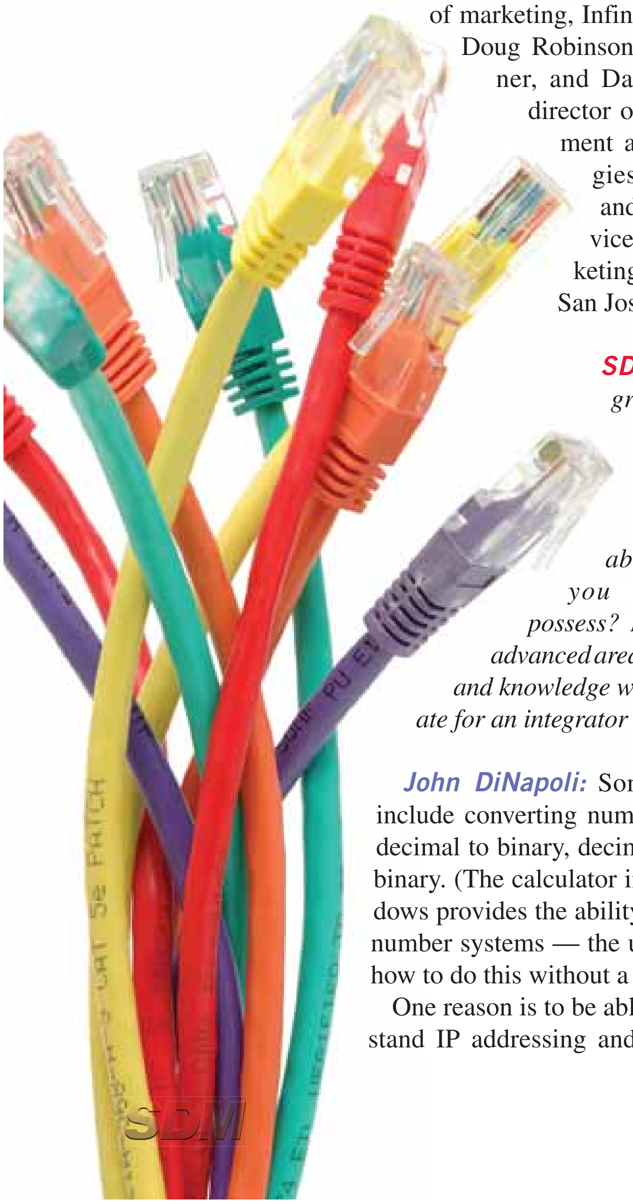
IN THE TRENCHES

Tips for preparing your technicians for field access control work.

By Laura Stepanek, Editor

There is a wealth of information available in the access control industry to help prepare technicians for the field work of installing and implementing a successful network-based access control system. Classroom training is one way to gain this expertise. An informal sharing of knowledge is another way. SDM asked several experts who work with access control integrators every day to share their experiences. Providing tips and techniques on preparing for a network solution are: John DiNapoli, vice president of marketing, Infinias, Fishers, Ind.; Doug Robinson, managing partner, and David W. Barnard, director of dealer development at RS2 Technologies, Munster, Ind.; and Dennis Geiszler, vice president of marketing at Keri Systems, San Jose, Calif.



SDM: *For an integrator to install an access control system on a data network, what basic knowledge about networks do you recommend he possess? In addition, what advanced areas of network skills and knowledge would be appropriate for an integrator to master?*

John DiNapoli: Some of the basics include converting number systems, e.g. decimal to binary, decimal to hex, hex to binary. (The calculator in Microsoft Windows provides the ability to convert these number systems — the user should know how to do this without a PC.)

One reason is to be able to better understand IP addressing and how to be able to subnet the Classes (A, …, E) into networks and host addresses.

Other basic concepts integrators need to understand include

- Networking protocols, such as TCP/IP (what they are and what they do);
- The difference between UDP (Unigram Data Protocol) and TCP (Transport Control Protocol);
- DHCP — what it is and how it works;
- The differences between a hub, a router, a mid-span and a switch;
- IP addressing (IPv4 today; IPv6 soon) and how it works;
- PoE and PoE+ (What are the differences? Which pins carry power, data? How much power is required by a PoE device? How to determine the power-per-port of the mid-span/PoE switch, and if the switch can provide the max watts per port for the application;
- Simple command prompts, such as ping, regedit, ftp and ipconfig.

My recommendation for formal training is Cisco Certified Entry Networking Technician (CCENT).

Doug Robinson: They should understand how basic TCP/IP networks work in general.

Skills to know include:

- How to assign an IP address, subnet mask and gateway address in a device and what these different pieces of information mean and where to get them.
- How to use basic TCP/IP commands such as the PING utility to verify network connectivity.

Use of network "sniffer" or packet monitor software would be helpful for advanced troubleshooting.

Dennis Geiszler: If we are talking about Ethernet or TCP/IP networks, a reasonable understanding of network principles and network device deployment is needed. Knowledge of MAC addresses, TCP/IP (network) addressing and subnets would be necessary.

If the installer isn't proficient in all areas, they should subcontract with a dealer who is, or bring in a network consultant for the project.

SDM: *In designing or planning a network-based system for a customer, what must an integrator ask about the customer's network and the way it is configured?*

John DiNapoli: Will the customer's network be using static IP addresses or do they have a DHCP server? When they configure their device, some only use static IP addresses; some only use DHCP.

They should be working in conjunction with the IT manager, stating that they're going to need IP addresses and which they are going to use.

They also need to ask what subnet range of IP addresses will be allocated for use by the access control devices.

Third, do they plan to use PoE? Some customers will have corporate standards, and others won't know what it is. If they have a large infrastructure already, finding some IP ports won't be difficult. It also depends on how close they are to a router or a switch. Some AC devices support PoE and others don't. There is a new standard coming out that provides more power. We can support up to 450 mA of power, which covers most electric strikes, but not mag locks or long-range readers and biometric readers.

Doug Robinson: Is it a TCP/IP-based network? What network speeds are supported (10MB, 100MB, gigabit, etc.)? Does the backbone support POE (Power over Ethernet) connections? Are there any firewalls present (ports may have to be opened for communication to the access control devices)? Is there a wireless backbone, and if so, what protocols and encryption methods are supported?

David W. Barnard: If the customer has multiple facilities, they may or may not be connected over a Wide Area Network (WAN). If they are not connected over a WAN, you may need to use other communications methods such as modem/dial-up communications, create a Virtual Private Network (VPN) or other method to make use of the World Wide Web.

Some of these options are not readily recognized by some systems integrators and end users. Most of them require the opening up of "ports" in the customer's firewall, which requires that great care be taken not to expose the customer's network to the outside world.

Dennis Geiszler: Ask about what bandwidth is available, especially if video will be running on the network. Access control data uses very little bandwidth, but moving video around on a network can affect both general network speed and video system performance.

It may sometimes be necessary to run a separate TCP/IP network for the security system, especially if the customer's IT manager has concerns about network traffic and reliability. It is important to know how a customer's network is configured, especially if there are multiple locations with multiple subnets, and what other devices and subsystems may be sharing the network. ■

For more information, log onto www.nist.gov, www.infinias.com, www.rs2tech.com and www.kerisys.com.

Let's Get Specific

What are some of the ways in which your company's products/solutions provide ease of installation?

Doug Robinson: We include a utility for our non-Web-based panels to allow one step configuration for the network communications parameters. Our new controllers have a Web-based user interface for ease of setting the network communications parameters. All of our access control hardware ships with "Quick Reference Sheets" so necessary connections can be made quickly and easily from a single sheet of paper instead of having to read a large installation manual to get them installed.

John DiNapoli: Wiring at the door is the same — the main differences are: CAT5 from the eIDC (Integrated Door Controller) to the nearest switch minimizes the cost to install. PoE can provide power to the readers, sensors and strike. Upon power-up, the LEDs on the eIDC blink out the IP address. The eIDC supports both static IP and DHCP; factory default is DHCP.

The eIDC is 100 percent intelligent; it will work standalone if there is a problem communicating with the server. With its built-in Web server it can be used as a standalone device; just enter the IP address into a browser and manage it.

Dennis Geiszler: When designing a system, we try to do as much as possible to automate the installation to minimize the effort the installer has to make and to avoid any potential places where they could make a mistake or be confused. As technology moves forward, that isn't always easy because we try to stay at the forefront, but we know that anything we can do to make a dealer's life easier and more profitable will benefit them and ultimately Keri in the long run.

Keri's Auto USB networking solution has an easy USB plug-and-play scheme using off-the-shelf parts that simulates a TCP/IP network for our NXT Ethernet-enabled hardware platform.