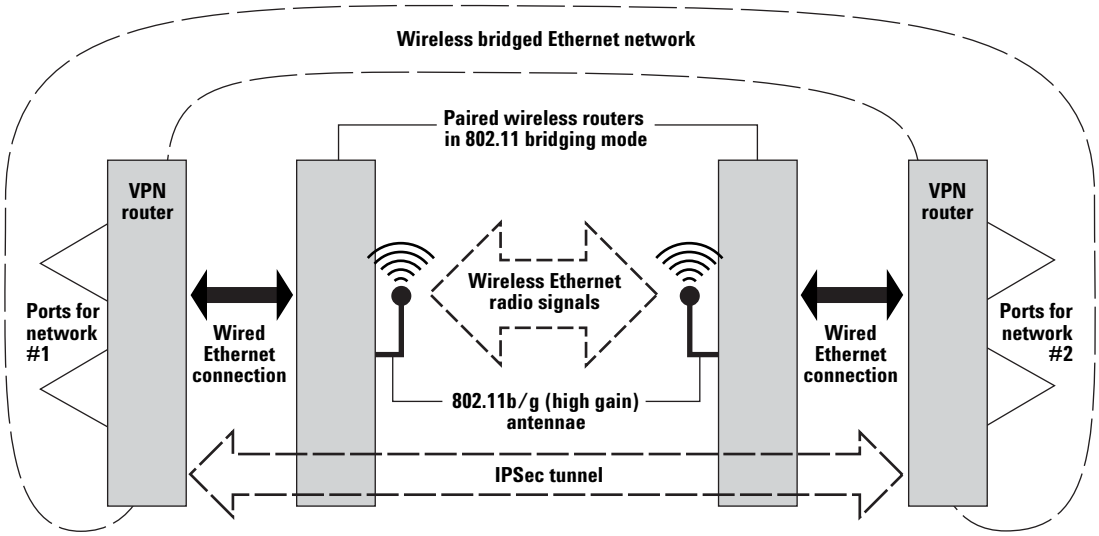
However, WPA may not be available in all possible configuration modes for wireless access points. For instance, in tests at Agilent, we were unable to use WPA with a D-Link DWL-2100AP access point in wireless bridging mode, where two access points seamlessly bridge the two networks they connect into one, larger network. Only WEP security was available in this mode, and we have found no commercial products that claim to implement WPA for bridging mode. If this remains true for 802.11i, we recommend either not using bridging mode for bridging from your intranet or putting two VPN routers on either side of the wireless access points to use secure IPSec communications (see page 9) to guarantee wireless security will not be broken (see Figure 4 for a sketch of such a configuration).

Scenario 3: Functional test systems

Functional test systems represent a third potential for LAN connectivity. In addition to the benefits discussed in the earlier application notes in this series, several points need to be considered when applying LAN technologies to functional test systems: security and independence from network infrastructure, timing, and deployment.

- Application note AN1465-10 discusses security and independence from network infrastructure through the use of static network configurations and inexpensive network router products to create a secure, independent network segment. A second LAN card devoted to a private instrument network is another alternative. You can also establish VPN tunnels to connect distributed test systems to leverage existing network infrastructure to connect testing (and test database systems, etc.) devices and computers securely.
- The issue of timing is often misunderstood with respect to LAN. While it is true that the timing of TCP/IP communications is inherently nondeterministic, that doesn't mean you cannot make timed measurements. IEEE Std. 1588 addresses the challenge of distributed, LAN-based measurements, using precise clocks and timing to achieve synchronicity on the order of 100 ns or better. Agilent is introducing instruments that meet IEEE 1588 requirements, including models in the new LXI (LAN eXtenstions for Instrumentation) format. (Of course, you can always use external timing buses and trigger lines to synchronize LAN instruments that are co-located.)

Figure 5. Wirelessly bridged Ethernet network with VPN tunnel for additional security



- Deploying LAN systems can be more challenging than GPIB systems, primarily because it is often difficult or impossible to use the same instrument address ("resource address" in VISA terminology) when deploying a LAN application from one location or system to another. TCP/IP addresses are 32-bit integers, and in many situations they are globally unique, so they must be changed in order to duplicate a system. With GPIB, in contrast, test engineers can be reasonably certain they can always call their function generator "GPIB::10::INSTR" on as many computer systems as required, since the GPIB primary address is relative to the computer and the GPIB adapter (as opposed to being a globally unique number). The Agilent IO Libraries Suite 14 brings back some of this simplicity by letting you assign a friendly name to each instrument or resource in the form of an alias. For instance, you can assign your function generator any name you like even though it resides at a specific IP address.

Configuring a VPN

Although an endless variety of VPN implementations are available, only a few criteria need to be considered when choosing a configuration for distributed test and measurement applications: (1) Does the application require an always-on connection, or will a temporary connection suffice? (2) What level of security is required? Does the system need to be protected only from inadvertent access attempts, or is powerful encryption and security necessary to prevent deliberate, malicious attacks? (3) What are the available options in the desired price and performance range that meet your other criteria?

This section explores two configurations that can address virtually any combination of these criteria: client/server tunneling and peer-to-peer IPSec tunneling.

Client/server tunneling

Client/server VPN tunnels have become a popular means to allow remote access to enterprise networks. A key advantage of this method is that it can be used over the Internet and over routers and firewalls. VPN tunnels were designed to minimize the impact of firewalls, and updated firewalls can be configured to allow VPN tunnels through, making them the best choice for exposing instruments securely over the Internet. Another advantage of Client/server VPN tunnels is multiple, noncontinuous connections from clients. Server hardware or software designed to support such tunnels allows multiple clients to connect and disconnect from the VPN server at random times for random durations, making these tunnels the best choice for ad hoc sharing (such as is common in R&D labs, for instance).

Approaches

Two common approaches to implementing these tunnels are known as L2TP/IPSec (IP Security with Layer-2 Tunneling Protocol) and PPTP/MPPE with MS-CHAPv2 (Microsoft Point-to-Point Encryption over Point-to-Point Tunneling Protocol with Microsoft Challenge-Handshake Authentication Protocol version 2.) Each of these technologies is a combination of a transport layer and a security layer. The transport layer packages up network communication so that it can be successfully transmitted over the secured, virtual tunnel between the client and server, while the security layer provides protection from deliberate or inadvertent deception or attacks.

The transport layers (L2TP and PPTP) provide similar capabilities, although the newer L2TP is becoming the more common choice. However, the security layers present distinct differences. Of the two, IPSec provides the best support for encryption, authentication, and data integrity; MPPE with MS-CHAPv2 is considered less secure. In general, MPPE with MS-CHAPv2 is good enough for home use and for use over secured intranets, but IPSec is the only truly secure choice for use on or over the Internet.

Implementation notes

Windows 2000 and XP offer built-in IPSec/L2TP and MPPE/PPTP with MS-CHAPv2 clients as part of their dial-up networking support, and all VPN routers have some combination of IPSec, L2TP, PPTP, and MS-CHAP protocol support. The speed of the connection can vary greatly based on the router's implementation, especially if the router has an encryption co-processor built in to offload the computational burden of encrypting the tunneling data. As you would expect, cost typically increases with performance and capabilities.

By default, such VPN configurations turn off any other Internet connection when the VPN connection is active by configuring the default internet gateway to go through the VPN connection. If you don't want this to happen, configure the VPN tunnel to manually create the necessary TCP/IP routing information so that only information addressed for the private network across the VPN tunnel is sent across that tunnel, and all other network connections are sent through the primary network connection.

To provide a working example of client/server VPN tunnel configuration, we've posted detailed instructions and open-source, contributed utilities for establishing an MPPE/PPTP with MS-CHAPv2 VPN Tunnel between a Windows 2000/XP client and a D-Link™ DI-804HV VPN server at **www.agilent.com/find/adn_vpn_examples.** Configuration instructions for connecting a Windows 2000/XP MPPE/PPTP client to a D-Link™ DI-804HV are available at: **http://support.dlink.com/faq/view.asp?prod_id=1439.**

Peer-to-peer IPSec tunneling/bridging

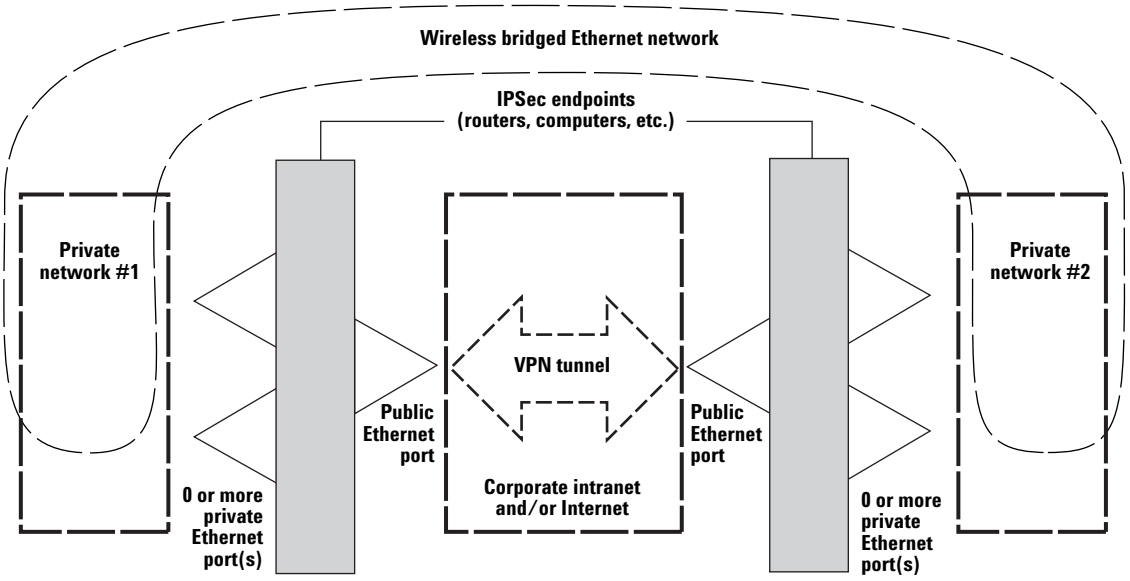
IPSec provides its own tunneling mode where two networks are virtually joined by establishing a secure tunnel between the network endpoints on a larger network, such as a corporate intranet or the Internet. The networks that the tunnel endpoints connect can be anything from a single computer to a large corporate LAN. This tunneling mode is designed for permanent network configurations between two points with known IP addresses or host names (making it peer-to-peer, rather than a client/server architecture). An example application of IPSec tunneling would be to virtually connect two campuses of an organization via an IPSec tunnel over the Internet so that the two ends of the tunnel are combined into one large, secure virtual LAN.

There are a few situations where IPSec tunneling is the preferred choice. Because of the always-on configuration of this tunnel, IPSec tunneling is a good choice for virtually connecting a set of measurement hardware and a controller/monitor, such as in a test system with a remote controller or a remote data acquisition application (see Figure 6). Because the endpoints of the tunnel can be networks of devices, IPSec tunneling is a good choice for connecting two separate test systems or permanently connecting a test system controller.

IPSec tunnels may not work across corporate firewalls, so the tunnel end-point hardware may have to be exposed to the Internet to allow such tunnels to be connected over the Internet.

As part of their IPSec feature set, Windows 2000 and XP provide the capability for IPSec tunneling,

Figure 6. IPSec VPN combining two private networks



although their configuration tools are too complex to use without instructions or experienced help. However, the Windows implementation is very flexible and powerful, allowing traffic destined for the private network behind the remote IPSec endpoint to be automatically encrypted and sent over the tunnel and all other TCP/IP traffic to continue to its destination unimpeded.

Many VPN routers also have IPSec tunneling support, with varying degrees of configuration help. VPN routers without a hardware encryption co-processor can be an order of magnitude slower than the most powerful, more expensive routers with an encryption co-processor built-in. Configuration information and contributed utilities for configuring an IPSec tunnel between a Windows 2000/XP client and a D-Link DI-804HV router are also available at **www.agilent.com/find/adn_vpn_examples.**

Comparing network performance

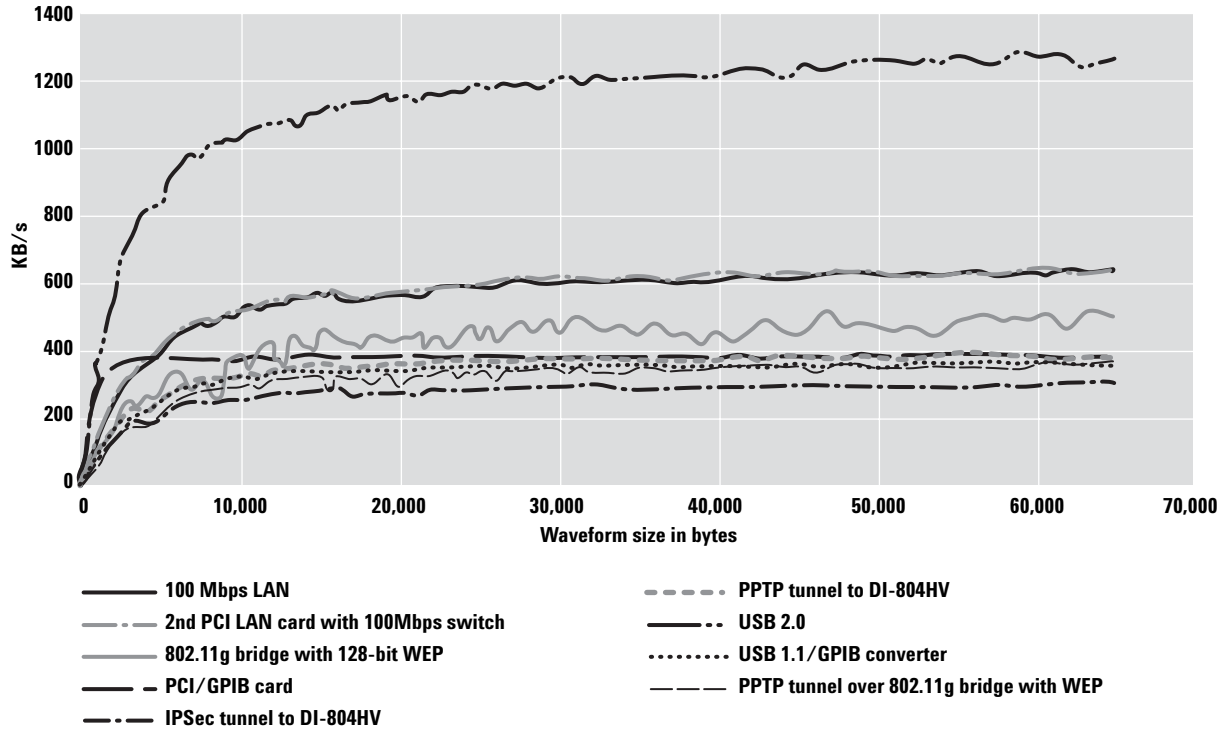
As you would expect, various networks have different performance characteristics, based on a combination of the underlying technology and the specific details of each vendor's implementation. Moreover, various instruments behave differently depending on the I/O connection type as well. Figure 7 compares the data rates measured while uploading a waveform from a PC to an Agilent 33220A function generator over a variety of transports/networks. (The results include the time necessary to upload the waveform, plus the time it took to receive a response from the instrument that it had successfully received the data.)

As you can see from the chart, using a second PCI LAN card to create a private LAN incurs no extra cost compared to using the primary LAN card and the corporate intranet's infrastructure to connect to the instrument. Using an 802.11g wireless Ethernet bridge did incur a small performance penalty, as it is limited to 54 Megabits per second, less than the 100 Mbps LAN. In contrast, using the encryption features of the D-Link DI-804HV VPN router caused some of the slowest results because this model does not have a data encryption co-processor, meaning that the encryption of the data packets has to be done by the router's primary CPU.

Summary

LAN is a powerful, compelling choice for many test and measurement tasks and systems, but engineers need to be aware of its limitations and complexities to create reliable, long-lasting configurations. The huge variety of LAN mediums, devices, protocols, and technologies mean that a large body of complete tools and solutions are available to choose from when designing test systems. Picking the right technologies to use and deploy is essential to developing the best system in the least amount of time.

Figure 7. Comparative data rates over various network/transport schemes.



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

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 different standards and protocols (e.g., LAN to GPIB)

GPIB — general purpose interface bus; the dominant 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

IP — Internet protocol; requires an address to communicate

LAN — local-area network

NAT — Network Address Translation; maps private addresses to one or more public addresses to enable access to intranet or Internet

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

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: Network Configuration,* AN 1465-10 (pub no. 5989-1413EN) **http://cp.literature.agilent.com/litweb/pdf/5989-1413EN.pdf**
- *Using LAN in Test Systems: PC Configuration,* AN 1465-11 (pub no. 5989-1415EN) **http://cp.literature.agilent.com/litweb/pdf/5989-1415EN.pdf**
- *Using USB in the Test and Measurement Environment,* AN 1465-12 (pub no. 5989-1417EN) **http://cp.literature.agilent.com/litweb/pdf/5989-1417EN.pdf**
- *Using SCPI and Direct IO vs. Drivers,* AN 1465-13 (pub no. 5989-1414EN) **http://cp.literature.agilent.com/litweb/pdf/5989-1414EN.pdf**

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.pdf**
- *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 Software Architecture* (AN 1465-4) pub no. 5988-9819EN **http://cp.literature.agilent.com/litweb/pdf/5988-9819EN.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 System Deployment* (AN 1465-7) pub no. 5988-9822EN **http://cp.literature.agilent.com/litweb/pdf/5988-9822EN**
- *Operational Maintenance* (AN 1465-8) pub no. 5988-9823EN **http://cp.literature.agilent.com/litweb/pdf/5988-9823EN**

www.agilent.com

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.**

By internet, phone, or fax, get assistance with all your test & measurement needs

Online assistance:
www.agilent.com/find/assist
Phone or Fax

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

Canada:
(tel) 877 894 4414
(fax) 800 746 4866

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

Europe:
(tel) (31 20) 547 2111
(fax) (31 20) 547 2390

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

Korea:
(tel) (82 2) 2004 5004
(fax) (82 2) 2004 5115

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) 6836 0252
(e-mail) tm_asia@agilent.com

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

Printed in the USA May 17, 2005
5989-1416EN

Agilent Technologies