network
MONITORING
In the early 1980’s, while the industry struggled with the limitations of pulsed analog communication formats, the founder and president of DMP asked, "If two or more computers, separated by the globe, can talk in real time, why can’t alarm panels and a receiver do the same?"

DMP saw in this emerging computer networking technology the potential to drastically improve the way alarm panels and receivers communicate.

With networking technologies in mind, DMP began to design, develop and perfect the industry’s first Network Monitoring™ systems. Some 20+ years later, the DMP vision has become a patented, UL-listed reality for the modern world, where networked digital data communications are the new standard.
DIGITAL DATA, TODAY’S TECHNOLOGICAL STANDARD

Digitized voice-data has been in use for several years by telephone companies to increase the efficiency and reliability of the Public Switched Telephone Network. So you probably use digital data communication every time you use the telephone in your home or office.

Email and Instant Messaging are two more familiar types of digital network communication that have become common communications tools because of their speed and low cost. Another form of digital communication, only recently available to the public, is VoIP (Voice Over Internet Protocol), which dramatically cuts the cost of long-distance voice communications. VoIP uses digitized voice to allow voice conversations over the internet.

HOW RELIABLE IS NETWORK MONITORING?

The beauty of Network Monitoring is that it doesn’t rely on a server or a dedicated path for its communications. Instead, it communicates redundant signals via a network of paths to ensure...
reliability. The Internet doesn't break. It's always there, just on the other side of your Internet Service Provider (ISP).

DMP Network Monitoring meets UL 'AA' High Line Security requirements by having the panel communicate with the receiver at fixed intervals, as often as once per minute.

Because the receiver knows when to expect each check in from the panel, the receiver generates an alarm if the expected check in doesn't come in on time, to let the central monitoring center operator know that the panel's network path needs attention. This way, system personnel can be alerted before system users are even aware of a problem.

DMP Network Monitoring equipment has been approved by the National Institute of Standards and Technology (NIST), and provides 128-bit encryption to the signal to satisfy the toughest security application requirements of the U.S. government.

For the first time ever, the City of New York Fire Department has approved the use of DMP cellular and DMP network communicators for primary fire alarm signaling to central stations.
HOW DOES NETWORK MONITORING WORK?

You don’t have to be a networking genius to install or program a DMP panel for Network Monitoring. By default, DCHP mode is enabled in the panel. The panel will automatically request an IP address, gateway address, and subnet mask for you. To connect to the panel, TCP trapping can be used. If DHCP is not supported by the particular network that is being used, ask the local network administrator for the following:

- IP address for the panel to use (LOCAL IP ADDRESS)
- IP address of the gateway router (GATEWAY IP ADDRESS)
- The network’s SUBNET MASK (we won’t talk about this here, but the network administrator will know what it means)
- That the local gateway’s Port 2001 (or whatever the panel’s ALARM PORT is set to—ask the monitoring center) is opened bi-directionally to allow UDP and TCP protocols. Panel signals go OUT and acknowledgements come IN through this port.
Once the panel’s NETWORK OPTIONS have been programmed with this information, Network Monitoring works like this:

1. The alarm panel is connected to your local area network, or LAN, and is programmed to send signals to the receiver’s IP Address supplied by the monitoring center.

   Every piece of equipment connected to ANY network (computers, printers, routers, alarm communicators, etc.) has an IP Address that identifies the equipment to the network.

2. Your local network has a piece of equipment, called a gateway that separates your network from, but also connects it to, the Internet.

   The panel is programmed to use your network’s gateway to send signals from the local network through your Virtual Private Network (VPN) or the Internet – no server required!

3. The receiver, usually located off-site, is also connected to the network via a gateway. The network connection looks something like this:
4 All signals sent from the panel include to and from IP address information and are sent over the local network, through the gateway and broadcast to the ‘outside world’.

Other networks’ gateways use the signal’s to and from IP address information to route the signal along the least congested network avenues to its final destination.

Signals may travel to the receiver using one route this time and an alternative route next time, if necessary.

But only the monitoring center’s gateway allows the signal to pass through to the receiver’s IP Address.

5 When a signal is received, the receiver sends an acknowledgement back to the panel’s IP Address and the cycle is complete.

If the panel does not receive an acknowledgement from the receiver, the panel keeps trying to send the signal. After a number of attempts, the panel can signal another receiver via a pre-programmed backup IP address or dialer backup.