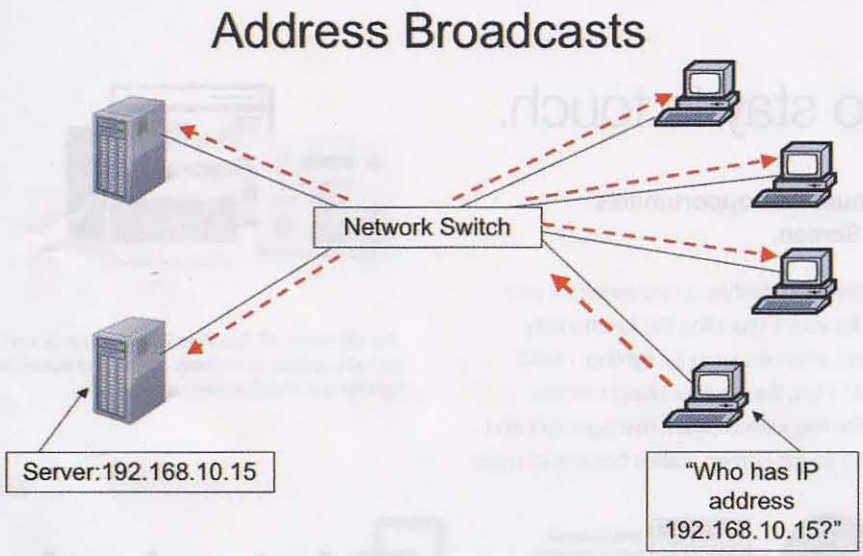
by David Engebretson, Contributing Technology Writer

IP NETWORK TESTING

Avoid the 7 Deadly Sins of IP Programming & Installation

In church one Sunday, my mind wandered during the assistant pastor's sermon on the Seven Deadly Sins. I realized a couple of key issues: first, that I might be guilty of sloth (whatever that is), and also that there are a number of mistakes that can be made in connecting IP devices to clients' networks that can cause serious problems for their network communications. So let's take a look at the Seven Deadly IP Programming and Installation Sins that can render our customers' networks and/or our IP security devices *hors de combat*.

1. Duplicated IP address on the LAN. In most cases our devices (DVRs, NVRs, IP cameras and encoders) need static IP addresses so they can be located by the authorized users and so that port forwarding and firewall manipulations can be established to provide for remote Internet connectivity. Because of the relationship between IP and MAC addresses, it's critical that every device on a LAN, be it a physical security device or not, must have a unique IP address. When one computer tries to reach another device on a LAN, a "broadcast" packet is sent to every device on the network and basically asks, "Who's got IP address 192.168.10.15? If you're out there, please send me your MAC address because I need to communicate with you." If two devices have the exact same IP address, based on their location on the network and the speed of the switching equipment, the broadcast request might be answered by one machine at one time, while the other device might answer a second time. A duplicated IP address can wreak havoc on a LAN, and technicians must ensure that the static IP address that they program into an IP-enabled security device is not in use by anything else on the network. After selecting the address use the "ping" command to check that the address is not in use, and make sure that the address selected does not fall into the range of dynamic DHCP addresses issued by the network server.



Devices find each other on LANs by sending out "broadcast" packets. If two (or more) devices have the same IP address, the sending computer will not receive the same MAC address each time it broadcasts.

2. Not testing for Internet bandwidth prior to connecting IP cameras/encoders or video devices. Internet connections are like two pipes — one going up to the Internet (uplink) and one coming down to the clients' DSL, cable modem, or other broadband connection (downlink). If the goal is to provide video that can be viewed remotely, it's important to test the client's uplink bandwidth, as this will determine how many frames per second and at what resolution/compression settings. To test for uplink bandwidth, go to http://myspeed.visualware.com/index.php from any Internet-connected PC on the client's LAN. After a couple of minutes the results will be provided. What you're looking for is the size of the uplink and also the "Quality of Service," which in the case of this test means packet loss. If the size of the uplink is less than 500 kbps and/or the packet loss is in excess of 5 percent, either of these conditions may cause erratic remote video viewing. Test the client's Internet connections to avoid future failures and frustrations when