Tech Note - 20

Surveillance Systems that Work!™

GUARD DOG Surveillance Systems

Computer Networking - Simplified

When it comes to Information Technology system design and maintenance, commercial business owners often rely on "outside suppliers" or if the operation is large enough, an on-board IT professional (or staff of professionals). This short piece is certainly not intended to replace the knowledgeable IT gurus, rather, to help small business owners understand the basics of network design so they can, without fear and the expense of professional assistance, configure a network DVR for remote access on their network or from the Internet.

The Router

First, in simplified terms, a router is nothing more than an information gate keeper with internal directives that can be set to allow (or disallow) information (data) to pass from one point to another. In addition to being the hardware crossing guard typical routers also provide a portal to the outside world (a spot for an Internet connection) as well as a few (4-16 usually) wired connections (Ethernet, Cat-5 typically) to other computers and/or other network connectable devices (printers, hub switches, etc.). Additionally, many routers today also have wireless communication capabilities. Like (or in addition to) their older wired brothers (sisters) all the internal functions of a wireless router are the same as a wired router – just the wires are replaced with relatively low powered wireless communication capabilities. Before we can configure the router, we need to first understand some basic networking principles.

Internet Connections

Internet Service Providers (ISPs) grant Internet connection service in two basic IP (Internet Protocol) configurations – Static and Dynamic. Static IPs like their name suggests, remain the same while dynamic IPs change from connection time to connection time. Static IP service is generally a bit more expensive (in the range of $75 to $100 and up depending on up/down transfer rates - bandwidth) than dynamic IPs ($10-$75 depending on up/down transfer rates - bandwidth) and service fees are generally reoccurring monthly expenses.

Bandwidth

Technically speaking, bandwidth is the width of the range (or band) of frequencies that an electronic signal uses on a given transmission medium. In this usage, bandwidth is expressed in terms of the difference between the highest-frequency signal component and the lowest-frequency signal component. In computer networks, bandwidth is often used as a synonym for data transfer rate - the amount of data that can be carried from one point to another in a given time period (usually a second). This kind of bandwidth is usually expressed in bits (of data) per second (bps). Occasionally, it's expressed as bytes per second (Bps). A device that works at 57,600 bps has twice the bandwidth of a modem that works at 28,800 bps.

Conversationally, bandwidth is analogous to a water flow in a pipe. When water pressure is constant, a ½" diameter hose would provide less water (over a given period of time) than would a 4” diameter pipe. In this example the 4” diameter pipe would be said to have a higher bandwidth than the ½” diameter hose.

Tying it all Together

A group of inter-connected computers (or computer devices) is called a Local Access Network or LAN. Each device (computer, cash register, printer, etc.) connected to the LAN has its own unique ID Number or Internal IP Address. The LAN itself also has a unique ID Number this is called a Subnet Mask. The subnet mask and the internal IP address work together to provide both network communication and network security functions. Yet another group of ID numbers called Dynamic Naming Service (DNS) exists to identify and differentiate .com .org or .net (as examples) and to provide recognizable word-name addresses (like Microsoft.com, Google.com, etc.) rather than obscure 32 bit ID numbers (such as 209..232.56.18 etc.). All these ID numbers work together (behind the scenes) so that when a user types, “www.google.com” (for example) the information from the Google Website is returned to the specific device (computer) on the specific subnet mask on the specific network that made the request.

So… why might all this be important?

Network Considerations

For OWNER SIMPLICITY sake the DNS ID and the external IP address (the number you need to type to get access to your new DVR) is provided by your ISP but all the rest of the ID numbers noted are internally assigned by the individual given the task of network administration. That said, while Windows (2000 & up) will automatically assign internal IP addresses to connected devices it is usually better practice to manually define the internal IP addresses. Remember, the goal of this Tech Note was to gain a basic understanding of network administration and how to work with “The Gate Keeper”, “the system traffic cop” – The Router.

Also remember, the router’s purpose in the system is to direct and restrict traffic (information flow) between network connected devices. By manually assigning device IP addresses it’s far simpler to keep straight what should be going on where and thus how to configure the router’s internal traffic signals.

Specific Direction

Rather than try to explain how the traffic flow is monitored let us simply provide some simple IP address naming directions. In the end, like knowing how to drive rather than understanding how the internal combustion engine works, is most helpful. It's usually good practice (when considering network design) to maintain the internal LAN (Local Access Network) naming configuration the same at each facility. If the internal IP address for one facility’s router is 192.168.0.1 then that should be the internal IP address for each router at each location.

Likewise, since each computer will have its own internal IP address, perhaps the accounting computer at each location is assigned the number 10. Its IP address would then (given the same convention) be 192.168.0.10. Other computers having to do with your business’s operation might then be #'d 11-19 and would receive IP addresses of 192.168.0.11, 192.168.0.12… to 192.168.0.19.

Cash registers (if not now) eventually will be IP based as well and simply connect to the system via the router or a simple network switch. They might be assigned 20's numbers. Example: 192.168.0.20, 192.168.0.21, etc.

Finally, each peripheral device (like a DVR computer) will have its own set of IP #'s, perhaps beginning with 30... Example: 192.168.0.30, 31, etc.

All this may seem as clear as Polynesian Argil (which I doubt really exists) or it may be fully understood... I don't know. Nonetheless, the upshot is to come up with a standardized convention that can be expanded upon well into the future then make it the same for each location.

Whatever the convention, in order to connect our DVR to your network and ultimately to the Internet, we need to know what IP address (internal) to assign to the DVR. We also need to know the Subnet Mask of the network, the Default gateway (of the router) and the Preferred DNS Server address. These are all terms any respectable IT Professional will readily understand.

Router Port Assignments (Sometimes called Port Forwarding)
Whoever is setting up the new router will need to port assign (fwd) the following router ports **to the IP address designated to the DVR**... This is IT Speak for, "It's OK to open the door to this computer... but don't you dare open the same door to any other device on the network.

Port 80	-	Firewall exclusion for DirectWeb
Port 3000	-	Image transmission
Port 3001	-	Command (including PTZ) transmission
Port 3003	-	Setting information transmission
Port 3007	-	Network transmission speed and bandwidth control
Port 8800	-	Audio data transmission

If this sound like Polynesian Argil, there's NO NEED for a PANIC ATTACK... all this configuration can be done at any time without harm to any data or the internal function of all systems involved.

GuardDog Surveillance Systems, Inc.
N3183 State Road 16-26
Juneau, WI 53039
(920) 342-0703
WEB: www.guarddogvideo.com