

## **Building a Secure Ethernet Environment**

By Frank Prendergast  
Manager, Network Certification Services  
Schneider Electric's Automation Business  
North Andover, MA

The trend toward using Ethernet as the sole communications network for business and industry has raised concerns about security. While proprietary networks for building or factory automation have major drawbacks in terms of limiting information flow and higher cost, their separation from other systems provides a measure of protection against unauthorized access. So how do you take advantage of the benefits of Ethernet connectivity within a secure environment?

A comprehensive security plan must protect against unauthorized access from both internal and external sources. Methods of security can range from technologies based within the infrastructure itself such as physical connection paths and Virtual Local Area Networks (VLANs) to hardware and software-based devices such as firewalls and security management servers.

### **Logical & Physical Security**

The most secure network, of course, is one that has no connections to other systems. But that defeats the major advantage of Ethernet--its easy connectivity to other Ethernet networks or the Internet for information sharing.

One of the most often-overlooked security measures is physically securing switches and wiring closets. Something as simple as enclosing devices in a lockable cabinet or closet and limiting access to authorized persons can prevent tampering or accidental de-coupling of a device link. In addition to physically preventing unauthorized access, it also makes sense to secure a backup copy of switch configurations using TFTP (Trivial File Transfer Protocol), a feature found in many switches, each time a change is made. This is not only a security measure but also a recovery method if a device should fail and require replacement.

Another method of easily securing infrastructure devices such as switches is password protection. Out of the box, most switches can be accessed using a serial DB9 console connection. This management interface is used to assign an IP address for remote TCP/IP-based telnet management.

Default passwords for switches may be standardized across a manufacturer's entire product line and are published in product documentation and on the web. Many users, including IT organizations, fail to change the default passwords and permissions. If an unauthorized user reaches an unsecured switch, he or she would be in complete command of the switch with the ability to change configurations or disable ports. It is therefore essential, even without an Ethernet connection to the corporate LAN or Internet, that physical security and password protection is part of any security program.

### **TRANSPARENT READY® Security**

Web-enabled TRANSPARENT READY devices from Schneider Electric such as CONNEXIUM® switches and FACTORYCAST® modules for programmable logic controllers (PLCs) have extended functionality with graphical interfaces, web hosting and Java/ActiveX controls. Once installed on a network, the default password on each device should be changed and additional user IDs created as necessary to restrict services to authorized users only.

PLC programming tools such as Schneider Electric's CONCEPT® software and SCADA programs such as MONITOR PRO™ can also be configured to have varying levels of access to user logic and other components. Some of the CPUs in Schneider Electric controllers are also equipped with keys to allow the CPU to be started or stopped and to protect the internal memory. These keys should be removed and distributed to authorized personnel.

Particularly in large environments, documenting code changes, device and infrastructure changes and cabling identification is the key to maintaining the security of devices and programs that may be serviced infrequently.

### **Routing & Switching Security**

As the sophistication of an Ethernet network for building or factory automation grows, features once found only in enterprise class devices are finding their way into daily use at the workgroup level. Access control features can be configured in some switches and routers to allow only specific workstations to access a device or pass through to a target. These features include "Virtual LAN" implementation, port security, password implementation and access control list filtering on supported switches and routers.

These special features may not be available on some manufacturers' products or models, so it is important to check each vendor's capabilities before specifying or purchasing a particular product. These features may also require specialized skills to configure and administer.

### Physical Security

Physical security is crucial to a secure operating environment. Switches and routers must be held in place in a secure and sturdy fashion, preferably installed in a rack or enclosure in a secure area. Network equipment is usually equipped to be restored to factory defaults should a password be forgotten. For this reason, all ports including console and auxiliary ports should be secured by a lock or located in a lockable enclosure to prevent unauthorized access.

### Port-based security

Port security on a switch can prevent unauthorized users from plugging in devices, such as workstations or printers. Devices like these could disrupt network operations by introducing excessive amounts of traffic and possibly errors. Administratively disabling unused ports will prevent traffic from entering the network if an unauthorized device is plugged in.

Additionally, port-based hardware address (MAC address) management may be used on a switch in order to deny access to a non-authorized device. Service will not be provided if a non-configured MAC address is sensed. This can also be used as a precaution against connecting more than the allotted number of workstations or devices to a port. If a device is replaced with one having a different MAC address, the port assignment must be appropriately re-assigned by the network administrator.

Access lists can also be utilized on supported switches and routers to permit or deny users from gaining access to specific network devices or specific resources on network devices. This is commonly known as packet and service filtering and is placed on certain interfaces. Using access lists ties up processor resources, however, and has to be locally administered on each interface within each routing device. As a result, access lists are not always the most optimal way to secure resources. Proper setup by a professional is crucial when using these filtering devices, since improper setup could render the network inoperable.

### Access control lists

An example of access control list implementation is to allow a programmer to program a device but to restrict the programmer from accessing the device from a web browser. An access control list is used to accomplish this. The list would allow the programmer to access the device via his workstation, but would prevent the destination port from being port 80, the port a web browser would use to connect to any http host.

### **Virtual LANs**

Virtual LANs are a grouping of Ethernet ports on an IEEE 802.1Q compliant switch or a grouping of switches. A VLAN may be used to help isolate packet and broadcast traffic on a factory automation network, for example, from the IT network. Measures like this are generally reserved for isolating extraneous traffic such as broadcasts that may interfere with control communications, but can also be implemented as security tools.

Switches can be divided into VLANS that could render devices on separate VLANS unreachable. The downside to switch port-based VLANS as a security strategy is management, since a port can belong to multiple VLANS extending across multiple switches.

Multi-layered VLANS can be challenging to administer. For multiple VLANS to span multiple switches, the Spanning Tree Protocol, STP, may have to be disabled as well. For example, if two VLANS exist on each of two switches, each VLAN needs a

connection to the corresponding VLAN on the other switch, requiring two links between each switch. STP will disallow multiple links between devices to prevent loops.

VLANs can also be used to segment broadcast domains within a network. Since VLANs are logically segmented local area networks, physical areas do not restrict them. Utilizing VLANs reclaims network bandwidth by breaking down broadcast domains and segments one network of devices from another within the same switch.

VLAN segmentation is accomplished by assigning the ports of a device into separate VLAN memberships. For example, ports 1 and 2 may be assigned to VLAN1. Ports 3 and 4 may be assigned to VLAN2. Ports 1 and 2 will not see broadcasts or traffic from ports 3 and 4, and vice versa. This separation is accomplished at OSI layer 2. If a third VLAN were created using ports 1, 2, 3, 4 and 5, then a device on port 5 would see all broadcast traffic from ports 1, 2, 3 and 4.

An example of this type of implementation is if the network administrator wants to separate traffic from office computers from PLC or SCADA devices. As these devices may not normally communicate with each other, separating them with a VLAN would allow the two networks to co-exist on the same switch.

Other configurations can be implemented in order to conserve bandwidth for automation or other control devices. These settings include whether or not to pass or block multicasts and rate limit broadcasts. Other technologies such as Quality of Service (QoS), IEEE 802.3p, can prioritize packets on seven levels by setting three bits in the packet header. This allows traffic types or port assignments to have a higher priority should a bottleneck occur and can be very useful to prioritize automation traffic. Though not specifically a security measure, it does preserve the integrity of an automation network.

## **Firewall Technologies**

A firewall is a device that is implemented on a network to provide security from potential intruders. A firewall has more granular control over what can and cannot be accessed from outside the secure network than an access list can provide. A firewall can be a

network appliance or a piece of software on a stand-alone server or router equipped with multiple network adapters or interfaces. A firewall provides this granular control by using its own protocol stack and, depending on the firewall, it checks each level of the stack for erroneous information.

Network appliance firewalls are a bundled, ready-to-run single purpose computer that provides an operating system and firewall application. The device is tuned for service as a firewall and is managed from a secure workstation "inside" the firewall. These may be helpful to enterprises as a self-contained solution.

Other firewall manufacturers provide software that installs onto an existing PC or UNIX workstation with multiple network adapters dedicated to this task. In both cases, some providers offer add-on software and hardware modules for remote authentication and encryption/decryption accelerators for improved performance. These configurations may be helpful to enterprises that require scalability, more interfaces or other features.

A firewall works by examining each packet that passes between the two adapters and comparing access rules at several different levels before allowing that packet to pass. Once a packet has been validated by all of the requirements to pass through, the firewall applies network address translation (NAT). NAT is used to hide the internal network IP addresses by substituting the actual source address with the outside address of the firewall. This acts to hide the original internal address of the sender inside the firewall.

Firewalls allow filtering on MAC addresses, IP addresses, port numbers or even certain commands and services. Each firewall offers a different level of security depending on the vendor, features and costs. Selecting and implementing a firewall into any infrastructure requires research, planning and feature/cost comparison.

Every vendor offers a different set of features, such as authentication support, logging, additional memory and performance classes. The more security checks performed, for example, the slower transactions will take place. Some firewall management suites also allow rules to be downloaded and applied to other network devices such as routers that may be internal or external.

## **Authentication Technologies**

Password management for devices can also be an issue. Server platforms are available to centrally administer passwords. These services include RADIUS (remote authentication dial-in user service) and TACACS/TACACS+ (terminal access controller/access controller system). These services allow the secure centralized maintenance of logins and passwords. Access to a device, network or resource such as a server can be centrally administered on such a server. When users request access to a device, the user's credentials are checked against a database on the server for permission.

Authentication is the process where a network user establishes an identity. Verifying the identity of a user requires at least one of three authentication factors: a password, a smart card or token with hardware or software and biometrics. Each of these approaches has different advantages and drawbacks.

Passwords can be forgotten or shared, compromising the original goal of security. In addition, passwords can be stolen by monitoring keyboard keystrokes or network traffic, by tricking individuals into revealing their password or with brute force methods such as dictionary attack utilities.

Smart cards or tokens work in conjunction with hardware or software on the host, so each generated response is unique for every login. While providing strong security measures, smart cards and tokens can be lost or stolen or forgotten, and must be issued and tracked, so they are more expensive than passwords to implement and manage.

The strongest single approach is biometric authorization, such as fingerprint or retinal or iris scans or voice or facial recognition. Although it achieves a higher level of security, users also face more inconvenience as a consequence.

## **Secure Remote Access**

As more and more employees find themselves on assignment outside the office, the need for remote access continues to increase. Remote access servers (RAS) and virtual

private network (VPN) are two technologies that offer remote access service. Remote access is vital to organizations for sales, support, branch offices and off-site partners.

With RAS, a remote access client uses the telecommunications infrastructure to create a temporary physical circuit with a port on a remote access server. With VPN, a VPN client uses the Internet to create a virtual point-to-point connection with a remote VPN server.

Although RAS has proven popular, many businesses are looking at low-cost VPN to perform the same functions and reduce telecommunications costs. A VPN can be defined as a means for using the public network infrastructure, such as the Internet, to provide private, secure access to applications and corporate network resources for remote employees, business partners and customers. With a VPN deployed across the Internet, virtual private connections can be established from almost anywhere in the world, providing secure access to a central network without having to dial directly into the corporate network.

VPNs reduce telecommunications costs since the remote user need only connect to a local Internet access point rather than dial long distance. A VPN uses a secure tunneled connection, allowing only authenticated users access to the corporate Intranet. With tunneling, each message packet is encapsulated or "wrapped" within an IP packet for transmission across the public network via an encrypted "tunnel." Encapsulation is presented at the security server or firewall. Upon authentication, the packet is then decoded and unwrapped for forwarding to the destination host.

There are a number of widely used VPN protocols, including L2TP, IPSec and SOCKS5. These protocols are the building blocks used to create VPN links. Some of the protocols overlap in functionality and offer similar but complementary capabilities.

Virtual private networking solutions may be a combination of many different technologies such as encryption, user and data authentication and access control techniques working together to deliver a VPN solution that protects data privacy and ensures appropriate access control. The technologies that comprise the security component of a VPN are authentication, data encryption, user access control and event logging.

The most important differences between VPN and RAS are the client/server software and the communications access. VPN is a much less costly approach in terms of telecommunications, equipment and personnel costs and administration can easily be handled by mid-level IT personnel. It is also a more secure approach since user and data authentication and encryption capabilities are inherent in the software.