






- Easy Installation
- Fast and Secure

Use Powerline...



...or use Wi-Fi



Easy Installation

- Connect IP communicator to ECP buss, zone triggers or the dialer via the dialer capture module
- Connect to an available port on the **router** 
- Router connection can be made wirelessly using **Powerline**  or **Wi-Fi**  devices
- An IP address may be issued dynamically by the router (**DHCP**).  A **static IP**  address may also be used.
- Program account information into IP communicator using AlarmNet Direct programmer or 7720P
- Honeywell control panels may be downloaded using IP communication and Compass software



System Operation

- Once powered and connected, the IP communicator automatically seeks the AlarmNet servers in a private, secure and authenticated connection
- **Port 443**  is typically available for outbound secure Internet access
- No installation knowledge about encryption keys, network protocol, the **firewall**  or other computer networking knowledge is required to complete the installation






AlarmNet Dual-Redundant Network

AlarmNet-i solutions do not compromise the security of your router

- Opening **IP server ports**  may allow malicious attacks on your network
- The chance for **viruses**  on the computer are increased as is the likelihood of a post-sale service call



Fast and Secure

- AlarmNet maintains fully **AES encrypted**  secure connections to both the central station as well as the protected premise and only communicates in a totally authenticated and secure manner
- No **encryption keys**  are ever transmitted – maximum data security is assured
- AlarmNet-i solutions only listen to AlarmNet and are super resistant to typical attacks
- Typical response time, end-to-end to the central station, is under six seconds
- AlarmNet offers automatic **technology rollover**  with re-transmission to the central station using any of three technologies including, Internet, Mobitex radio or 800 number POTS service



Internet, wireless communications or POTS

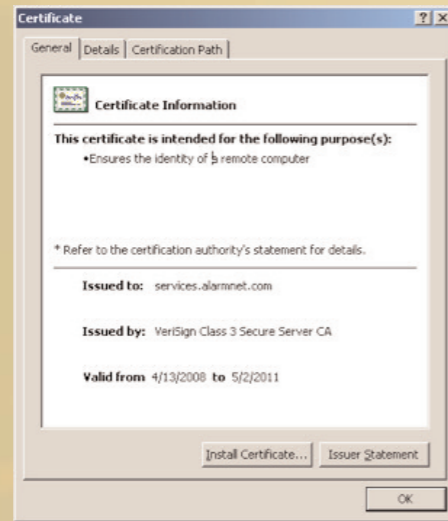


Professional Central Station



Port 443

- A secure Internet connection which is most commonly used for online transactions, such as banking, passing of credit card information, corporate information systems, personal information, etc.
- When port 443 is being used you will see https://www.
 - The s in https represents a secure connection
 - https://services.alarmnet.com/TotalConnect/
- This ensures additional protection from eavesdroppers (hackers)
 - Additional encryption to complement the AlarmNet device encryption methods
 - A signed certificate is typically used for HTTPS connectivity
 - These certificates are typically purchased and signed by companies such as VeriSign, which encrypt and authenticate data flow between computer networks which most people recognize as the small padlock icon in their Web browser when shopping online.
- The advantage AlarmNet has by using port 443 is that the ports are typically open in a corporate, small business or residential network and are not prone to the data inspection



Firewall

- A firewall is a dedicated appliance, or software running on a computer, which inspects network traffic passing through it and denies or permits passage of network traffic based on a set of rules programmed in the appliance (router) or software (firewall settings in Internet Explorer)
- A firewall's basic task is to regulate the type of traffic between computer networks based on a set of rules that permit, deny, encrypt and decrypt network traffic between computer networks
- A firewall's function within a network is similar to firewalls with fire doors in building construction. For computer networks, firewalls are used to prevent network intrusion to the private network. In building construction, firewalls are intended to contain and delay structural fire from spreading to adjacent structures.

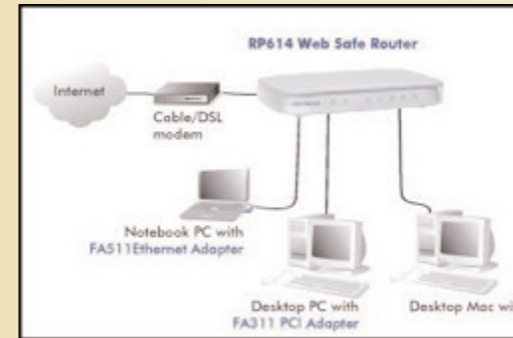


Router

- A router is a device in computer networking that forwards data packets to their destinations based on their addresses
- Many residential end-users may want to set-up a LAN (Local Area Network) or WLAN (Wireless LAN) and connect all computers to the Internet without having to pay a full broadband subscription service to their ISP for each computer on the network. This is when residential end-users will want to look at smaller routers (often called broadband routers) that enable two or more computers to share an Internet connection. Within a business or organization, you may need to connect multiple computers to the Internet, but also want to connect multiple private networks. These are the types of functions a router is designed for.
- What defines a router is not its shape, color, size or manufacturer, but its job function of routing data packets between computers. A cable modem which routes data between your PC and your ISP can be considered a router. In its most basic form, a router could simply be one of two computers running the Windows 98 (or higher) operating system connected together using ICS (Internet Connection Sharing). In this scenario, the computer that is connected to the Internet is acting as the router for the second computer to obtain its Internet connection.
- Broadband or ICS routers allow you to share one Internet connection between multiple computers. They will look a bit different depending on the manufacturer or brand, but wired routers are generally a small box-shaped hardware device with ports on the front or back

into which you plug each computer, along with a port to plug in your broadband modem. These connection ports allow the router to do its job of routing the data packets between each of the computers and the data going to and from the Internet.

This image shows the flow of data to multiple computers sharing one high speed Internet connection.



- Wireless broadband routers look much the same as a wired router with the obvious exception of the antenna on top and the lack of cable running from the PCs to the router when it is set up. Creating a wireless network adds a few more security concerns as opposed to wired networks, but wireless broadband routers do have extra levels of embedded security. Along with the features found in wired routers, wireless routers also provide features relevant to wireless security such as Wi-Fi Protected Access (WPA) and wireless MAC address filtering. Additionally, most wireless routers can be configured for "invisible mode" so that your wireless network cannot be scanned by outside wireless clients. Wireless routers will often include ports for Ethernet connections as well.



Wi-Fi

- Wi-Fi is the trade name for the popular wireless technology used in home networks, mobile phones, video games and other electronic devices that require some form of wireless networking capability. In particular, it covers the various IEEE 802.11 technologies (including 802.11n, 802.11b, 802.11g, and 802.11a).
- The purpose of Wi-Fi is to provide wireless access to digital content. This content may include applications, audio and visual media, Internet connectivity or other data. Wi-Fi generally makes access to information easier since it can eliminate some of the physical restraints of wiring.



Power-Line Ethernet Adapters

- A power line Ethernet bridge is a HomePlug device used to extend a LAN into a separate room using the existing electrical system in the building. An Ethernet cable from the network router is plugged into a bridge which plugs into an AC wall outlet. In a separate room, a second bridge plugs into the wall outlet to provide an Ethernet port for the computer.



DHCP (Dynamic Host Configuration Protocol)

- A protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. In some systems, the device's IP address can even change while it is still connected.
- Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address.



Static IP Addressing

- An IP address which is permanently assigned to a particular user. Static IP addressing is, however, generally used by businesses or any organization running its own site. It is also available for individuals from some ISPs, allowing them to set up FTP or Websites on their home computers. Static IP addressing allows a higher degree of tracking of an individual user's actions on the Internet, but requires actions from a network administrator to implement.

Data Encryption

- Encryption is the process of taking information that exists in some readable form and converting it into non-readable form
- The advantage of data encryption is that even if other control mechanisms are comprised by an intruder, the data is still unusable because it is not readable



Encryption Keys

- The 7845i-GSM supports private key encryption. Private key encryption means that both the sender and the receiver know the KEY used to encrypt the data.
 - Each device produced by Honeywell is loaded with a globally unique identifier called a MAC number and a large random number or KEY. This KEY and MAC number are also stored in the AlarmNet servers. When a device contacts AlarmNet, it sends the MAC number in the clear followed by the message that is encrypted using the KEY data. The server looks up its copy of the KEY based on the MAC number and uses that KEY to decrypt the message.
- The 7845i-GSM uses 256 bit AES (Rijndael) encryption which is required for certain government installations. The AlarmNet-i AES Encryption Software Module Version 1.0 contained in the Honeywell products has NIST approval. Listings for this approval can be found at <http://csrc.nist.gov/cryptval/aes/aesval.html>; certification number 127.



AES Encryption

- Advanced Encryption Standard. AES is one of the most secure encryption technologies and has been cleared by the U.S. Government for secret and top-secret data encryption.



AlarmNet Technology Rollover

- The AlarmNet Data Center provides a unique capability for redundancy and diverse alarm paths for our central station customers
- Alarm Paths:
 - Internet (7810iR-ent can connect directly to an automation system port)
 - Radio (7830R connected to a 685 or MX800 receivers and its radio line card)
 - 800 Plus service (POTS transmission to most central station receivers)
- How it works:
 - The central station uses Internet as the primary path, radio as the secondary path and 800 plus as the third path (example)
 - The AlarmNet Data Center routes message to the central station. If the primary path is unavailable, that respective message is "bounced back". The data center then routes that message to the secondary path immediately. If the path is unavailable (bounced back) the data center then sends the message to the third path immediately.
 - Internet paths and radio paths are supervised typically every five minutes via the AlarmNet Data Center
 - Central stations can make their own choice for their technology preference and how many paths they want to have for rollover capability



Ports

- Every IP address is divided into ports. IP addresses are divided into ports so that one IP address can be used by multiple programs to send and receive data at the same time. Ports make it possible for you to check your e-mail and browse the web at the same time. This is possible because browsing the web uses port 80 and getting your e-mail uses port 110. You can think of a port as a path for data.
- Port forwarding opens a specific port to a computer behind the router, allowing all incoming traffic on that port to be sent directly to that server.

Generally, forwarding is done so the outside world can connect to some type of server that is located behind your router/firewall.

- By default, a router will block all connections. By allowing an incoming connection, you are instructing the router to pass the request (typically) without any type of data integrity.
- Port forwarding simply allows the firewall to accept a connection on a port and forward it to an IP address on the inside of your network which could potentially lead to eavesdroppers or create vulnerabilities on your network for viruses, spyware, etc.



Viruses

- A computer virus attaches itself to a program or file enabling it to spread from one computer to another, leaving infections as it travels. Like a human virus, a computer virus can range in severity: some may cause only mildly annoying effects while others can damage your hardware, software or files.