

Secure IP Forwarding in the Security Industry - White Paper

This white paper addresses the issue of how an independent alarm company can maintain their independence and at the same time uses IP (Internet Protocol) to send signals to their central stations. It also addresses the need to provide redundancy as well as disaster recovery for IP based security and fire alarms.

The alarm panel business has progressed significantly since its early days of only communicating their signals through the use of copper phone lines. Today system vendors and installers have a choice of several robust means of connecting with a monitoring station including dial up, radio links of all ranges, cellular and IP pathways.

Of all these transmission methods, the Internet version has grown the fastest in the shortest amount of time since its mass introduction. Internet based communications have been replacing the original standard telephone line in homes and residences around the United States in staggering numbers on a daily basis. The most common transport method (protocol) used on the Internet is known as TCP/IP or IP. Alarm panel manufactures have taken advantage of both TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) protocols; each has its own advantages.

AT&T recently released a staggering fact that 700,000 POT's (Plain Old Telephone) lines a month are either being turned off or are getting converted to VoIP (Voice over IP). This is mind numbing to understand how many alarm systems will potentially be in danger of either not working at all or working sporadically over VoIP circuits. This has become a primary driver to move alarm systems off of dial up (800) and onto some kind of a wired or wireless IP based platform.

In the early 1990's, during the explosion of Toll-Free numbers, the telecommunications industry took a huge positive turn towards standardization when the FCC (Federal Communications Commission) mandated that providers allow owners of toll-free numbers to have

complete control of how and who carried the traffic of calls that came to their numbers.

This newfound freedom gave way to major competition and cost reductions for the consuming public. Toll-free owners could not only switch their carriers based on best price or service offerings, they had new technologies and features at hand. For example, they could change where their calls would terminate all based on time, origination and many other parameters and eventually were able to do this in near real time.

Now, some 20 years later, in an effort to understand and regulate the future of telecommunications in this country, the creation of the American Recovery and Reinvestment Act of 2009 was established by the US Government. From this came a directive to the US Federal Communications to submit a National Broadband Plan to Congress by February 17, 2010. As one of the public responses to the FCC's request for comments regarding this plan, AT&T acknowledged not only the forthcoming obsolescence, but also the current obsolescence of the existing wire line telephone system. In its filing, the company called upon the Commission to begin consideration of a formal deadline for the transition of all wire line customers to a system comprising of broadband and IP-based connectivity and even refraining from referring to 3G or 4G services in a cellular context.

Research for what we now call the Internet was started in the early 1960's. Initially it was a network designed for the military to be able to communicate after an atomic war. The idea was to have a network where messages could be automatically routed via the fastest way possible and also that it was self-healing in the event of network segment failures.

In the 1970's this continued to evolve, universities were starting to get connected to various networks, email is starting to emerge and by the mid 1980's the terms Internet, information superhighway and World Wide Web were the new buzzwords.

In technical terms every device on an IP network is assigned a numeric address, XXX.XXX.XXX.XXX. While this was very efficient it was unrealistic for the general public to remember these numbers especially if these numbers needed to change for any reason.

In order to not only make it easier to remember where things were but also to allow for emergency moves or changes to networks, URL's (Uniform Resource Locators) were created, so as an example instead of typing in 216.64.210.28 you could just type www.pepsi.com.

The Internet has been engineered to use URL's through a very complex system called DNS (Domain Name Servers) and while this works well for Internet browsing and sending emails there are a number of problems such as speed, reliability and security when it comes to sending critical signals to the central stations. For this reason the industry has not allowed the use of DNS servers, only static IP addresses for alarm signaling. As this White Paper is being written, one of the worlds most famous hacking organizations "Anonymous," has taken down the largest DNS provider in the world, GoDaddy. For almost a full day GoDaddy was unable to serve DNS records out, imagine if this were your alarm account.

The original IP addressing scheme (IPv4) uses 4 groups of numbers ranging from 0 to 255 (example 216.064.210.028) this gives you a total of addresses available worldwide of 4,294,967,296. We have reached a point where there are real shortages. The next scheme out there is IPv6 this allows for 8 groups of 4 hexadecimal value's (example 2001:0db8:85a3:0042:0000:8a2e:0370:7334) it's unlikely we will ever run out in the foreseeable future.

Presently in the alarm industry, the current offerings of IP based alarm equipment (alarm panels) are ones that use anywhere from 1 to 18 hard coded IPv4 addresses. Normally two are used as a primary and a secondary for backup. These addresses have traditionally belonged to the central station or more technically to the ISP's (Internet Service Providers) that is serving the central monitoring station.

With toll free numbers used for dial up panels, you could change the ownership or where they were terminated at very easily and instantly. This is not true with IP. Most IP addresses belong to or are registered with the ISP and these addresses are not portable at all and more importantly never will be. If the dealer wants to change central stations or the central station wants to switch or has to switch ISP's, these static IP addresses will all



have to be changed in the field equipment. This could cost an alarm company 100's of thousands of dollars and take months to do.

Even if the central station was set up for the special routing BGP (Border Gateway Protocol) that an installer could route IPv4 addresses to, it's too cost prohibitive and there are not enough IPv4 addresses left in small blocks so that your average alarm company could afford to obtain it's own IPv4 address space from ARIN (American Registry for Internet Numbers).

This is where *KeepYourIP* comes in. We have our own ARIN IP addresses that we can lease to alarm companies or central stations. The addresses work just like the current toll free numbers in that you can have them re-routed in real time with no special equipment at the central station or be forced to use BGP, or have any of the expense of ASN's (Autonomous System Numbers).

This gives the alarm company or central station the freedom to use IP based panels without the concern of reprogramming all the field equipment in the event they need to move central stations or change ISP's.

What *KeepYourIP* offers is a very simple web interface. It allows the alarm company or central station to obtain new IP addresses, enter a label or name, specify a port and then the target destination IP address. The whole set up takes only a few minutes to complete.

KeepYourIP has three data centers, two in California (Irvine and San Diego) and the other in Florida. In these facilities we have all the servers running in a virtual cloud type of environment, there is no single set of servers to fail, this is how we can keep five nines percentage of uptime.

Most alarm companies and central stations will get IP addresses provisioned in pairs, one from each bi-coastal data center. This will give total redundancy as these facilities are on different ISP's and different backbone networks.



There is no easier or cost effective way to manage IP traffic for alarm companies and central station in existence. There is no one in the business with as much experience in routing alarm traffic than *KeepYourIP*. We have pioneered this IP transmission for the alarm industry and have a proven unrivaled track record in this area, one that no other company can compare to or even compete with.



14 Goodyear

STE 125

Irvine, CA 92618

866-444-7007

info@keepyourip.com

www.keepyourip.com