

Network Security for LXI Systems

BY MIKE DEWEY, EDITOR

The ubiquity of LANs and the low cost of Ethernet are features that make LXI a very attractive alternative to other control bus implementations such as GPIB, RS-232, FireWire, or USB. However, unlike test systems that might be controlled by a localized network such as GPIB, systems that rely upon a LAN or WAN must contend with network security issues.

Depending on the specific architecture and span of connections that comprise a LAN-based test system, the requirements for a secure network can vary from minimal to extensive, with each LXI device and the associated system configuration conforming to a company's IT security policies.

The need for secure networks is universally recognized by all IT organizations. Consequently, implementing an LXI system that uses these same networks requires that test system designers and users apply the adopted policies and procedures to maintain the security integrity of the network.

Understanding Network Security

To understand how the incorporation of an LXI device or the design of an LXI system might impact the overall security of the controlling network, it's important to know the requirements, policies, and methods associated with creating a secure network. Protecting the integrity of your network and the

information transported requires addressing the following questions: How do you protect confidential information that is available on your private network from those who do not explicitly need to access it, and how do you protect your network and its resources from malicious users and accidents that originate outside your network?

Network security involves protecting against a variety of security threats, which can compromise both your network's information and performance. Several of the more common methods of attack include the following:

NETWORK PACKET SNIFFERS

Network packet sniffers can gain access to system-level account information by monitoring non-encrypted packet traffic. User account information, passwords, and even the integrity of the network can be compromised by intercepting network traffic packets.

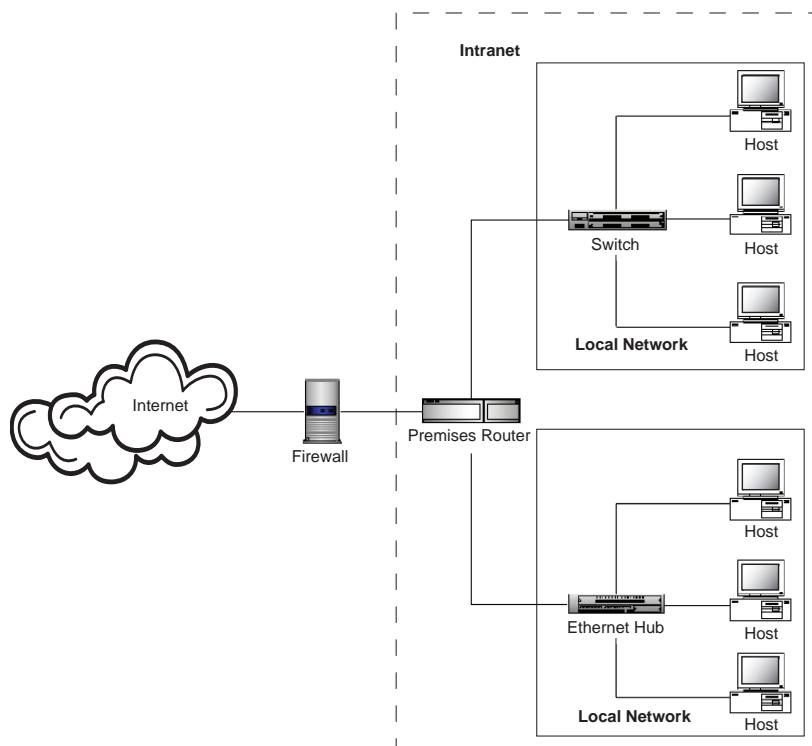


FIGURE 1. TYPICAL NETWORK CONFIGURATION

IP SPOOFING

IP spoofing involves an attacker who can send erroneous or embarrassing e-mail to someone within the organization appearing like it came from a known person within the organization. It also can be used to access user account and password information. The attack could come from within the organization or via a Telnet connection to an SMTP port on the system, which allows the attacker to insert bogus sender information.

PASSWORD ATTACKS

Password attacks can result in an unauthorized individual successfully penetrating the network, compromising a network's integrity. For example, an attacker could modify the routing tables of the network by having all packets routed to him or her for monitoring prior to delivery, effectively becoming a man in the middle.

DENIAL-OF-SERVICE ATTACKS

Denial-of-service attacks are somewhat different from other security breaches because they make a network or service unavailable for normal use. Basically, by overloading a service or server, they can effectively shut down a website or server. Depending on a network's specific architecture and topology, it is possible for a denial-of-service attack to cripple a complete network by flooding it with undesired or useless data packets and providing erroneous information regarding the status of network resources.

APPLICATION-LAYER ATTACKS

Application-layer attacks are probably the most visible or at least the most publicized types of security attacks and referred to as malicious software (malware). Viruses, worms, and Trojan horses are all types of malware.

A Trojan horse is any program that invites the user to run it but conceals a harmful or malicious payload. The malicious payload may take effect immediately and can result in many undesirable consequences, such as deleting all the user's files. More commonly, it may install further harmful software into the user's system to serve the creator's longer-term goals.

Trojan horses also can start a worm outbreak by injecting the worm into the user's local networks. The use of ActiveX controls is a known method for implementing a Trojan horse attack and one of the main reasons that many network computers are configured to disallow the use of ActiveX controls.

A network's vulnerability to security breaches or attacks can vary depending on the network's span or perimeter size as well as the number of access points. Generally, the larger the network, the more vulnerable it may be to security incursions. Types of networks include the following:

- LAN—a network that typically operates within a limited part of a building's floor or area. Private networks also can be classified as LANs.
- WAN—a network of subnetworks that interconnects LANs over a geographical area within a single organization.
- Intranet—a TCP/IP-based logical network within an organization's internal network structure.
- Internet—a global, public TCP/IP-based network that may be used

to interconnect WANs and LANs via a switched or a virtual switched connection using the Internet cloud.

- Virtual Private Network (VPN)—a network where data packets from an internal network are transmitted over the Internet using encryption to ensure a secure connection, resulting in a virtual private connection.

FIGURE 1 details a simple network that incorporates some of these network topologies.

Regardless of the network's complexity or size, establishing a secure network involves defining the security perimeter of your network; that is, the outer bounds of the network where traffic is monitored and managed to and from your network as well as defining what users are trusted. To ensure network security, all external interfaces to your network must be controlled including connections to the Internet, PCs, modems, and other network devices including instruments such as LXI devices.

All LXI devices conform to current TCP/IP networking standards. When they are connected to a LAN, they will operate in a defined manner. In the case of a network fault such as a duplicate IP address, they will have a benign effect on the network.

Depending on the type and size of a network, various network components will be used, some for simply interconnecting various network devices and others that provide not only connectivity but also a level of security. Network components for interconnecting Ethernet devices, LANs, WANs, and network infrastructure include hubs, switches, routers, and firewalls. Routers and firewalls are key components for constructing a secure network perimeter.

Routers provide the capability to interconnect and isolate multiple networks via high-level protocols such as TCP/IP. They also allow devices within a network to hide their presence from the wider network or Internet to create small, private networks.

A router is aware of all devices that are connected to its interfaces and based on routing tables. Data packets are sent to their appropriate destinations or another router for further routing. Many routers also contain security features that function as a simple firewall by filtering packets on individual interfaces based on source and destination IP addresses.

For example, a router that interfaces to a Web server can block all traffic except for that addressed to port 80. The term port in this case refers to a virtual slot in a TCP and UDP stack and is used to map a connection between two hosts. Ports are numbered from 0 to 65535 with the range 0 to 1023 being marked as reserved or privileged and the remaining ports marked as dynamic or unprivileged. For a well-known service such as HTTP, TCP port 80 is used by Web servers to establish a TCP connection with a user.

Although routers may incorporate a simple firewall, they generally will not filter packet payloads; an actual firewall is required to support this capability. A firewall's primary job is to protect a network from outside security threats and incursions.

However, unlike a personal firewall that a desktop computer may use, a network firewall can have two or more interfaces with traffic passing into and out of the firewall. It monitors traffic crossing network perimeters and imposes restrictions according to security policy. Firewalls typically are used to separate internal (private) and external

(public) networks. As data passes through the firewall, packet source and destination IP address, source and destination ports, packet payload, and other characteristics are examined to determine whether the packet should be allowed through the firewall.

Essentially, a firewall implements an access control policy for a network. For example, to eliminate vulnerability to outside attacks, the firewall can be configured to block access to well-known TCP/IP port-specific services such as Telnet, FTP, or SMTP. If your network requires an FTP site, it can be located outside the firewall in a perimeter network area, also known as a DMZ.

If the firewall has been configured with an appropriate rule set, malicious packets will not reach the Web server. However, it should be noted that firewalls alone are not sufficient to guard against malicious traffic.

Computer viruses can pass through firewalls undetected. As a result, it is essential that all users of the network adhere to an antivirus policy that includes the use of up-to-date antivirus software on all PCs and Windows-based instruments that may be connected to an intranet or Internet.

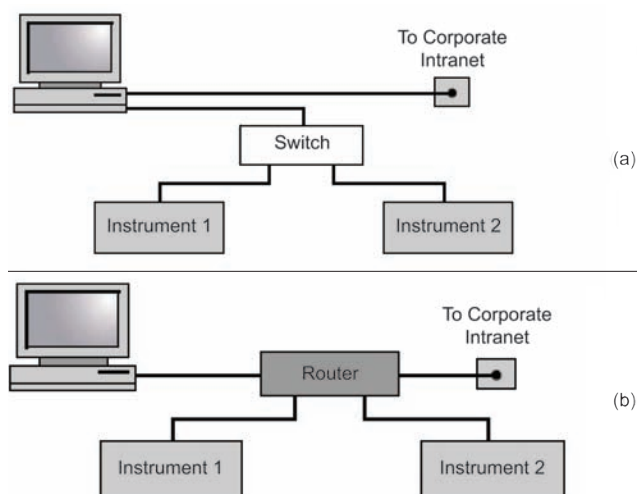


FIGURE 2. SUBNET CONFIGURATION

Figure 2a. Private Network With Separate Network Interfaces to PC and Intranet. Figure 2b. Router Isolated Private Network

Networks and LXI Devices

With a basic understanding of networks and security, test system designers can better determine how to best use LXI devices securely within a network. A test system's overall physical location requirements and the span or complexity of the network interconnecting LXI devices will largely determine the security measures needed to ensure a secure LXI test system network. In some cases, simply the configuration of the network may be sufficient to ensure a secure network; for more complex topologies, the use of security policies and hardware may be needed.

A local network is the most simple network configuration case and referred to as a private network or subnet. Creating a subnet for all LXI devices that are part of a test system, particularly if all devices are physically collocated in a system, guarantees that device control will not be compromised by other non-test system LAN traffic.

Additionally, a subnet provides protection against network viruses or worms by isolating the test system from the corporate intranet or Internet. A properly configured router supports the creation of a subnet by using a feature called network address translation (NAT), which allows the subnet devices to hide their presence from public networks. This is accomplished by using a private set of IP addresses that is not accessible from the public side of the router, effectively isolating the subnet from any other network.

Alternatively, a private LAN can be created by using a dedicated network card that interfaces to LXI devices via a switch or hub. If a network error does occur within the subnet, the error condition is isolated without impacting the rest of the network. **FIGURES 2a** and **2b** depict the dedicated network-interface and router-isolated implementations.

With a subnet, any Windows-based PCs and LAN-controlled Windows-based instruments connected to the network must have updated antivirus software. However, since most LXI devices use a non-windows OS, virus attacks on these devices are not likely. Consequently, they do not normally include virus protection.

The most likely means of virus infiltration into an isolated network will be via portable memory devices where malware can be introduced via a memory stick or floppy disk. When connected to a corporate network, even via a router, devices with a USB, floppy disk, or any other I/O port represent potential security holes in a security perimeter. Consequently, it is incumbent upon the user to not only protect network devices, but also to ensure that malware is not introduced via one of these security holes, which could then propagate throughout your corporate network.

A more complex network for interconnecting LXI devices incorporates two or more subnets. For example, a test system distributed within one facility might require interconnection among several subnets via the company's intranet (**FIGURE 3**).

For this type of network topology, the overall network security is achieved by isolating various network functions to minimize exposure to security breaches as well as manage user access to specific devices within the network. This type of topology relies upon routers and firewalls to manage access and filter traffic to and from the internal network to ensure no malicious payload can enter or leave the organization. Deploying additional firewalls between the routers and the Web servers can prevent malicious traffic from reaching servers and subnets.

Behind the network's firewall, the premises router separates the various subnets according to specific activities or tasks. For example, a distributed LXI data acquisition system may comprise several different subnets that represent geographically different locations within a facility.

Access to and isolation of these subnets are managed by the premises router via filtering rules established by a network administrator. In this way, a virtual network of LXI devices can be created with access limited to users needing to control and manage the test system.

If other users are present on a subnet that is part of an LXI system, it is possible for these users to access an LXI device, disrupting your test or data acquisition session. This is because LXI devices presently

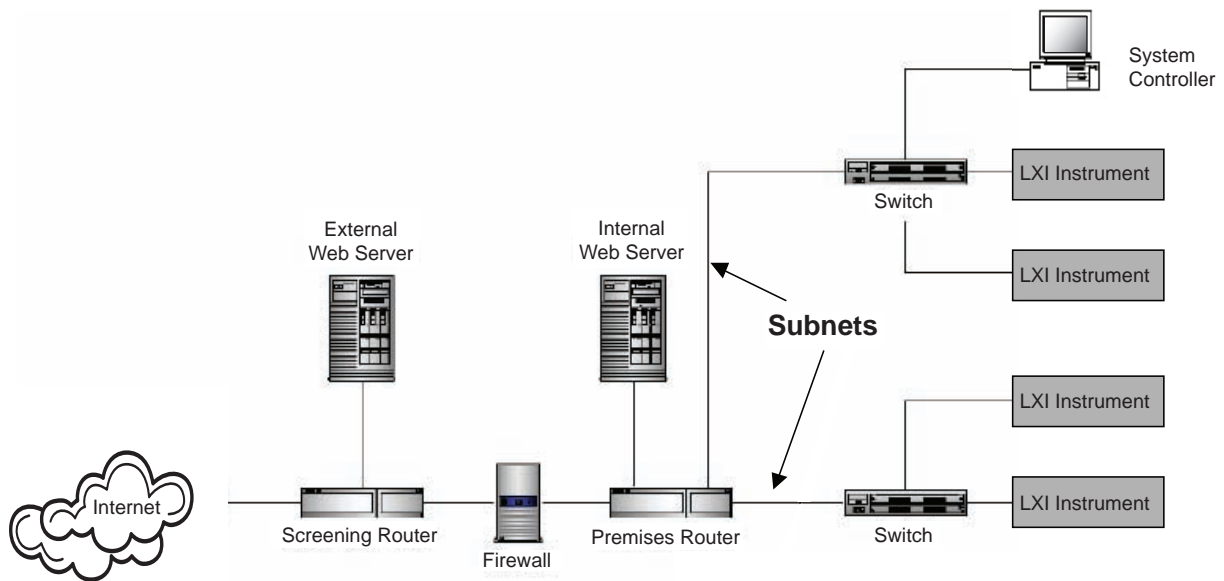


FIGURE 3. INTRANET TEST SYSTEM CONFIGURATION

cannot create a locked LAN I/O session between the instrument and a controller, which ensures a stable connection and blocks other attempts to access the instrument for the duration of a session. However, by properly constructing your subnets and working with your system administrator to manage user access, you can mitigate unauthorized access to LXI devices and maintain the integrity and reliability of your LXI system when using an intranet connection.

LXI devices also can be controlled over great distances. It is conceivable that a distributed test or data acquisition system might require instrumentation located at two distant facilities.

As shown in **FIGURE 4**, this type of network topology might involve two distant groups of LXI devices interconnected by perimeter routers that are, in turn, connected via the Internet. However, since the Internet is an unsecured network, creating an end-to-end, secure connection via the Internet requires a VPN.

VPNs offer a variety of features and capabilities. However, the primary criterion to consider regarding a VPN is whether the connection is temporary or always on. These types of connections are supported by client/server tunneling or peer-to-peer IP security (IPSec) tunneling, respectively.

The temporary connection allows access to WANs via remote clients and supports the access of instruments located on a remote, secure network. This type of VPN allows multiple clients to be connected to the remote devices and is most appropriate for test system networks requiring ad hoc access by various users. Two common approaches to implementing these tunnels use 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.)

Alternatively, for a test system or data acquisition that requires a dedicated connection between two or more remote networks, a peer-to-peer VPN connection will provide a permanent, secure end-to-end connection between two distant perimeter routers.

Some key points associated with the use of VPNs include the following:

- VPNs are capable of transporting secure traffic over unsecured networks via the use of tunneling which uses a combination of transport and security layers to transmit data over routers and through firewalls.
- IPSec provides the best support for encryption, authentication, and data integrity and its own tunneling mode, establishing a secure, always-on tunnel between two networks. It is the only truly secure method for communications via the Internet.
- Many routers support VPN connections as well as IPSec tunneling support, providing a secure, always-on connection. However, VPN routers without a hardware encryption co-processor can be an order of magnitude slower than a router with a built-in encryption co-processor. This may be a concern if your distributed test network has moderate to high data bandwidth requirements.

Like the intranet/WAN-based system, you still need to know what devices and users are present on each of your subnets so judicious configuration of each network is necessary to ensure overall system performance integrity. In addition, coordination with your network administrator is required to establish the correct type of VPN connection.

Finally, in spite of all the security infrastructure features present within a network, it is imperative that all Windows devices connected to your network, no matter where they are physically located, be protected with antivirus software. Any unprotected I/O port or device within the perimeter of your virtual network offers the opportunity to compromise not only your local network, but also your company's entire network. With a potentially large system with multiple devices located in remote locations, the need to adhere to security policies and procedures is more acute.

Summary

The requirements for building a secure test system will be primarily determined by the complexity of the overall network used to control all LXI devices. A local system with several devices connected to a single switch will have very minimal security requirements, assuming that all devices are located behind a common firewall and

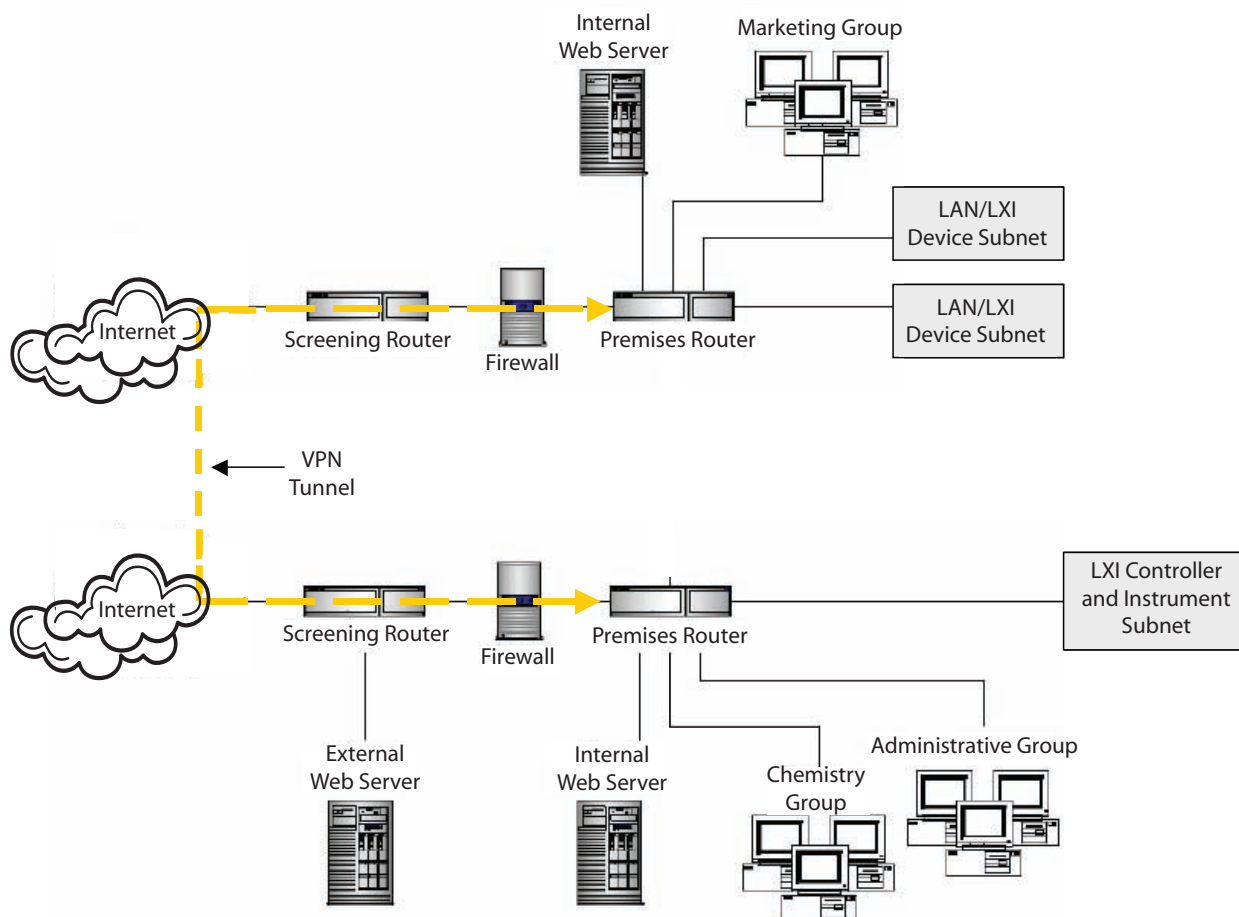


FIGURE 4. DISTRIBUTED TEST SYSTEM WITH VPN

the PC is isolated in some way from the intranet and Internet.

LXI systems that move beyond the use of a local network no doubt will be subject to a company's IT security policies, automatically providing a level of network security equal to all other devices connected to the same WAN. In this case, the combination of firewalls and IT security policies will most likely provide sufficient security.

Distributed LXI systems that use the connectivity of the Internet will need to leverage all of the security measures defined by an organization's IT department. Tools such as VPNs and authentication policies will need to be leveraged to construct a secure, distributed LXI test system.

Even with all of the best network security hardware, a secure network still requires that everyone adhere to the IT department's security policies. Just like all other devices that are connected to the network, LXI devices represent potential security risks. Connecting to your corporate intranet and the Internet means observing the same security policies for LXI devices that are used for any other device connected to the network.

Additional Reading

1. Internetworking Technologies Handbook, Cisco Systems.
2. Zimmerman, S.C., Secure Infrastructure Design, CERT® Coordination Center, 2002.
3. *Using LAN in Test Systems*, Application Note 1465-14, Agilent Technologies, 2005.

4. *Using LAN in Test Systems*, Application Note 1465-10, Agilent Technologies, 2004.

5. Firewalls FAQ, <http://www.interhack.net/pubs/fwfaq/>

6. Curtin, M., *Introduction to Network Security*, Kent Information Services, March 1997.

7. *Network Security Basics*, Secure IT Consulting Group, 2002.

ABOUT THE AUTHOR

Mike Dewey, the marketing product manager at Geotest-Marvin Test Systems, previously has held various positions in design engineering, engineering management, marketing, and product management with GenRad/Teradyne, ADR Ultrasound, and Motorola Government Electronics Group. He is a member of the IEEE and has served as a board member for both the PXI Systems Alliance and the VXI Consortium and been an LXI Consortium advisory member on the marketing, technical, and physical working group committees. Mr. Dewey received a B.S.M.E. from Syracuse University and an M.S.E.E. from Georgia Institute of Technology. e-mail: miked@geotestinc.com

