

APPLICATION NOTE

Introduction	1
The Network Monitoring™	
Advantage	2
Savings	2
Speed	2
Quality of Service.....	2
Security.....	2
How to Further Minimize the Risk.....	3
DMP Network Communication	3
iCOMSL™ Routers	4
XT Series/XR100N/XR500N/XR500E Panel Operation.....	5
Network Monitoring at a Central Station.....	5
Important Compatibility Information..	5
SCS-150 Main Processor Card	5
SCS-150 Compatibility	5
What the System Administrator Needs to Know	6
Internet Access Requirements.....	6
The DMP Advantage.....	6
Bandwidth Usage.....	7
Recommended Number of Standard Line Network Accounts.....	7

Introduction

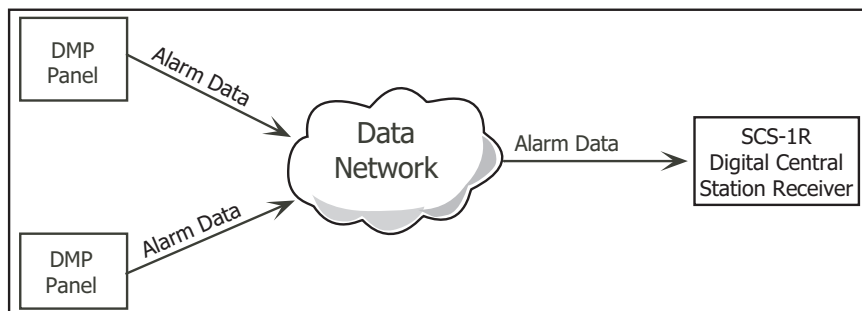
DMP forged the way to a new era for the security and fire alarm industry with the first UL certifications for Network Monitoring™ for burglary in 2001 and for Commercial Fire in 2002. The ability to monitor alarm signals over the Internet offers many advantages for central stations and alarm subscribers. Data transmission is secure, extremely fast, and fully supervised. DMP offers all of this value at a significant cost savings over traditional dial-up or dedicated line communication.

Sending alarm and system information to a central monitoring station through the Internet is not only superior to analog communication, but it is also a communication method approved and accepted by Underwriters Laboratories (UL) for Standard Line Security and for Commercial Fire using the communication protocol patented by DMP and protected under U.S. Patents 6,040,770 and 6,255,945. Before you configure your panel or central station for Network Monitoring, determine whether it must comply with Standard Line Security or ANSI/UL 864 Commercial Fire.

All DMP XT Series™, XR100 and XR500 Series panels offer built-in network options. However, for third-party panels or as a stand-alone option, the iCOMSL Router is the answer.

Each DMP SCS-101 Network Line Card is capable of monitoring 3,200 accounts that require check-in or up to 65,535 accounts that do not require check-in.

This document demonstrates how to take advantage of the options for Network Monitoring using existing corporate Data Networks and the Internet.



DMP NETWORK MONITORING™ OPTIONS

APPLICATION NOTE

The Network Monitoring™ Advantage

Network Monitoring offers a significant advantage for both central stations and alarm customers in terms of savings, speed, quality of service, and security.

Savings

By using a full-time Internet connection, company internal LAN/WAN, or Point of Sale (POS) network already available in many business locations, the costs of adding and maintaining an additional phone line are avoided, as are any long-distance charges between the panel and central station. Using Network Monitoring with DMP equipment, central stations can increase their Recurring Monthly Revenue (RMR) by offering Standard Line Security and ANSI/UL 864 Commercial Fire to a national or international area without the expense of a private leased line for each account.

Speed

Central stations gain an advantage through Network Monitoring speed. Dial-up alarm transmissions average from 5 to 45 seconds. The typical time needed for a Network Monitoring alarm transmission is 50 to 70 milliseconds. In cases where each second counts, Network Monitoring allows the fastest possible alarm responses.

Quality of Service

Network Monitoring allows central stations to offer customers increased quality of service. If a panel at each location attempts to communicate an opening report over a traditional phone line, it is possible for some panels to receive a busy signal from the central station receiver. Because Network Monitoring communication occurs in a matter of milliseconds, many more accounts can communicate with the receiver in a short period of time.

Security

Risk to central station receivers is minimal with Network Monitoring. If you compare the risks of Network Monitoring to the risks traditionally associated with the Internet, the most common hacker targets do not exist. Network Monitoring reduces risks due to:

- Root access can be restricted to Local Only
- Operates using single-purpose devices
- No web site to deface
- Does not accept e-mail or executable files (the most common way to distribute viruses)
- Receiver operating system does not accept commands from host communication
- Proprietary operating system and alarm message format that is unfamiliar to hackers

Furthermore, it would be extremely difficult for a hacker to break into a panel or central station receiver through the Network Monitoring connection because several pieces of unfamiliar information are required to gain access. A potential hacker would have to know all of the following:

- Account number
- IP address
- Port number used by system
- Panel secret remote key
- DMP proprietary communication protocol

How to Further Minimize the Risk

Just as with any other form of central station communication, there are measures you can take to improve your security and reliability level.

- Use a packet filtering network router
- Restrict the panel root access to Local Only or prohibit telnet access
- Consider a backup ISP provider
- Use strong passwords consisting of both letters and numbers

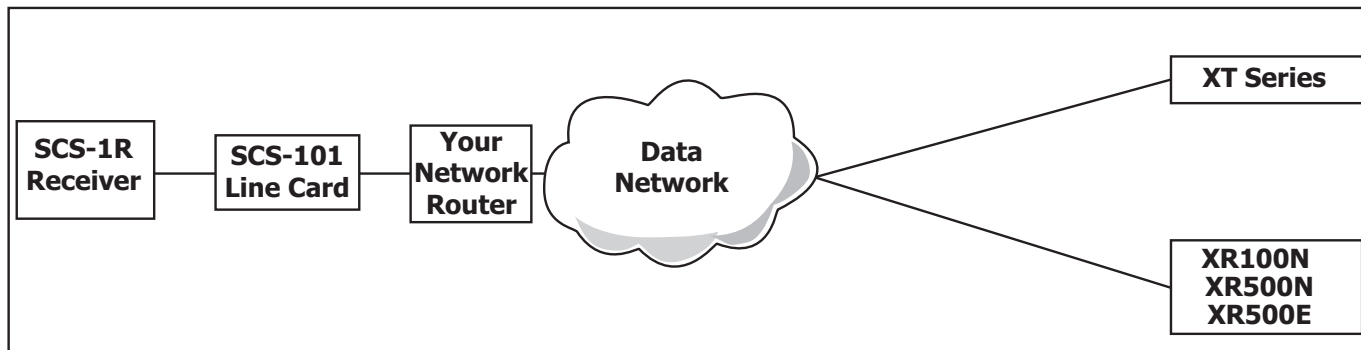


Figure 1: Network Monitoring Schematic

DMP Network Communication

DMP offers multiple solutions for Network and Internet communication to meet your needs. The XT Series, XR100N, XR500N and XR500E (Encrypted), panels offer built-in network communication. These products provide fully supervised, two-way network communications for the specified panels.

The built-in network capabilities of the XT Series, XR100N, XR500N, and XR500E panels let you simply connect your Internet cable directly to an available Ethernet connection. These panels can communicate alarm and system messages over a full-time Internet, LAN, or WAN Ethernet network connection to a DMP SCS-1R Receiver.

All these products offer state-of-the-art network communication by sending alarm data to the central station using either UDP (User Datagram Protocol) or TCP (Transmission Control Protocol) communication. DMP Network Monitoring™ is extremely fast, fully supervised, and provides reliable, high-security communication. UDP and TCP are completely compatible with existing Internet connection methods such as Frame Relay, ISDN, DSL, cable, satellite or virtually any other connection method.

The UDP encapsulation low-overhead and reverse-polling technology allow you to connect the alarm system to the subscriber's existing Internet connection with no impact on network performance. Also, the UDP protocol accommodates either simple firewall or proxy server configurations.

TCP enables two hosts to establish a connection and exchange data streams. TCP guarantees data delivery which guarantees packets are delivered in the same order in which they were sent.

Message authentication is processed through a proprietary authentication scheme, making the technology inaccessible to the hacker world, unlike potential weaknesses of common operating systems as described on hacker web-sites. This provides a more secure system when connecting to the Internet.

At the protected premise, installing the appropriate DMP technology is fast and easy. Simply use standard keypad programming to configure the XT Series™, XR100N, XR500N, XR500E, or iCOM_{SL}. These panels and the iCOM_{SL} router also support DHCP and NAT (Network Address Translation) and can be remotely tested and configured. Remote programming is protected by a strong eight-character password.

APPLICATION NOTE

iCOM_{SL}™ Routers

The iCOM_{SL}™ Network Alarm Communicator brings network and Network Alarm communication to the XR5FC FACP as well as any alarm panel from any manufacturer. It allows alarm panels to communicate alarm and system messages over a full-time Internet, LAN, or WAN Ethernet network connection to a DMP SCS-1R Receiver.

The iCOM_{SL} provides six programmable zones and six open collector outputs. Input Mode can run in either Slave operation or Stand-alone operation. In Slave Operation, it communicates alarm messages from any security and fire alarm panel. The XR5F can be used to provide outputs to the six programmable inputs of an iCOM_{SL} (refer to LT-0631).

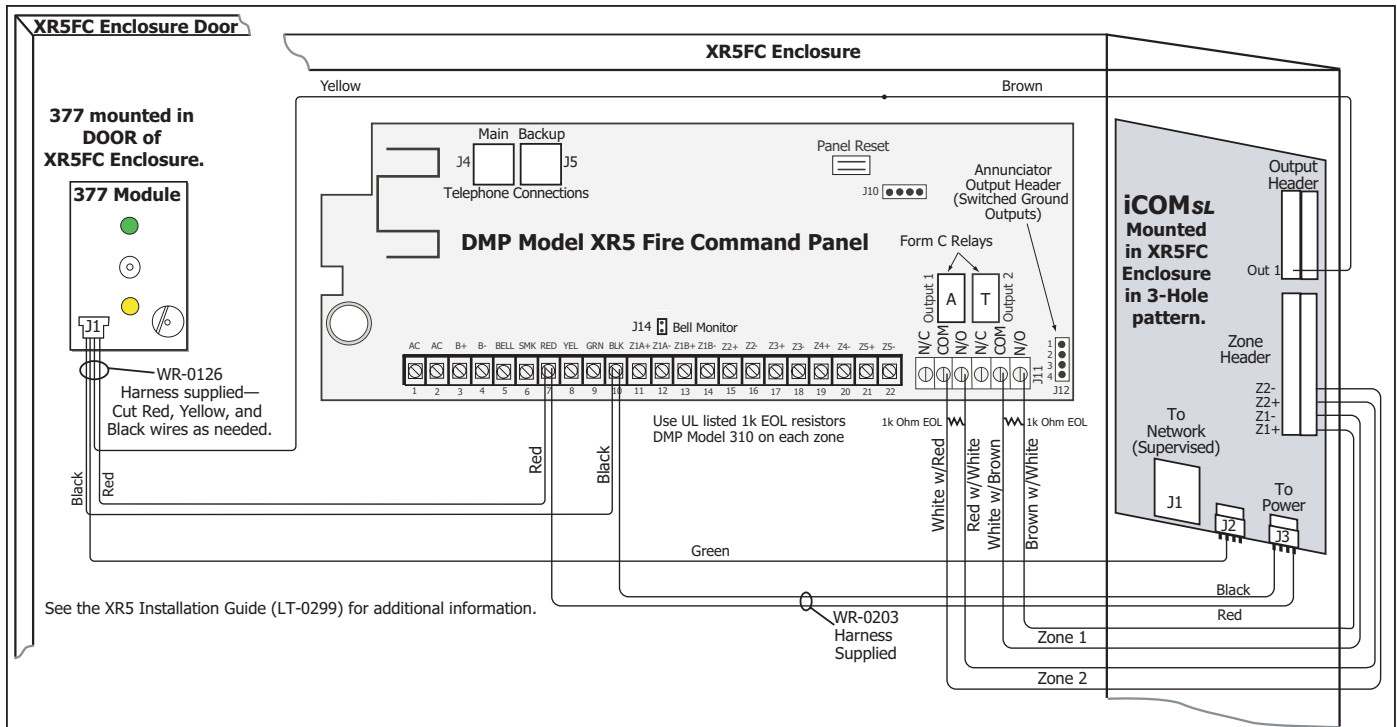


Figure 3: iCOM_{SL} with XR5FC FACP Installation

Stand-alone Operation

The iCOM_{SL} is versatile enough to use as a stand-alone security device, independent of any alarm panel. Providing six programmable zones and outputs, the iCOM_{SL} offers a compact and efficient alternative to a conventional alarm panel.

XT Series/XR100N/XR500N/XR500E Panel Operation

The XT Series, XR100N, XR500N, and XR500E have a built in Ethernet connector. Simply connect your Internet cable directly to the panel. This allows the panels to communicate alarm and system messages over a full-time Internet, LAN, or WAN Ethernet network connection to a DMP SCS-1R Receiver or a computer running DMP Alarm Monitoring™ software.

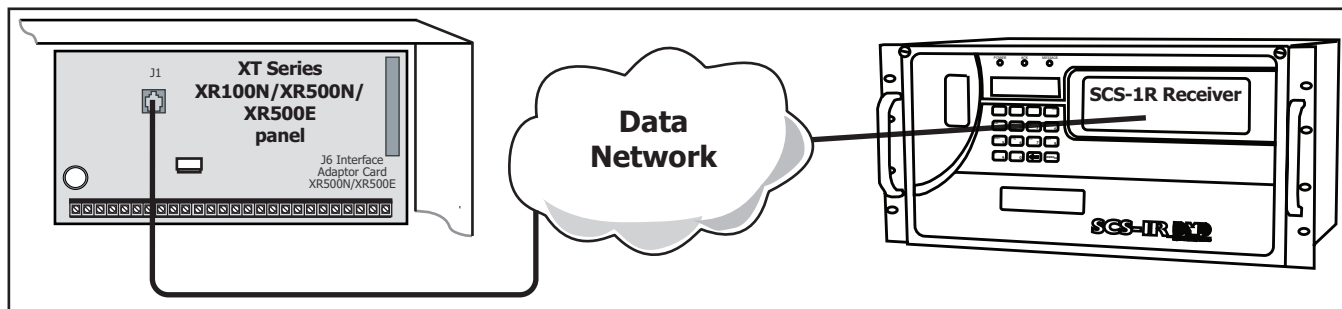


Figure 4: XT Series, XR100N, XR500N, XR500E and SCS-1R Receiver

Network Monitoring at a Central Station

To configure your SCS-1R Central Station Receiver for Network Monitoring you need the following items:

- SCS-1R Receiver
- SCS-101 Network Interface Card (level B or higher)
- Full-time Internet connection
- DMP Model 396 programming cable and a computer with HyperTerminal communication software (if using a computer to program the SCS-101)
- DMP 32-character keypad and Model 330 programming cable (if using a keypad to program the SCS-101)

Important Compatibility Information

The SCS-101 Level E hardware and Version 200 or higher software can ONLY be used with SCS-1R Receivers using firmware Version 903 or higher.

The SCS-101 line card Level D hardware and Version 103 or lower software can ONLY be used with the SCS-1R Version 902 or lower.

SCS-150 Main Processor Card

This processor card is an upgrade to the receiver, offering many new features and enhancements. The SCS-150 Processor contains the firmware for system operation, provides all time-keeping functions, and controls line cards, keypad, and printer. The new, faster card design offers a range of technology enhancements, including:

- 5,000-event memory
- Remote Panel programming via receiver line cards using new Auxiliary port
- Receiver system setup programming via SCS-1R keyboard/display and Remote Link™ via Auxiliary port
- Receiver software is now updatable using an SD card instead of EPROMs

SCS-150 Compatibility

The SCS-150/CONVERT (conversion kit) is fully compatible with existing SCS-1R receiver racks, power supplies, and line cards, and comes with all internal cables needed for installation in the SCS-1R receiver.

APPLICATION NOTE

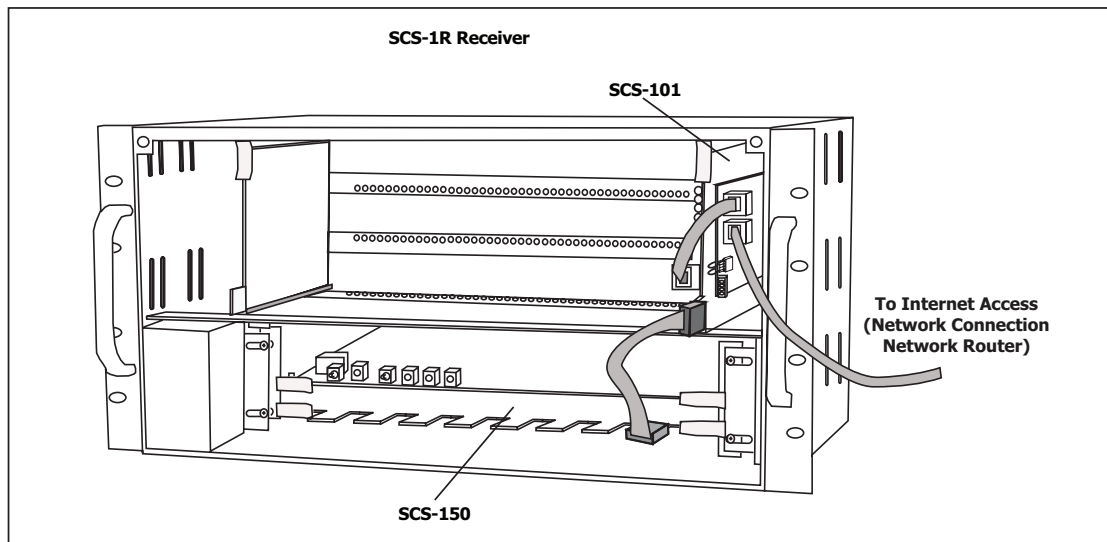


Figure 5: SCS-1R Receiver with SCS-101

What the System Administrator Needs to Know

The system administrator needs the following information to allow Network Monitoring signals to pass through a network firewall. Both incoming and outgoing signals pass through these settings. The port number is programmable and the system administrator may assign a different number. The default Port number is 2001 and the Protocol is UDP. As required, TCP operation is available and must be programmed in the Panel and the iCOMsL.

Internet Access Requirements

Several options are available for suitable full-time Internet connections, such as T-1, cable, DSL, satellite dish, or ISDN. The table below compares these connection types.

Be sure to obtain Internet access from a high-reliability source to assure maximum up-time. The same Internet access that monitors your security and fire panel can also be used to provide broadband Internet access for other uses, such as Internet access, e-mail, or a web server.

The DMP Advantage

Bringing your systems on-line using DMP products and technology offers several advantages over trying to accomplish the same thing with another manufacturer's product.

1. Connection, configuration, and operation simplicity – Bringing your DMP system on-line is as simple as connecting any other workstation or printer to the network.
2. A DMP system using the XT Series, XR100N, XR500N, XR500E panels or iCOMsL is truly a two-way communicator – Anything you normally do locally you can do remotely, such as manage user codes and arm or disarm any or all system areas. This is not one of those "spoofed" systems that connects to your security systems dialer connection and emulates a receiver. Those systems are only one-way. The DMP XT Series, XR100N, XR500N, XR500E and iCOMsL two-way systems put you in total control of the information you need.
3. A DMP Security System is network friendly – DMP systems connect at the same point as any other computer or printer. This is much safer for your network. Connecting a DMP system is as safe and non-intrusive as adding any other "dumb terminal" to your network.
4. Incredible versatility offered by the iCOMsL – Providing network communication for any alarm panel from any manufacturer, full data communication for DMP command processor panels. Also offering the ability to function as a stand-alone security device, placing the iCOMsL at the leading edge of alarm communication technology.
5. Information System department advantage – DMP products have minimal impact of your network bandwidth. The patented DMP NET format uses a reverse-polling technique for system supervision. This is far superior to the typical but inefficient forward polling systems that are constantly sending information across your network.

Bandwidth Usage

You may place up to five SCS-101 Network Interface Cards in an SCS-1R Receiver with the SCS-150 processor board. Each SCS-101 can manage up to 3,200 accounts that require check-in. With five SCS-101s installed, up to 16,000 accounts that require check-in can be managed by a single SCS-1R.

Message and Traffic Information	Size
Smallest Message per panel	18 Bytes
Largest Message per panel	93 Bytes
Most Frequent Message per panel (used for supervision)	23 Bytes
Opening/Closing Reports per panel (2 areas, 1 open and 1 close each per day)	284 Bytes
Average amount of traffic per day per panel (Based on a 2 area system, armed 15 hours per day)	5,324 Bytes
Average daily traffic for 200 locations (From the monitoring station)	1.1 MBytes

Recommended Number of Standard Line Network Accounts

Network Monitoring with DMP equipment also allows you to make the most efficient use of your Data Network and Network bandwidth. Each data transmission across the Data Network between a DMP panel and an SCS-1R Receiver is small and efficient. The table above shows the bandwidth required to monitor 200 network systems using DMP equipment. This table does not include the overhead imposed by Ethernet TCP or UDP protocols.



800-641-4282
www.dmp.com
Made in the USA

INTRUSION • FIRE • ACCESS • NETWORKS
2500 North Partnership Boulevard
Springfield, Missouri 65803-8877

LT-2029 © 2010 Digital Monitoring Products, Inc.

8/10

