White Paper

Networked door access system offers high-security, flexible installation options

Ethernet networking provides new capabilities in door access systems and enables those systems to deliver substantially faster operation than what is provided by traditional systems.

Many business customers already have Ethernet networks in place to support their regular operations, and by using the business customer's existing Ethernet networks, security dealers can minimize the material and labor costs involved in deploying networked door access. Typically business customers' Ethernet networks are connected to the Internet through a wide area broadband connection, and the networked door access system can use that connection for communications with a central monitoring station.

This white paper looks at an option in networked door access—the 734N Network Access Control Module from Digital Monitoring Products (DMP). The white paper highlights the minimal network bandwidth required by the 734N, along with the security features built into the product. In addition, it details two different installation options, offering dealers considerable flexibility to meet each customer's individual requirements.

The 734N Access Control Module from DMP allows security dealers to add networked access control capability to DMP XR150 and XR550 Series Control Panels. The module also can be used to support codeless arming and disarming of intrusion protection systems. The XR150 can support up to seven 734Ns, with each 734N connecting to a single door. With the XR550, up to 15 734Ns can be used, protecting as many as 15 doors.

Minimal bandwidth requirements

The 734N was designed to have minimal impact on network performance. The product is supervised in the panel through an exchange of data packets every five seconds. The payload of the data packets exchanged is a very small 18 bytes. The total traffic for all supervision, including network overhead, is approximately two kilobytes per minute per 734N. This would be equivalent to a very small email message.

If required, all the traffic between the 734N and the panel can be completely isolated from the rest of the network by connecting to a dedicated switch. (See "Installation Options" section).

Security Features

The security of the 734N module is multi-faceted.

Most importantly, the 734N is a single-purpose network device. What this means is that all the ports in the TCP/IP stack used in the 734N are disabled and allow no inbound connections. This design feature prevents a potential intruder from making any type of connection with the 734N through the network. Any communication between the 734N and the XR Series panel is initiated by the 734N.

For additional security, all communication between the 734N and the control panel is encrypted using 128-bit Advanced Encryption Standard (AES) communication. AES it the type of encryption selected by the National Institute of Standards and Technology (NIST) for encrypting U.S. government classified information up to the "secret" level.

Even if someone were to somehow intercept communications between the 734N and the panel (a virtually impossible scenario for the reasons outlined above), the interceptor would not be able to decipher the communications without using multiple supercomputers over a period of multiple decades.

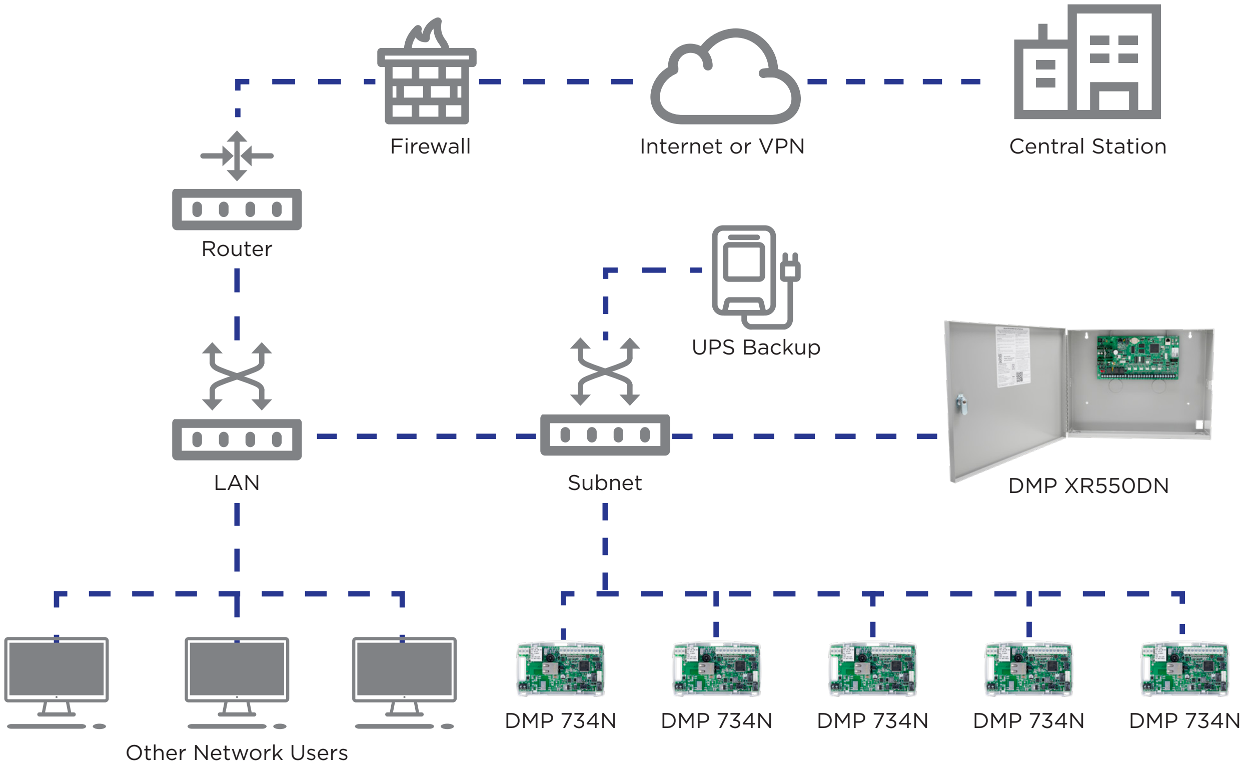
AES encryption has largely replaced the 56-bit Data Encryption Standard (DES), which was previously used by the U.S. government. It's important to note that doubling the key size for an algorithm does not simply double the required number of operations required to crack the key, but rather squares them. That means that if a device existed that could crack a 56-bit encryption key in one second, it would take that device billions of years to crack a 128-bit encryption key.

Installation options

There are two basic installation options for the 734N modules and the panel to which they are connected.

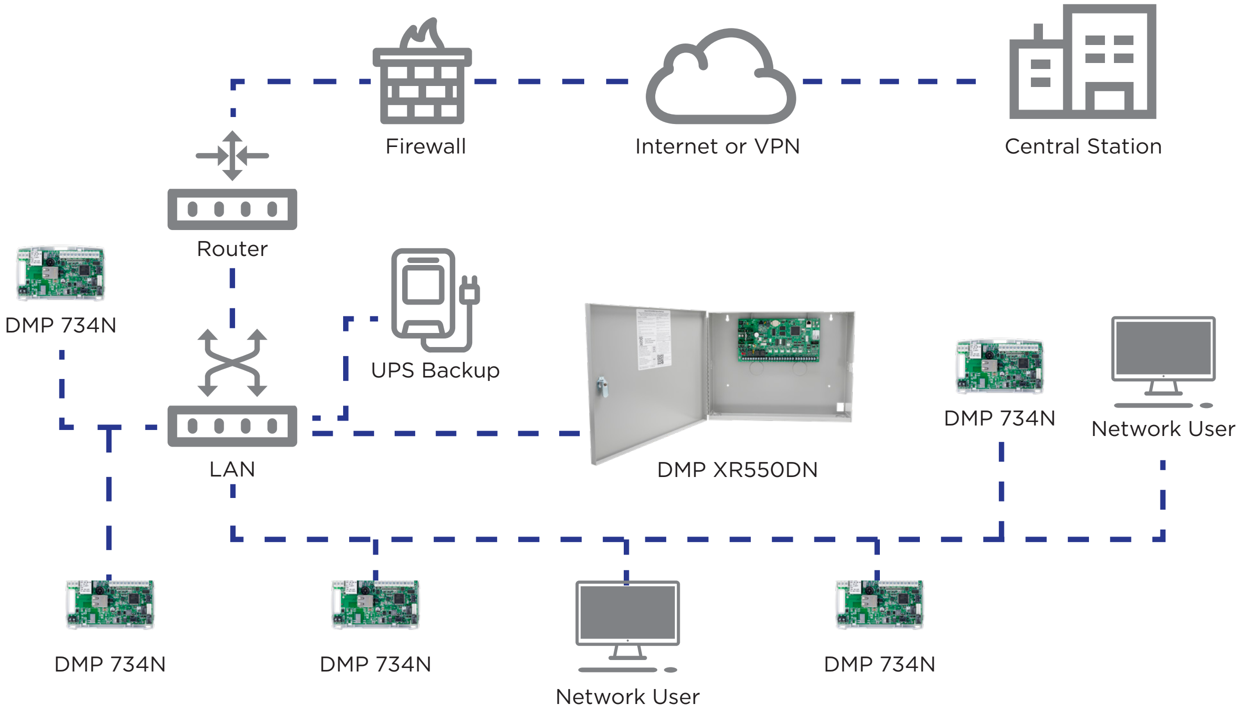
One option is to connect the 734N modules and the panel—and only those devices—to a single Ethernet switch, and then to connect the switch to the remainder of the network. When this approach is used, all traffic between the 734N modules and the panel is confined to the switch to which they are connected, while still allowing the panel to communicate with the central station through the customer's pre-existing network. The installers also should make sure that an auxiliary power supply is connected to the switch so that the system will be able to continue to operate in the event of a power failure. This option is illustrated in the following figure:

Segmented Application



Alternatively, the 734N modules and the panel can be directly connected to the pre-existing network without installing a separate switch for them. Here, too, an auxiliary power supply should be installed, and in this case it would back up the entire network. This option is illustrated in the figure below:

LAN Application



The second installation option is the most economical as it does not require a dedicated switch and, depending on where the 734N modules are located, it also may minimize the material and labor costs required for equipment wiring. But this option may not be appropriate for all customers.

Despite the minimal bandwidth requirements of the 734N module, some businesses may have a policy against allowing traffic from security devices to run over the network that supports their regular operations. For those customers the dedicated switch method or a virtual local area network (VLAN) may be required.

DMP is a privately held independent manufacturer of innovative intrusion, fire, access control, network and cellular communication products that are designed and made in the United States of America. DMP is the recognized leader in alarm communication over data networks, with products that are available through professional electronic security companies. For more information visit www.dmp.com.

866-266-2826
DMP.com
INTRUSION • FIRE • ACCESS • NETWORKS
2500 North Partnership Boulevard
Springfield, Missouri 65803-8877